SAP BusinessObjects Business Intelligence
Dokumentversion: 4.1 Support Package 3 - 2014-04-06

Administratorhandbuch für SAP BusinessObjects Business Intelligence

Inhaltsverzeichnis

1 Dokumentverlauf. 19

2 Erste Schritte. 21

2.1 Informationen zu diesem Handbuch. 21

2.1.1 An welchen Benutzerkreis richtet sich dieses Handbuch?. 21

2.1.2 Informationen zur Business-Intelligence-Plattform. 21

2.1.3 Variablen. 22

2.1.4 Terminologie. 22

2.2 Vor dem Beginn. 24

2.2.1 Grundlegende Begriffe. 24

2.2.2 Schlüsselprogramme für die Verwaltung. 27

2.2.3 Schlüsselaufgaben. 29

3 Architektur. 32

3.1 Überblick über die Architektur. 32

3.1.1 Komponentendiagramm. 33

3.1.2 Architekturschichten. 34

3.1.3 Datenbanken. 35

3.1.4 Server, Hosts und Cluster. 36

3.1.5 Webanwendungsserver. 37

3.1.6 Software Development Kits. 38

3.1.7 Datenquellen. 40

3.1.8 Authentifizierung und Einzelanmeldung. 40

3.1.9 SAP-Integration. 42

3.1.10 Integrierte Versionskontrolle. 43

3.1.11 Upgrade-Pfad. 44

3.2 Server, Dienste, Knoten und Hosts. 44

3.2.1 Serveränderungen seit XI 3.1. 46

3.2.2 Dienste. 47

3.2.3 Dienstkategorien. 55

3.2.4 Servertypen. 57

3.2.5 Server. 63

3.3 Clientanwendungen. 65

3.3.1 Installiert mit Clienttools von SAP BusinessObjects Business Intelligence. 65

3.3.2 Installiert mit SAP BusinessObjects Business Intelligence. 69

3.3.3 Separat erhältliche Anwendungen. 70

3.3.4 Webanwendungsclients. 71

3.4 Prozess-Workflows. 75

3.4.1 Start und Authentifizierung. 75

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3.4.2 Programmobjekte. . . . 77
3.4.3 Crystal Reports. . . . 79
3.4.4 Web Intelligence. . . . 83
3.4.5 Analysis. . . . 85

4 Systemkonfigurationsassistent. . . . 87
4.1 Einführung in den Systemkonfigurationsassistenten. . . . 87
4.2 Angeben der von Ihnen verwendeten Produkte. . . . 87
4.3 Auswählen von Implementierungsvorlagen. . . . 89
4.4 Festlegen von Datenordnerspeicherorten. . . . 91
4.5 Überprüfen von Änderungen. . . . 93
4.6 Protokolldateien und Antwortdateien. . . . 93
4.6.1 Verwenden von Antwortdateien. . . . 94

5 Verwalten von Lizenzen. . . . 98
5.1 Verwalten von Lizenzschlüsseln. . . . 98
5.1.1 Anzeigen von Lizenzinformationen. . . . 98
5.1.2 Hinzufügen von Lizenzschlüsseln. . . . 98
5.1.3 So zeigen Sie die aktuelle Kontoaktivität an. . . . 99

6 Verwalten von Benutzern und Gruppen. . . . 100
6.1 Übersicht über die Kontoverwaltung. . . . 100
6.1.1 Benutzerverwaltung. . . . 100
6.1.2 Gruppenverwaltung. . . . 101
6.1.3 Verfügbare Authentifizierungstypen 102
6.2 Verwalten von Enterprise-Konten und allgemeinen Konten. . . . 103
6.2.1 So erstellen Sie ein Benutzerkonto. . . . 103
6.2.2 So ändern Sie ein Benutzerkonto. . . . 104
6.2.3 Löschen eines Benutzerkontos. . . . 105
6.2.4 Erstellen von neuen Gruppen. . . . 106
6.2.5 So ändern Sie die Eigenschaften einer Gruppe. . . . 106
6.2.6 So zeigen Sie Gruppenmitglieder an. . . . 106
6.2.7 Hinzufügen von Untergruppen. . . . 107
6.2.8 Festlegen von Gruppenmitgliedschaften. . . . 107
6.2.9 So löschen Sie eine Gruppe. . . . 108
6.2.10 Hinzufügen von Benutzern oder Benutzergruppen in Massenvorgängen. . . . 108
6.2.11 So aktivieren Sie das Guest-Konto. . . . 109
6.2.12 Hinzufügen von Benutzern zu Gruppen. . . . 109
6.2.13 Ändern der Kennworteinstellungen. . . . 111
6.2.14 Gewähren von Zugriff für Benutzer und Gruppen. . . . 112
6.2.15 Steuern des Zugriffs auf Posteingänge von Benutzern. . . . 113
6.2.16 Konfigurieren von BI-Launchpad-Optionen. . . . 113

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6.2.17 Verwalten von Attributen für Systembenutzer . . . 116
6.2.18 Priorisierung von Benutzerattributen über mehrere Authentifizierungsoptionen hinweg . . . 118
6.2.19 Hinzufügen von neuen Benutzerattributen. . . . 118
6.2.20 Bearbeiten benutzerdefinierter Benutzerattribute. . . . 119
6.3 Verwalten von Aliasen. . . . 120
6.3.1 Erstellen von Benutzern und Hinzufügen eines Drittthersteller-Alias. . . . 120
6.3.2 Erstellen eines neuen Alias für einen vorhandenen Benutzer. . . . 121
6.3.3 So weisen Sie einen Alias eines anderen Benutzers zu. . . . 121
6.3.4 So löschen Sie einen Alias. . . . 122
6.3.5 So deaktivieren Sie einen Alias. . . . 123

7 Festlegen von Rechten. . . . 124
7.1 Funktionsweise von Rechten in der BI-Plattform. . . . 124
7.1.1 Zugriffsberechtigungen. . . . 124
7.1.2 Einstellungen für erweiterte Rechte. . . . 125
7.1.3 Übernahme. . . . 126
7.1.4 Typspezifische Rechte. . . . 131
7.1.5 Ermitteln effektiver Rechte. . . . 132
7.2 Verwalten von Sicherheitseinstellungen für Objekte in der CMC. . . . 133
7.2.1 So lassen Sie Rechte für einen Prinzipal auf einem Objekt anzeigen. . . . 134
7.2.2 So weisen Sie einer Zugriffskontrollliste für ein Objekt Prinzipale hinzu. . . . 134
7.2.3 Ändern der Sicherheit für einen Prinzipal auf einem Objekt. . . . 135
7.2.4 Festlegen von Rechten für einen Ordner der obersten Ebene in der BI-Plattform. . . . 136
7.2.5 Überprüfen von Sicherheitseinstellungen für ein Subjekt. . . . 136
7.3 Arbeiten mit Zugriffsberechtigungen. . . . 139
7.3.1 Auswählen zwischen den Zugriffsberechtigungen *Ansicht* und *Ansicht auf Abruf*. . . . 141
7.3.2 Kopieren von vorhandenen Zugriffsberechtigungen. . . . 142
7.3.3 Erstellen von Zugriffsberechtigungen. . . . 143
7.3.4 Umbenennen von Zugriffsberechtigungen. . . . 143
7.3.5 So löschen Sie eine Zugriffsberechtigung. . . . 143
7.3.6 So ändern Sie Rechte in einer Zugriffsberechtigung. . . . 144
7.3.7 Verfolgen der Beziehung zwischen Zugriffsberechtigungen und Objekten. . . . 145
7.3.8 Standortübergreifende Verwaltung von Zugriffsberechtigungen. . . . 145
7.4 Auflösen der Übernahme. . . . 147
7.4.1 So deaktivieren Sie die Übernahme. . . . 148
7.5 Delegieren der Administration mithilfe von Rechten. . . . 148
7.5.1 Welche der beiden Optionen "*Rechte von Benutzern für Objekte ändern*" sollte verwendet werden?. . . . 150
7.5.2 Eigentümerrechte. . . . 152
7.6 Zusammenfassung der Empfehlungen zur Verwaltung von Rechten. . . . 152

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8 Sichern der BI-Plattform. 153
8.1 Überblick zum Thema Sicherheit 153
8.2 Notfallwiederherstellungsplanung. 153
8.3 Allgemeine Empfehlungen zur Sicherung der Implementierung. 154
8.4 Konfigurieren der Sicherheit für Dritthersteller-Serverpakete. 155
8.5 Aktive Vertrauensstellung. 155
8.5.1 Anmeldetoken. 156
8.5.2 Ticketverfahren für verteilte Sicherheit. 156
8.6 Sitzungen und Sitzungsnachverfolgung. 157
8.6.1 CMS-Sitzungsnachverfolgung. 158
8.6.2 Verwalten von Sitzungen. 158
8.7 Umgebungsschutz. 159
8.7.1 Webbrowser zu Webserver. 159
8.7.2 Webserver und die BI-Plattform. 160
8.8 Auditieren von Änderungen an der Sicherheitskonfiguration 160
8.9 Prüfen der Webvorgänge. 160
8.9.1 Schutz vor unberechtigten Anmeldeversuchen. 160
8.9.2 Kennworteinschränkungen. 161
8.9.3 Anmeldeeinschränkungen. 161
8.9.4 Benutzerbeschränkungen. 161
8.9.5 Guest-Konto-Einschränkungen. 162
8.10 Verarbeitungserweiterungen. 162
8.11 Übersicht über die BI-Plattform-Datensicherheit. 162
8.11.1 Sicherheitsmodi für die Datenverarbeitung. 163
8.12 Verschlüsselung in der BI-Plattform. 165
8.12.1 Arbeiten mit Clusterschlüsseln. 166
8.12.2 Verschlüsselungsbeauftragte. 168
8.12.3 Verwalten von Kryptografieschlüsseln in der CMC. 169
8.13 Konfigurieren von Servern für SSL. 174
8.13.1 Erstellen von Schlüssel- und Zertifikatdateien. 174
8.13.2 Einrichten von SSL bei Verwaltung des Zertifikats durch eine Zertifizierungsstelle. 176
8.13.3 Konfigurieren des SSL-Protokolls. 179
8.14 Erläuterung der Kommunikation zwischen BI-Plattform-Komponenten. 183
8.14.1 Überblick über BI-Server und Kommunikationsports. 183
8.14.2 Kommunikation zwischen BI-Plattform-Komponenten 186
8.15 Konfigurieren der BI-Plattform für Firewalls. 191
8.15.1 Konfigurieren des Systems für Firewalls. 192
8.15.2 Debuggen einer Firewall-Implementierung. 195
8.16 Beispiele für typische Firewallszenarios. 196
8.16.1 Beispiel: Implementierung der Anwendungsschicht in einem getrennten Netzwerk. 196
8.16.2 Beispiel: Trennung von Thick-Client und Datenbankschicht von BI-Plattform-Servern durch eine Firewall. 199

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.17 Firewall-Einstellungen für integrierte Umgebungen. 201
8.17.1 Spezifische Firewall-Richtlinien für die SAP-Integration. 201
8.17.2 Firewall-Konfiguration für die JD Edwards EnterpriseOne-Integration. 203
8.17.3 Spezifische Firewallrichtlinien für Oracle EBS. 204
8.17.4 Firewall-Konfiguration für PeopleSoft Enterprise-Integration 205
8.17.5 Firewall-Konfiguration für die Siebel-Integration. 207
8.18 BI-Plattform und Reverse-Proxy-Server 208
8.18.1 Unterstützte Reverse Proxy-Server 208
8.18.2 Allgemeine Informationen zur Implementierung von Webanwendungen 209
8.19 Konfigurieren von Reverse Proxy-Servern für BI-Plattform-Webanwendungen. 209
8.19.1 Ausführliche Anweisungen zur Konfiguration von Reverse Proxy-Servern. 209
8.19.2 Konfigurieren der Reverse Proxy-Server. 210
8.19.3 Konfigurieren des Apache-2.2-Reverse Proxy-Servers für die BI-Plattform 211
8.19.4 Konfigurieren des WebSEAL-6.0-Reverse Proxy-Servers für die BI-Plattform 211
8.19.5 Konfigurieren von Microsoft ISA 2006 für die BI-Plattform 212
8.20 Spezielle Konfiguration für die BI-Plattform in Reverse-Proxy-Umgebungen. 214
8.20.1 Aktivieren eines Reverse Proxys für Webdienste. 214
8.20.2 Aktivieren des Stammpfads für Sitzungscookies für ISA 2006. 216
8.20.3 Aktivieren von Reverse Proxys für SAP BusinessObjects Live Office. 219

9 Authentifizierung. 220
9.1 Authentifizierungsoptionen in der BI-Plattform. 220
9.1.1 Primäre Authentifizierung. 221
9.1.2 Sicherheits-Plugins. 222
9.1.3 Einzelanmeldung bei der BI-Plattform. 222
9.2 Enterprise-Authentifizierung. 225
9.2.1 Übersicht über die Enterprise-Authentifizierung. 225
9.2.2 Einstellungen der Enterprise-Authentifizierung. 225
9.2.3 Ändern der Enterprise-Einstellungen. 226
9.2.4 Aktivieren der vertrauenswürdigen Authentifizierung. 227
9.2.5 Konfiguration der vertrauenswürdigen Authentifizierung für Webanwendungen. 229
9.3 LDAP-Authentifizierung. 239
9.3.1 Verwenden der LDAP-Authentifizierung. 239
9.3.2 Konfigurieren der LDAP-Authentifizierung. 241
9.3.3 Zuordnen von LDAP-Gruppen. 251
9.4 Windows AD-Authentifizierung. 262
9.4.1 Verwenden der Windows AD-Authentifizierung. 262
9.4.2 Vorbereiten des Domänencontrollers. 263
9.4.3 Konfigurieren der AD-Authentifizierung in der CMC. 264
9.4.4 Konfigurieren des BI-Plattform-Diensts zur Ausführung des SIA. 271
9.4.5 Konfigurieren des Webanwendungsservers für die AD-Authentifizierung. 273
9.4.6 Einrichten der Einzelanmeldung. 282

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.4.7 Fehlerbehebung Windows AD-Authentifizierung. . . . 297
9.5 SAP-Authentifizierung. . . . 299
9.5.1 Konfigurieren der SAP-Authentifizierung . . . 299
9.5.2 Erstellen von Benutzerkonten für die BI-Plattform. . . . 300
9.5.3 Verbinden mit SAP-Berechtigungssystemen. . . . 301
9.5.4 Einstellen von SAP-Authentifizierungsoptionen. . . . 303
9.5.5 Importieren von SAP-Rollen. . . . 307
9.5.6 Konfigurieren der Secure Network Communication (SNC). . . . 311
9.5.7 Einrichten der Einzelanmeldung beim SAP-System. . . . 324
9.5.8 Konfigurieren der Einzelanmeldung für SAP Crystal Reports und SAP Netweaver. . . . 328
9.6 PeopleSoft-Authentifizierung. . . . 329
9.6.1 Übersicht. . . . 329
9.6.2 Aktivieren der PeopleSoft Enterprise-Authentifizierung. . . . 329
9.6.3 Zuordnen von PeopleSoft-Rollen zur BI-Plattform. . . . 330
9.6.4 Zeitgesteuertes Verarbeiten von Benutzeraktualisierungen. . . . 333
9.6.5 Verwenden der PeopleSoft-Sicherheitsbrücke. . . . 335
9.7 JD Edwards-Authentifizierung. . . . 345
9.7.1 Übersicht. . . . 345
9.7.2 Aktivieren der JD Edwards EnterpriseOne-Authentifizierung. . . . 345
9.7.3 Zuordnen von JD-Edwards-EnterpriseOne-Rollen zur BI-Plattform. . . . 346
9.7.4 Zeitgesteuertes Verarbeiten von Benutzeraktualisierungen. . . . 348
9.8 Siebel-Authentifizierung. . . . 350
9.8.1 Aktivieren der Siebel-Authentifizierung. . . . 350
9.8.2 Zuordnen von Rollen zur BI-Plattform. . . . 351
9.8.3 Zeitgesteuertes Verarbeiten von Benutzeraktualisierungen. . . . 354
9.9 Oracle EBS-Authentifizierung. . . . 356
9.9.1 Aktivieren der Oracle-EBS-Authentifizierung. . . . 356
9.9.2 Zuordnen von Oracle-E-Business Suite-Rollen zur BI-Plattform. . . . 357
9.9.3 Aufheben der Zuordnung von Rollen . . . 361
9.9.4 Anpassen von Rechten für zugeordnete Oracle EBS-Gruppen und -Benutzer . . . 362
9.9.5 Konfigurieren der Einzelanmeldung für SAP Crystal Reports und Oracle EBS. . . . 363

10 Serververwaltung. . . . 365
10.1 Arbeiten mit dem Verwaltungsbereich "Server" in der CMC. . . . 365
10.2 Verwalten von Servern mithilfe von Skripts unter Windows . . . 368
10.3 Verwalten von Servern unter Unix . . . 368
10.4 Anzeigen und Ändern des Serverstatus. . . . 369
10.4.1 Anzeigen des Status von Servern. . . . 369
10.4.2 Starten, Stoppen und Neustarten von Servern. . . . 370
10.4.3 Anhalten eines Central Management Servers. . . . 373
10.4.4 Aktivieren und Deaktivieren von Servern. . . . 374
10.5 Hinzufügen, Klonen oder Löschen von Servern. . . . 375

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10.5.1 Hinzufügen, Klonen und Löschen von Servern. . . . 375
10.6 Clustern von Central Management Servern. . . . 378
10.6.1 Clustern von Central Management Servern. . . . 378
10.7 Verwaltung von Servergruppen. . . . 383
10.7.1 Erstellen von Servergruppen. . . . 384
10.7.2 Arbeiten mit Serveruntergruppen. . . . 385
10.7.3 Ändern der Gruppenzugehörigkeit eines Servers. . . . 386
10.7.4 Zugriffsrechte auf Server und Servergruppen für Benutzer. . . . 387
10.8 Konfigurieren von Adaptive Processing Servern für Produktionssysteme. . . . 388
10.9 Ermitteln der Systemleistung. . . . 389
10.9.1 Überwachen der BI-Plattform-Server. . . . 389
10.9.2 Analysieren der Servermetrik. . . . 389
10.9.3 Anzeigen der Systemmetrik. . . . 390
10.9.4 Protokollieren der Serveraktivität. . . . 390
10.10 Konfigurieren von Servereinstellungen. . . . 391
10.10.1 Ändern der Eigenschaften eines Servers. . . . 392
10.10.2 Anwenden von Diensteinstellungen auf mehrere Server. . . . 392
10.10.3 Arbeiten mit Konfigurationsvorlagen. . . . 393
10.11 Konfigurieren von Netzwerkeinstellungen für Server. . . . 395
10.11.1 Optionen für die Netzwerkumgebung. . . . 396
10.11.2 Optionen zur Identifizierung des Serverhosts. . . . 396
10.11.3 Konfigurieren eines mehrfach vernetzten Rechners. . . . 398
10.11.4 Konfigurieren von Portnummern. . . . 401
10.12 Verwalten von Knoten. . . . 404
10.12.1 Verwenden von Knoten. . . . 404
10.12.2 Hinzufügen eines neuen Knotens. . . . 406
10.12.3 Neuerstellen von Knoten. . . . 411
10.12.4 Löschen von Knoten. . . . 414
10.12.5 Umbenennen eines Knotens. . . . 417
10.12.6 Verschieben von Knoten. . . . 419
10.12.7 Skriptparameter. . . . 423
10.12.8 Hinzufügen von Windows-Server-Abhängigkeiten. . . . 428
10.12.9 Ändern von Benutzeranmeldedaten für einen Knoten. . . . 428
10.13 Umbenennen eines Rechners in einer BI-Plattform-Implementierung. . . . 429
10.13.1 Ändern von Cluster-Namen. . . . 429
10.13.2 Ändern der IP-Adresse. . . . 429
10.13.3 Umbenennen von Rechnern. . . . 431
10.14 Verwenden von 32-Bit- und 64-Bit-Bibliotheken von Drittherstellern mit der BI-Plattform. . . . 435
10.15 Verwalten von Server- und Knotenplatzhaltern. . . . 436
10.15.1 Anzeigen von Serverplatzhaltern. . . . 436
10.15.2 Anzeigen und Bearbeiten der Platzhalter eines Knotens. . . . 436

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

11 Verwalten von CMS-Datenbanken (Central Management Server). 437
11.1 Verwalten von Verbindungen zur CMS-Systemdatenbank. 437
11.1.1 Auswählen von SQL Anywhere als CMS-Datenbank. 437
11.1.2 Auswählen von SAP HANA als CMS-Datenbank. 438
11.2 Auswählen einer neuen oder bereits vorhandenen CMS-Datenbank. 439
11.2.1 So wählen Sie eine neue oder vorhandene CMS-Datenbank unter Windows aus. 440
11.2.2 So wählen Sie eine neue oder vorhandene CMS-Datenbank unter UNIX aus. 441
11.3 Neu erstellen der CMS-Systemdatenbank. 441
11.3.1 So erstellen Sie die CMS-Systemdatenbank unter Windows neu. 442
11.3.2 So erstellen Sie die CMS-Systemdatenbank unter UNIX neu. 443
11.4 Kopieren von Daten von einer CMS-Systemdatenbank in eine andere. 444
11.4.1 Vorbereitung für das Kopieren einer CMS-Systemdatenbank. 444
11.4.2 Kopieren einer CMS-Systemdatenbank unter Windows. 445
11.4.3 Kopieren von Daten von einer CMS-Systemdatenbank unter UNIX. 446

12 Verwalten von Web Application Container Servern (WACS). 447
12.1 WACS. 447
12.1.1 Web Application Container Server (WACS). 447
12.1.2 Hinzufügen oder Entfernen zusätzlicher WACS in einer Implementierung. 450
12.1.3 Hinzufügen oder Entfernen von Diensten auf dem WACS. 453
12.1.4 Konfigurieren von HTTPS/SSL. 455
12.1.5 Unterstützte Authentifizierungsmethoden. 458
12.1.6 Konfigurieren von AD Kerberos für WACS 458
12.1.7 Konfigurieren der AD Kerberos-Einzelanmeldung 466
12.1.8 Konfigurieren von RESTful-Webdiensten. 468
12.1.9 WACS und Ihre IT-Umgebung. 478
12.1.10 Konfigurieren von Webanwendungseigenschaften. 481
12.1.11 Fehlerbehebung. 482
12.1.12 WACS-Eigenschaften. 485

13 Sichern und Wiederherstellen Ihres Systems. 487
13.1 Übersicht über Sicherung und Wiederherstellung. 487
13.2 Terminologie. 487
13.3 Anwendungsfälle für Sichern und Wiederherstellen. 489
13.4 Sicherungen. 490
13.4.1 Sichern des gesamten Systems. 491
13.4.2 Sichern der Servereinstellungen. 494
13.4.3 Sichern von BI-Inhalt. 497
13.5 Wiederherstellen des Systems. 497
13.5.1 Wiederherstellen des gesamten Systems. 498
13.5.2 Wiederherstellen der Servereinstellungen. 503
13.5.3 Wiederherstellen von BI-Inhalt. 506

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

13.6 BackupCluster- und RestoreCluster-Skript. 506

14 Kopieren Ihrer BI-Plattform-Implementierung. 509
14.1 Übersicht des Kopierens des Systems. 509
14.2 Terminologie. 509
14.3 Anwendungsfälle für Systemkopien. 509
14.4 Planen des Kopierens Ihres Systems. 510
14.5 Überlegungen und Einschränkungen. 511
14.6 Verfahren zum Kopieren vom System. 513
14.6.1 Exportieren aus einem Quellsystem. 513
14.6.2 Importieren in ein Zielsystem. 517

15 Hochstufverwaltung. 521
15.1 Herzlich willkommen bei der Hochstufverwaltung. 521
15.1.1 Übersicht. 521
15.1.2 Funktionen. 521
15.1.3 Anwendungszugriffsrechte. 522
15.1.4 Unterstützung für WinAD in der Hochstufverwaltung. 523
15.1.5 Überschreibungsinformationen in BI-Plattform 4.1 SP3. 523
15.2 Erste Schritte mit der Hochstufverwaltung. 524
15.2.1 Zugriff auf die Hochstufverwaltung. 524
15.2.2 Benutzeroberflächen-Komponenten. 524
15.2.3 Verwenden der Option "Einstellungen". 526
15.3 Verwenden der Hochstufverwaltung. 533
15.3.1 Erstellen und Löschen von Ordnern. 533
15.3.2 Einen Auftrag erstellen. 534
15.3.3 Erstellen eines neuen Auftrags durch Kopieren eines vorhandenen Auftrags. 537
15.3.4 Suchen nach Aufträgen. 537
15.3.5 Bearbeiten von Aufträgen. 538
15.3.6 Hinzufügen eines InfoObjects zu einem Auftrag. 539
15.3.7 Verwalten der Abhängigkeiten eines Auftrags. 540
15.3.8 Suchen nach abhängigen Objekten 541
15.3.9 Hochstufen von Aufträgen mit nicht verbundenen Repositorys. 541
15.3.10 Hochstufen eines Auftrags mithilfe einer LCMBIAR-Datei. 543
15.3.11 Zeitsteuern von Auftragshochstufungen. 546
15.3.12 Anzeigen des Auftragsverlaufs. 548
15.3.13 Rollback für Aufträge ausführen. 548
15.4 Verwalten unterschiedlicher Versionen eines InfoObjects. 551
15.4.1 Anwendungszugriffsrechte für die Versionsverwaltung. 551
15.4.2 Sichern und Wiederherstellen von Subversion-Dateien. 552
15.5 Hochstufen des vollständigen Repository-Inhalts mithilfe der Hochstufverwaltung. 553
15.5.1 Vorbereiten der Quell- und Zielsysteme. 553

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15.5.2 Migrationsstrategien. 555
15.6 Schritte zur vollständigen Systemhochstufung. 556
15.6.1 Hochstufen von Benutzern und Benutzergruppen (Auftrag 1). 557
15.6.2 Hochstufen abhängiger Objekte (Auftrag 2). 557
15.6.3 Hochstufen von Primärobjekten (Auftrag 3). 559
15.6.4 Nach der Hochstufung. 559
15.7 Verwenden der Befehlszeilenoption. 560
15.7.1 Ausführen des Befehlszeilenprogramms unter Windows. 560
15.7.2 Ausführen des Befehlszeilenprogramms unter Unix. 561
15.7.3 Befehlszeilenparameter. 561
15.7.4 Beispiel für eine Eigenschaftendatei. 567
15.8 Verwenden des erweiterten Change and Transport System. 568
15.8.1 Voraussetzungen. 568
15.8.2 Konfigurieren der BI-Plattform und CTS+-Integration. 569
15.8.3 Hochstufen von Aufträgen über CTS. 576

16 Versionsverwaltung. 580
16.1 Verwalten mehrerer Versionen von BI-Ressourcen 580
16.2 Manuelles Starten und Stoppen von Subversion unter Unix. 581
16.3 Erforderliche Dateien für Subversion unter Solaris 10 und RedHat Linux 5. 582
16.4 Verwenden der Option „Versionsverwaltungseinstellungen“. 582
16.4.1 Standardeinstellungen für das Versionsverwaltungssystem. 583
16.4.2 Einrichten des Versionsverwaltungssystems ClearCase in Windows. 584
16.4.3 Einrichten des Versionsverwaltungssystems ClearCase in Unix. 584
16.5 Vergleichen von verschiedenen Versionen desselben Auftrags. 585
16.6 Aktualisieren von Subversion-Inhalten. 585
16.7 Unterversionen für geclusterte Processing Job Server konfigurieren. 586
16.7.1 Option A: Konfigurieren des Subversion-Hauptrechners, bevor das Versionsverwaltungssystem verwendet wird. 586
16.7.2 Option B: Konfigurieren von Subversion, nachdem das Versionsverwaltungssystem das Verzeichnis der Arbeitskopie erstellt hat. 586
16.7.3 Konfigurieren anderer Subversion-Rechner. 587
16.8 Zugriff auf dieselbe ClearCase-Sicht von verschiedenen Versionsverwaltungsservern aus. 588

17 Grafischer Vergleich. 589
17.1 Grafischer Vergleich in der Hochstufverwaltung. 589
17.1.1 Vergleich von Objekten oder Dateien mittels des Grafischen Vergleichs. 590
17.1.2 Vergleichen von Objekten oder Dateien mithilfe des Versionsverwaltungssystems. 591
17.1.3 Zeitgesteuerte Verarbeitung des Vergleichs. 592

18 Verwalten von Anwendungen. 594
18.1 Verwalten von Anwendungen über die CMC. 594
18.1.1 Übersicht. 594

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18.1.2 Gemeinsame Einstellungen für Anwendungen. 595
18.1.3 Anwendungsspezifische Einstellungen. 596
18.2 Verwalten von Anwendungen über BOE.war-Eigenschaften. 636
18.2.1 BOE-WAR-Datei. 636
18.3 Anpassen der Eingangspunkte für die BI-Launchpad- und die OpenDocument-Anmeldung. 645
18.3.1 Dateispeicherorte von BI-Launchpad und OpenDocument. 645
18.3.2 Definieren einer benutzerdefinierten Anmeldeseite. 646
18.3.3 Hinzufügen der vertrauenswürdigen Authentifizierung bei der Anmeldung. 647
18.4 Anpassen von Anwendungsbenutzeroberflächen. 648
18.4.1 Web Intelligence. 648

19 Verwalten von Verbindungen und Universen. 664
19.1 Verwalten von Verbindungen. 664
19.1.1 So löschen Sie eine Universumsverbindung. 664
19.2 Verwalten von Universen. 665
19.2.1 So löschen Sie Universen. 665

20 Überwachung. 666
20.1 Informationen zur Überwachung. 666
20.2 Monitoring-Begriffe. 666
20.2.1 Architektur. 668
20.3 Konfigurieren von Datenbank-Support für die Überwachung 670
20.3.1 Konfiguration zur Verwendung der Derby-Datenbank. 671
20.3.2 Konfiguration für die Verwendung der Audit-Datenbank. 671
20.4 Konfigurationseigenschaften. 678
20.4.1 JMX-Endpunkt-URL. 682
20.4.2 HTTPS-Authentifizierung für Überwachungsdiagnosen. 683
20.4.3 Kennwortverschlüsselung für Diagnosen. 683
20.5 Integrieren in andere Anwendungen. 683
20.5.1 Integrieren des Monitorings in IBM Tivoli. 684
20.5.2 Integrieren des Monitorings in SAP Solution Manager 686
20.6 Cluster-Unterstützung für den Überwachungsserver. 687
20.7 Fehlerbehebung. 687
20.7.1 Dashboard. 688
20.7.2 Warnmeldungen. 688
20.7.3 Kontrollmodulliste. 689
20.7.4 Diagnosen. 690
20.7.5 Metriken. 691
20.7.6 Diagramm. 691

21 Auditing. 692
21.1 Übersicht. 692

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

21.2 Seite CMC-Auditing. 698
21.2.1 Auditing-Status. 698
21.2.2 Konfigurieren von Audit-Ereignissen. 700
21.2.3 Konfigurationseinstellungen des Audit-Datenspeichers (ADS). 703
21.3 Audit-Ereignisse. 704
21.3.1 Überwachungsereignisse und -details. 714

22 Plattformsuche. 734
22.1 Plattformsuche. 734
22.1.1 Plattformsuche-SDK. 734
22.1.2 Geclusterte Umgebung. 734
22.2 Einrichten der Plattformsuche. 735
22.2.1 Implementieren von OpenSearch. 735
22.2.2 Konfigurieren von Reverse-Proxy-Servern. 737
22.2.3 Konfigurieren von Anwendungseigenschaften in der CMC. 737
22.3 Arbeiten mit der Plattformsuche. 741
22.3.1 Indizierung von Inhalten im CMS-Repository. 741
22.3.2 Liste der Indizierungsfehler. 743
22.3.3 Suchergebnisse. 743
22.4 Integration der Plattformsuche mit SAP NetWeaver Enterprise Search. 750
22.4.1 Erstellen eines Connectors in SAP NetWeaver Enterprise Search 750
22.4.2 Importieren einer Benutzerrolle in die BI-Plattform. 751
22.5 Suchvorgänge über NetWeaver Enterprise Search. 752
22.6 Auditing. 752
22.7 Fehlerbehebung. 753
22.7.1 Selbstreparatur. 753
22.7.2 Problemszenarios. 753

23 Föderation. 756
23.1 Föderation. 756
23.2 Begriffe in Föderation. 757
23.3 Verwalten von Sicherheitsrechten. 759
23.3.1 Für die ursprüngliche Website erforderliche Rechte. 759
23.3.2 Für die Zielwebsite erforderliche Rechte. 760
23.3.3 Föderation-spezifische Rechte. 761
23.3.4 Replizieren der Sicherheit eines Objekts. 762
23.3.5 Replizieren der Sicherheit durch Zugriffsberechtigungen. 763
23.4 Optionen für Replikationstypen und Replikationsmodi. 763
23.4.1 Einseitige Replikation 763
23.4.2 Beidseitige Replikation 764
23.4.3 "Von ursprünglicher Website aus aktualisieren" oder "Von Ziel aus aktualisieren". 764
23.5 Replizieren von Dritthersteller-Benutzern und -Gruppen. 766

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

23.6 Replizieren von Universen und Universumsverbindungen. 767
23.7 Verwalten von Replikationslisten. 768
23.7.1 Erstellen von Replikationslisten. 769
23.7.2 Ändern von Replikationslisten. 771
23.8 Verwalten von Remoteverbindungen. 772
23.8.1 Erstellen von Remoteverbindungen. 773
23.8.2 Ändern von Remoteverbindungen. 775
23.9 Verwalten von Replikationsaufträgen. 775
23.9.1 Erstellen von Replikationsaufträgen. 776
23.9.2 Zeitgesteuertes Verarbeiten von Replikationsaufträgen. 778
23.9.3 Ändern von Replikationsaufträgen. 778
23.9.4 Anzeigen eines Protokolls nach einem Replikationsauftrag. 779
23.10 Verwalten der Objektbereinigung. 780
23.10.1 Verwenden der Objektbereinigung. 780
23.10.2 Beschränkungen der Objektbereinigung. 780
23.10.3 Häufigkeit der Objektbereinigung. 781
23.11 Erkennen und Auflösen von Konflikten. 782
23.11.1 Konfliktauflösung bei der einseitigen Replikation. 782
23.11.2 Konfliktauflösung bei der beidseitigen Replikation. 784
23.12 Verwenden von Web Services in Föderation. 788
23.12.1 Sitzungsvariablen 788
23.12.2 Zwischenspeichern von Dateien 788
23.12.3 Benutzerdefinierte Implementierung 789
23.13 Remote-Zeitsteuerung und lokale Ausführung von Instanzen. 790
23.13.1 Remote-Zeitsteuerung. 790
23.13.2 Lokal ausgeführte Instanzen. 792
23.13.3 Instanzenfreigabe. 792
23.14 Importieren und Höherstufen replizierter Inhalte. 793
23.14.1 Importieren replizierter Inhalte. 793
23.14.2 Importieren replizierter Inhalte und Fortsetzen der Replikation 794
23.14.3 Höherstufen von Inhalten aus einer Testumgebung. 795
23.14.4 Neuverweisen auf eine Zielwebsite. 795
23.15 Optimale Vorgehensweisen. 796
23.15.1 Einschränkungen der aktuellen Version. 799
23.15.2 Behandeln von Fehlermeldungen. 800

24 Ergänzende Konfigurationen für ERP-Umgebungen. 804
24.1 Konfigurationen für die SAP NetWeaver-Integration. 804
24.1.1 Integrieren in SAP NetWeaver Business Warehouse (BW). 804
24.2 Konfigurieren für die JD Edwards-Integration. 847
24.2.1 Konfigurieren der Einzelanmeldung für SAP Crystal Reports. 847
24.2.2 Konfigurieren der SSL (Secure Sockets Layer) für JD-Edwards-Integrationen. 848

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.3 Konfigurieren für die PeopleSoft Enterprise-Integration. 850
24.3.1 Konfigurieren der Einzelanmeldung (SSO) für SAP Crystal Reports und PeopleSoft Enterprise. 850
24.3.2 Konfigurieren der SSL-Kommunikation. 851
24.3.3 Leistungsoptimierung für PeopleSoft-Systeme. 852
24.4 Konfiguration für Siebel-Integration. 854
24.4.1 Konfigurieren von Siebel für die Integration in die SAP-BI-Plattform. 854
24.4.2 Erstellen des Crystal-Reports-Menüelements. 855
24.4.3 Kontextsensitivität. 856
24.4.4 Konfigurieren der Einzelanmeldung für SAP Crystal Reports und Siebel. 858
24.4.5 Konfigurieren für Secure Sockets Layer-Kommunikation. 859

25 Verwalten und Konfigurieren von Protokollen. 861
25.1 Protokollieren der Ablaufverfolgung für Komponenten. 861
25.2 Ablaufverfolgungsprotokollierungsebenen. 861
25.3 Konfigurieren der Serververfolgung. 862
25.3.1 Festlegen der Protokollierungsebene in der CMC. 863
25.3.2 Festlegen der Protokollierungsebene für für mehrere Server in der CMC. 863
25.3.3 Konfigurieren der Serververfolgung mit der Datei "BO_trace.ini". 864
25.4 Konfiguration der Ablaufverfolgung für Webanwendungen. 867
25.4.1 Einstellen der Ablaufverfolgungsprotokollierungsebene der Webanwendung in der CMC 867
25.4.2 Konfigurieren der Ablaufverfolgungseinstellungen mit der Datei `BO_trace.ini`. 868
25.5 Konfiguration der Ablaufverfolgung für das Upgrade-Management-Tool. 873
25.5.1 Konfiguration der Ablaufverfolgung für das Upgrade-Management-Tool. 874
25.6 Konfigurieren der Verfolgung für BI-Plattform-Client-Anwendungen. 874

26 Integration in SAP Solution Manager. 875
26.1 Übersicht über die Integration. 875
26.2 Checkliste für die SAP Solution Manager-Integration. 875
26.3 Verwalten der System Landscape Directory-Registrierung. 876
26.3.1 Registrierung der BI-Plattform in der Systemlandschaft. 876
26.3.2 Auslösungszeitpunkt der SLD-Registrierung. 878
26.3.3 Protokollieren der SLD-Konnektivität 878
26.4 Verwalten von Solution Manager Diagnostics Agents. 879
26.4.1 Übersicht über Solution Manager Diagnostics (SMD). 879
26.4.2 Arbeiten mit SMD Agents. 879
26.4.3 SMAdmin-Benutzerkonto. 880
26.5 Verwalten der Leistungsinstrumentation. 880
26.5.1 Leistungsinstrumentation für die BI-Plattform. 880
26.5.2 Einrichten der Leistungsinstrumentation für die BI-Plattform. 881
26.5.3 Leistungsinstrumentation für die Webschicht. 882

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

26.5.4 Protokolldateien der Instrumentation . . . 882
26.6 Ablaufverfolgung mit SAP Passport. . . . 883

27 Befehlszeilenverwaltung. . . . 884
27.1 Unix-Skripte. . . . 884
27.1.1 Skripte: Dienstprogramme. . . . 884
27.1.2 Skriptvorlagen. . . . 889
27.1.3 In der BI-Plattform verwendete Skripte. . . . 890
27.2 Windows-Skripte. . . . 891
27.2.1 ccm.exe. . . . 892
27.3 Serverbefehlszeilen. . . . 895
27.3.1 Überblick über Befehlszeilen. . . . 895
27.3.2 Standardoptionen für alle Server. . . . 895
27.3.3 Central Management Server. . . . 896
27.3.4 Crystal Reports Processing Server und Crystal Reports Cache Server. . . . 898
27.3.5 Dashboards Processing Server und Dashboards Cache Server. . . . 899
27.3.6 Job Server. . . . 900
27.3.7 Adaptive Processing Server. . . . 901
27.3.8 Report Application Server. . . . 902
27.3.9 Web Intelligence Processing Server. . . . 903
27.3.10 Input und Output File Repository Server. . . . 904
27.3.11 Event Server. . . . 906

28 Repository Diagnostic Tool. . . . 907
28.1 Übersicht über das Repository Diagnostic Tool. . . . 907
28.2 Verwenden des Repository Diagnostic Tool. . . . 907
28.2.1 Verwenden des Repository Diagnostic Tool. . . . 908
28.2.2 Parameter für das Repository Diagnostic Tool. . . . 909
28.3 Inkonsistenzen zwischen CMS und FRS. . . . 915
28.4 Inkonsistenzen in den CMS-Metadaten. . . . 916

29 Anhang "Rechte". . . . 920
29.1 Informationen über den Anhang zu Berechtigungen. . . . 920
29.2 Allgemeine Rechte. . . . 920
29.3 Rechte für bestimmte Objekttypen. . . . 922
29.3.1 Ordnerrechte. . . . 922
29.3.2 Kategorien. . . . 923
29.3.3 Desktop Intelligence-Dokumente. . . . 923
29.3.4 Notizen. . . . 925
29.3.5 Crystal-Reports-Berichte. . . . 926
29.3.6 Web-Intelligence-Dokumente. . . . 926
29.3.7 Benutzer und Gruppen. . . . 927

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

29.3.8 Zugriffsberechtigungen. 929
29.3.9 Universumsrechte (.unv). 929
29.3.10 Universumsrechte (.unx). 931
29.3.11 Zugriffsberechtigungen für Universumsobjekte. 932
29.3.12 Verbindungsrechte. 933
29.3.13 Anwendungen. 935

30 Servereigenschaften (Anhang). 948
30.1 Über Servereigenschaften (Anhang). 948
30.1.1 Allgemeine Servereigenschaften. 948
30.1.2 Kerndienste-Eigenschaften. 950
30.1.3 Eigenschaften von Konnektivitätsdiensten. 963
30.1.4 Eigenschaften von Crystal-Reports-Diensten. 967
30.1.5 Analysis Services-Eigenschaften. 976
30.1.6 Eigenschaften des Datenföderations-Diensts. 978
30.1.7 Eigenschaften der Web-Intelligence-Dienste. 978
30.1.8 Eigenschaften der Dashboards-Dienste. 986

31 Anhang "Servermetrik". 989
31.1 Info zu Servermetriken (Anhang). 989
31.1.1 Allgemeine Servermetriken 990
31.1.2 Central Management Server-Metriken. 992
31.1.3 Connection Server-Metriken. 995
31.1.4 Event Server-Metriken. 996
31.1.5 File Repository Server-Metriken. 996
31.1.6 Adaptive Processing Server-Metriken. 997
31.1.7 Web Application Container Server-Metriken. 1002
31.1.8 Adaptive Job Server-Metriken. 1003
31.1.9 Crystal-Reports-Server-Metriken. 1005
31.1.10 Web Intelligence Server-Metriken. 1008
31.1.11 Dashboard-Servermetriken. 1009

32 Anhang "Server- und Knotenplatzhalter". 1012
32.1 Server- und Knotenplatzhalter. 1012

33 ADS-Schema (Audit-Datenspeicher). 1022
33.1 Übersicht. 1022
33.2 Schemadiagramm. 1022
33.3 ADS-Tabellen (Audit-Datenspeicher). 1022

34 Überwachungsdatenbankschema (Anhang). 1031
34.1 Trenddatenbankschema. 1031

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

35 Systemkopie-Arbeitsblatt (Anhang). 1034
35.1 Systemkopie-Arbeitsblatt. 1034

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1 Dokumentverlauf

Die folgende Tabelle enthält eine Übersicht über die wichtigsten Dokumentänderungen.

Version	Datum	Beschreibung
SAP BusinessObjects BI 4.1	Mai 2013	Erste Veröffentlichung dieses Dokuments
SAP BusinessObjects BI 4.1 Support Package 1	August 2013	• Das Kapitel “Hochstufverwaltung” wurde aktualisiert. • Das Kapitel “Verwalten von Lizenzen” wurde aktualisiert. • Sonstige Korrekturen und kleinere Aktualisierungen.

SAP BusinessObjects BI 4.1 Support Package 2	November 2013	• Das Kapitel “Versionsverwaltung” wurde aktualisiert.
		  ○ Der Abschnitt “Versionsverwaltung unter Solaris 10 starten” wurde hinzugefügt.
		  ○ Der Abschnitt “Manuelles Starten und Stoppen von Subversion unter Unix” wurde hinzugefügt.
		  ○ Der Abschnitt “Standardeinstellungen des Versionsverwaltungssystems” wurde hinzugefügt.
		  ○ Der Abschnitt “Verwenden der Option Einstellungen des Versionsverwaltungssystems” wurde aktualisiert.
		• Das Kapitel “Hochstufverwaltung” wurde aktualisiert.
		  ○ Der Abschnitt “Verwenden der Option LCM-Überschreibungseinstellungen” wurde aktualisiert.
		  ○ Der Abschnitt “Verwenden der Befehlszeilenoption” wurde aktualisiert.
		  ○ Der Abschnitt “Befehlszeilentool-Parameter” wurde aktualisiert.
		• Das Kapitel “Repository Diagnostic Tool” wurde aktualisiert.
		• Der Abschnitt “Anpassen der Web-Intelligence-Oberfläche” wurde aktualisiert.
		• Sonstige Korrekturen und kleinere Aktualisierungen.

SAP BusinessObjects BI 4.1 Support Package 3	März 2014	• Der Abschnitt “Verwalten von Sitzungen” wurde hinzugefügt. • Der Abschnitt “Anpassen von Anwendungs-Benutzeroberflächen” wurde neu strukturiert und aktualisiert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Version	Datum	Beschreibung
		• Design-Studio-Auditing wurde hinzugefügt. • Abschnitt zur Änderung des CMS-Anforderungs-Ports wurde hinzugefügt. • Informationen zur Verwendung der Oracle-Datenbänke zur Überwachung wurden hinzugefügt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2 Erste Schritte

2.1 Informationen zu diesem Handbuch

Dieses Handbuch enthält Informationen und Verfahren zur Implementierung und Konfiguration von SAP BusinessObjects Business Intelligence (der "BI-Plattform"). Gängige Abläufe werden in schrittweisen Anleitungen beschrieben. Diese werden durch ausführliche Hintergrundinformationen und technische Erläuterungen zu komplexeren Themenbereichen und Fragestellungen ergänzt.

Informationen zur Installation dieses Produkts finden Sie im *Installationshandbuch für SAP BusinessObjects Business Intelligence*.

2.1.1 An welchen Benutzerkreis richtet sich dieses Handbuch?

In diesem Handbuch wird die Implementierung und Konfiguration der BI-Plattform beschrieben. Lesen Sie dieses Handbuch, wenn Sie für eine der folgenden Aufgaben verantwortlich sind:

- Planen der ersten Implementierung
- Konfigurieren der ersten Implementierung
- Umfangreiche Änderungen an der Architektur vorhandener Implementierungen
- Optimieren der Systemleistung

Dieses Handbuch richtet sich an Systemadministratoren, die mit der Konfiguration, Verwaltung und Wartung einer BI-Plattform-Installation betraut sind. Es ist vorteilhaft, wenn Sie mit Ihrem Betriebssystem und Ihrer Netzwerkumgebung vertraut sind und über Kenntnisse in Bezug auf die Verwaltung der Webanwendungsserver und Scripting-Technologien verfügen. Um Administratoren mit einem unterschiedlichen Erfahrungshintergrund zu unterstützen, bietet dieses Handbuch jedoch detaillierte Hintergrundinformationen und Begriffserläuterungen, durch die sämtliche Verwaltungsaufgaben und -funktionen veranschaulicht werden.

2.1.2 Informationen zur Business-Intelligence-Plattform

Die Business-Intelligence-Plattform ist eine flexible und skalierbare Lösung, mit der Endbenutzern Informationen in verschiedenen Formaten, z. B. als Dashboards und interaktive Berichte oder über eine beliebige Webanwendung, im Intranet, Extranet, Internet oder in einem Unternehmensportal zur Verfügung gestellt werden können.

Als integriertes Paket für die Berichterstellung, Analyse und Bereitstellung von Informationen stellt die Plattform eine Lösung für erhöhte Endbenutzerproduktivität und reduzierten Verwaltungsaufwand dar. Die Plattform, ob sie zur Verteilung wöchentlicher Umsatzberichte, zur Erstellung individueller Serviceangebote für den Kunden oder zur Integration wichtiger Informationen in Unternehmensportale genutzt wird, schafft spürbare Vorteile innerhalb des Unternehmens und darüber hinaus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2.1.3 Variablen

In diesem Handbuch werden die folgenden Variablen verwendet.

Variable	Beschreibung
<INSTALLDIR>	Das Installationsverzeichnis der BI-Plattform. Unter Windows lautet das Standardverzeichnis `C:\Programme (x86)\SAP BusinessObjects\`.
<PLATTFORM64VERZ>	Der Name Ihres Unix-Betriebssystems. Die folgenden Werte sind zulässig: • aix_rs6000_64 • linux_x64 • solaris_sparcv9 • hpux_ia64
<SKRIPTVERZ>	Das Verzeichnis, in dem Skripts zur Verwaltung der BI-Plattform gespeichert sind. Unter Windows lautet das Verzeichnis **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`. Unter Unix lautet das Verzeichnis **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/`**<PLATFORM64VERZ>**`/scripts`.

2.1.4 Terminologie

In der BI-Plattform-Dokumentation werden die folgenden Begriffe verwendet.

Begriff	Definition
Addon-Produkte	Produkte, die mit der BI-Plattform arbeiten, jedoch über ein eigenes Installationsprogramm verfügen, beispielsweise SAP BusinessObjects Explorer
Audit-Datenspeicher (ADS)	Die zum Speichern von Audit-Daten verwendete Datenbank
BI-Plattform	Eine Abkürzung für die Plattform SAP BusinessObjects Business Intelligence
Gebündelte Datenbank; gebündelter Webanwendungsserver	Die Datenbank oder der Webanwendungsserver, die bzw. der mit der BI-Plattform ausgeliefert wird

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Begriff	Definition
Cluster	Zwei oder mehr CMS-Server (Central Management Server), die gemeinsam eine CMS-Systemdatenbank verwenden
Clustern	Erstellen von Vorlagen So erstellen Sie z.B. ein Cluster: 1. Installieren Sie einen CMS und eine CMS-Datenbank auf dem Rechner. 2. Installieren Sie einen CMS auf Rechner B. 3. Lassen Sie den CMS auf Rechner B auf die Datenbank auf Rechner A zeigen.
Cluster-Schlüssel	Wird zum Dechiffrieren der Schlüssel in der CMS-Datenbank verwendet Sie können den Clusterschlüssel im CCM ändern; dieser Schlüssel kann jedoch nicht so zurückgesetzt werden wie ein Kennwort. Er enthält verschlüsselten Inhalt und darf auf keinen Fall verloren gehen.
CMS	Eine Abkürzung für den Central Management Server
CMS-Datenbank	Die vom CMS zum Speichern von Informationen über die BI-Plattform verwendete Datenbank
Implementierung	Die auf einem oder mehreren Rechnern installierte, konfigurierte und ausgeführte BI-Plattform-Software
Installation	Eine Instanz von BI-Plattform-Dateien, die vom Installationsprogramm auf einem Rechner erstellt wird
Rechner	Der Computer, auf dem die BI-Plattform-Software installiert ist
Hauptrelease	Ein vollständiges Release der Software, z. B. 4.0
Migration	Der Prozess der Übertragung von BI-Plattform-Inhalten aus einem vorherigen Hauptrelease (zum Beispiel aus XI 3.1) mithilfe des Upgrade-Management-Tools. Dieser Begriff gilt nicht für Implementierungen mit demselben Hauptrelease. Siehe *Hochstufung*.
Nebenrelease	Ein Release einiger Komponenten der Software, z. B. 4.1.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Begriff	Definition
Knoten	Eine Gruppe von BI-Plattform-Servern, die auf demselben Rechner ausgeführt und von demselben Server Intelligence Agent (SIA) verwaltet werden
Patch	Kleines Update für eine bestimmte Support-Package-Version
Hochstufung	Prozess der Übertragung von BI-Plattform-Inhalten zwischen Implementierungen mit demselben Hauptrelease (beispielsweise 4.0 zu 4.0) anhand der Hochstufverwaltung
Server	Ein BI-Plattform-Prozess. Ein Server hostet mindestens einen Dienst.
Server Intelligence Agent (SIA)	Prozess, der eine Gruppe von Servern verwaltet, dazu zählen das Anhalten, Starten und Neustarten von Servern
Support Package	Softwareupdate für ein Neben- oder Hauptrelease
Webanwendungsserver	Server, der dynamischen Content verarbeitet. Beispielsweise ist Tomcat 7 der gebündelte Webanwendungsserver für 4.1.
Upgrade	Die Planungs-, Vorbereitungs-, Migrations- und Nachbereitungsprozesse, die zum Durchführen eines Migrationsprozesses erforderlich sind

2.2 Vor dem Beginn

2.2.1 Grundlegende Begriffe

2.2.1.1 Server Intelligence

Server Intelligence ist eine zentrale Komponente der BI-Plattform. In der Central Management Console (CMC) angewendete Änderungen an Serverprozessen werden vom Central Management Server (CMS) an die entsprechenden Serverobjekte übergeben. Der Server Intelligence Agent (SIA) wird verwendet, um Server automatisch neu zu starten oder herunterzufahren, wenn eine unerwartete Bedingung eintritt. Außerdem greift der Administrator zum Verwalten von Knoten auf ihn zu.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Der CMS archiviert Informationen zu Servern in der CMS-Systemdatenbank, sodass Sie problemlos Standardservereinstellungen wiederherstellen können. Da der SIA regelmäßig Abfragen an den CMS sendet, um Informationen zu den von ihm verwalteten Servern anzufordern, weiß der SIA, welchen Status Server aufweisen sollten und wann Maßnahmen zu ergreifen sind.

> **Hinweis**
>
> Eine BI-Plattform-Installation ist eine eindeutige Instanz der BI-Plattform-Dateien, die vom Installationsprogramm auf einem Rechner erstellt werden. Eine Instanz einer BI-Plattform-Installation kann nur innerhalb eines einzigen Clusters verwendet werden. Knoten, die zu verschiedenen Clustern derselben BI-Plattform-Installation gehören, werden nicht unterstützt, da diese Art der Implementierung nicht gepatcht oder aktualisiert werden kann. Nur Unix-Plattformen unterstützen mehrere Installationen der Software auf demselben Rechner, und zwar nur dann, wenn jede Installation unter einem eindeutigen Benutzerkonto ausgeführt und in einem separaten Ordner installiert wird, so dass die Installationen keine Dateien gemeinsam nutzen. Beachten Sie, dass alle Rechner im Cluster dieselbe Version und denselben Patch-Level aufweisen müssen.

Weitere Informationen

Server, Hosts und Cluster [Seite 36]

2.2.1.2 Server, Dienste, Knoten und Hosts

Die BI-Plattform verwendet die Begriffe Server und Dienst zur Bezeichnung von zwei Softwarevarianten, die auf einem BI-Plattform-Computer ausgeführt werden.

Als “Server” wird ein Prozess auf Betriebssystemebene bezeichnet (auf manchen Systemen wird dies Daemon) genannt), auf dem ein oder mehrere Dienste gehostet werden. Der Central Management Server (CMS) und der Adaptive Processing Server sind beispielsweise Server. Ein Server wird unter einem bestimmten Betriebssystemkonto ausgeführt und verfügt über eine eigene Prozess-ID (PID).

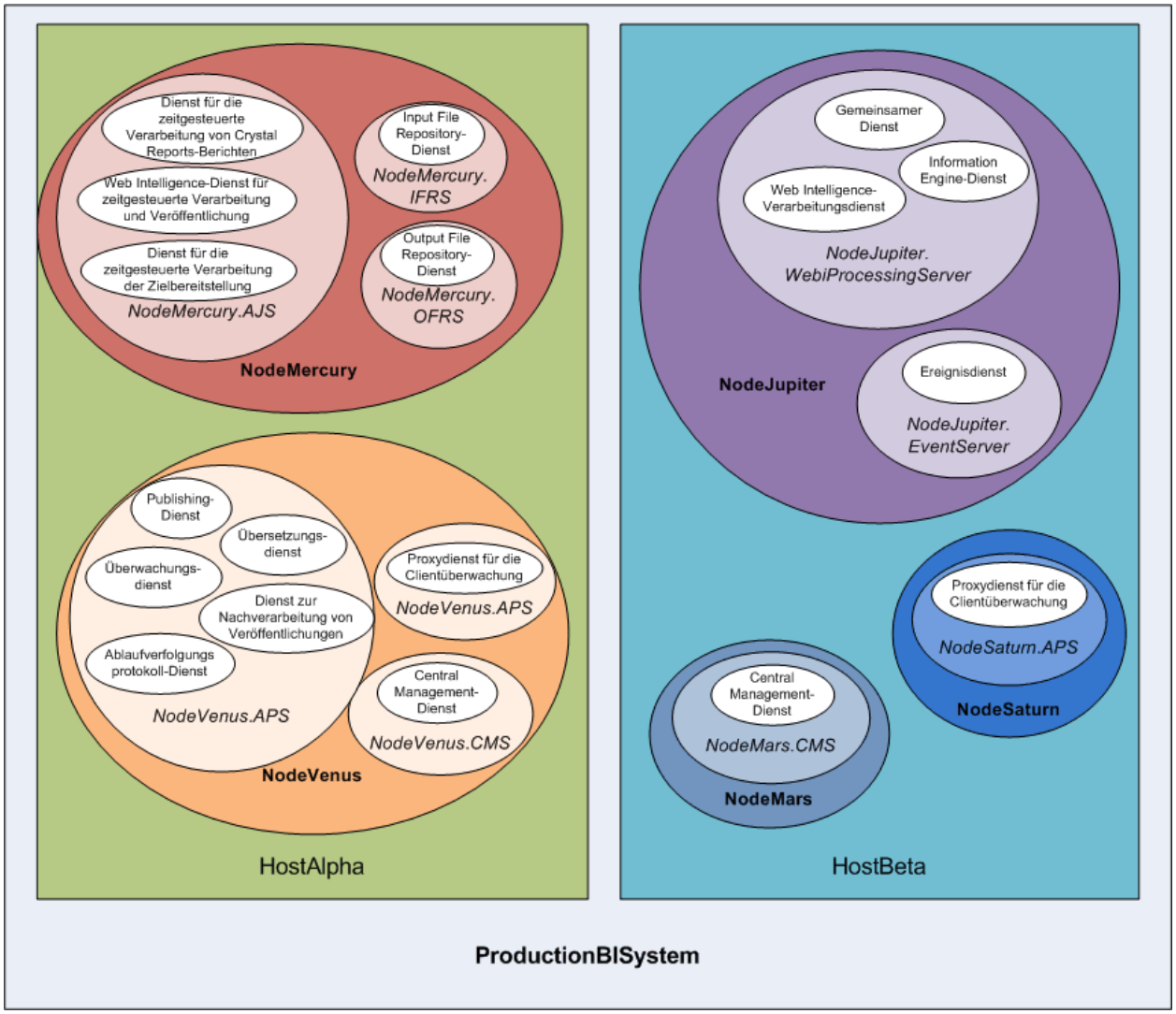
Ein Dienst ist ein Server-Untersystem, das eine bestimmte Funktion ausführt. Der Dienst wird im Speicherbereich des zugehörigen Servers und unter der Prozess-ID des übergeordneten Containers (Servers) ausgeführt. Der Dienst zur zeitgesteuerten Verarbeitung von Web Intelligence ist beispielsweise ein Untersystem, das innerhalb des Adaptive Job Server ausgeführt wird.

Ein Knoten entspricht einer Gruppe von BI-Plattform-Servern, die auf demselben Host ausgeführt und von einem einzelnen Server Intelligence Agent (SIA) verwaltet werden. Auf einem einzelnen Host können sich ein oder mehrere Knoten befinden.

Die BI-Plattform kann auf einem Einzelrechner installiert, über verschiedene Computer in einem Intranet verteilt oder in einem Wide Area Network (WAN) installiert werden.

Das folgende Diagramm zeigt eine hypothetische Installation der BI-Plattform an. Die Anzahl an Hosts, Knoten, Servern und Diensten – sowie die Server- und Diensttypen – weichen in echten Installationen davon ab.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.



Zwei Hosts bilden ein Cluster mit der Bezeichnung ProductionBISystem:

- Auf dem Host mit der Bezeichnung HostAlpha ist die BI-Plattform installiert und für zwei Knoten konfiguriert:
  - NodeMercury enthält einen Adaptive Job Server (`NodeMercury.AJS`) mit Diensten zum zeitgesteuerten Verarbeiten und Veröffentlichen von Berichten, einen Input File Repository Server (`NodeMercury.IFRS`) mit einem Dienst zum Speichern von Eingabeberichten sowie einen Output File Repository Server (`NodeMercury.OFRS`) mit einem Dienst zum Speichern der Berichtsausgabe.
  - NodeVenus enthält einen Adaptive Processing Server (`NodeVenus.APS`) mit Diensten zur Bereitstellung von Veröffentlichungs-, Überwachungs- und Übersetzungsfunktionen, einen Adaptive Processing Server (`NodeVenus.APS2`) mit einem Dienst für das Client-Auditing und einen Central Management Server (`NodeVenus.CMS`) mit einem Dienst zur Bereitstellung der CMS-Dienste.
- Auf dem Host mit der Bezeichnung HostBeta ist die BI-Plattform installiert und für drei Knoten konfiguriert:
  - NodeMars enthält einen Central Management Server (`NodeMars.CMS`) mit einem Dienst zur Bereitstellung der CMS-Dienste. Da der CMS auf zwei Rechnern installiert ist, stehen Lastausgleich, Abwehr- und Failover-Fähigkeiten zur Verfügung.
  - NodeJupiter: enthält einen Web Intelligence Processing Server (`NodeJupiter.Web Intelligence`) mit einem Dienst zur Bereitstellung von Web-Intelligence-Berichterstellungsfunktionen und einen Event

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Server (`NodeJupiter.EventServer`) zur Bereitstellung von Funktionen zur Überwachung von Berichten.
  - NodeSaturn enthält einen Adaptive Processing Server (`NodeSaturn.APS`) mit einem Dienst zur Bereitstellung von Client-Audits.

2.2.2 Schlüsselprogramme für die Verwaltung

2.2.2.1 Systemkonfigurationsassistent

Der Systemkonfigurationsassistent ist ein Tool, mit dem Sie Ihre BI-Plattform-Implementierung einfach und schnell konfigurieren können. Der Assistent führt Sie durch die grundlegenden Konfigurationsoptionen, wodurch eine funktionierende Implementierung entsteht, in der allgemeine Einstellungen wie diese verwendet werden:

- Welche Produktserver automatisch mit der BI-Plattform gestartet werden sollen
- Optimierung der Implementierung für maximale Leistung oder für eingeschränkte Hardware-Ressourcen
- Speicherorte der Systemordner

Der Assistent ist standardmäßig so eingestellt, dass er automatisch ausgeführt wird, wenn Sie sich an der Central Management Console (CMC) anmelden, Sie können diese Einstellung jedoch im Assistenten ändern. Sie können den Assistenten auch jederzeit aus dem Bereich *Verwalten* in der CMC starten.

> **Hinweis**
>
> In Produktivsystemen sollte der Assistent besser nicht auf die automatische Ausführung eingestellt werden, um ein versehentliches Neukonfigurieren zu vermeiden.

> **Hinweis**
>
> Es wird empfohlen, eine vollständige Sicherungskopie zu erstellen, bevor mithilfe des Assistenten Änderungen am System vorgenommen werden.

2.2.2.2 Central Management Console (CMC)

Die Central Management Console (CMC) ist ein webbasiertes Tool, mit dem Sie administrative Aufgaben (z.B. Benutzer-, Inhalt- und Serververwaltung) ausführen und Sicherheitseinstellungen konfigurieren können. Da es sich bei der CMC um eine webbasierte Anwendung handelt, können Sie alle administrativen Aufgaben in einem Webbrowser auf jedem Computer ausführen, der eine Verbindung mit dem Webanwendungsserver herstellen kann.

Verwaltungseinstellungen können nur von Mitgliedern der Gruppe "Administratoren" geändert werden, es sei denn, anderen Benutzern werden diese Rechte explizit gewährt. In der CMC können Rollen zugewiesen werden, um Benutzerrechte für die Ausführung kleinerer administrativer Aufgaben zu gewähren, z.B. Verwalten der Benutzer in Ihrer Gruppe oder Verwalten von Berichten in Ordnern, die Ihrem Team gehören.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2.2.2.3 Central Configuration Manager (CCM)

Der Central Configuration Manager (CCM) ist ein Tool für die Fehlerbehebung auf Servern und die Knotenverwaltung, das in zwei Varianten bereitgestellt wird. In einer Microsoft Windows-Umgebung können Sie mit dem CCM lokale Server und Remoteserver über die grafische Benutzeroberfläche oder über eine Befehlszeile verwalten. In einer UNIX-Umgebung können Sie mit dem CCM-Shell-Skript (`ccm.sh`) Server über eine Befehlszeile verwalten.

Sie können mit dem CCM Knoten erstellen und konfigurieren und den Webanwendungsserver starten oder stoppen, sofern es sich um den gebündelten, standardmäßigen Tomcat-Webanwendungsserver handelt. Unter Windows ermöglicht er Ihnen auch die Konfiguration von Netzwerkparametern, z.B. der SSL-Verschlüsselung (Secure Socket Layer). Diese Parameter gelten für alle Server innerhalb eines Knotens.

> **Hinweis**
>
> Die meisten Serververwaltungsaufgaben werden nun über die CMC und nicht im CCM ausgeführt. Ab sofort wird der CCM für die Fehlerbehebung und die Knotenkonfiguration verwendet.

2.2.2.4 Repository Diagnostic Tool

Mit dem Repository Diagnostic Tool (RDT) können Sie Inkonsistenzen zwischen der CMS-Systemdatenbank und dem FRS-Dateispeicher (File Repository Server) suchen, diagnostizieren und reparieren. Der Benutzer kann einen Grenzwert für die Anzahl der Fehler festlegen, die das RDT vor Ende der Ausführung findet und repariert.

Das RDT sollte nach der Wiederherstellung Ihres BI-Plattform-Systems verwendet werden.

> **Hinweis**
>
> In Produktivsystemen sollte das RDT regelmäßig ausgeführt werden, um eventuelle Systemprobleme aufzudecken, wobei jedoch die Option “Reparieren” zu deaktivieren ist. Führen Sie das RDT nur dann mit der aktivierten Reparaturoption aus, wenn Sie sicher sind, dass das RDT Reparaturen am System ausführen soll.

2.2.2.5 Upgrade-Management-Tool

Das Upgrade-Management-Tool (früher eine Funktion des Import-Assistenten) wird als Teil der BI-Plattform installiert und führt Administratoren durch den Prozess des Imports von Benutzern, Gruppen und Ordnern aus früheren Versionen der BI-Plattform. Außerdem können mit dem Tool Ereignisse, Servergruppen, Repository-Objekte und Kalender importiert und aktualisiert werden.

Informationen über das Upgrade von einer früheren Version der BI-Plattform finden Sie im *Aktualisierungshandbuch für SAP BusinessObjects Business Intelligence*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2.2.3 Schlüsselaufgaben

Je nach Situation können Sie sich auf bestimmte Abschnitte dieses Handbuchs konzentrieren. Außerdem stehen Ihnen für eine solche Recherche u. U. weitere Ressourcen zur Verfügung. Für jede der folgenden Situationen gibt es eine Liste, in der Aufgaben- und Themenvorschläge aufgeführt sind.

Weitere Informationen

Planen oder Ausführen der ersten Implementierung [Seite 29]
Konfigurieren der Implementierung [Seite 30]
Optimieren der Systemleistung [Seite 30]
Central Management Console (CMC) [Seite 27]

2.2.3.1 Planen oder Ausführen der ersten Implementierung

Bei der Planung und Durchführung Ihrer ersten Implementierung der BI-Plattform sollten Sie die folgenden Abschnitte in diesem Handbuch lesen:

- Um sich mit den BI-Plattform-Komponenten vertraut zu machen, lesen Sie “Architekturübersicht”.
- “Erläuterung der Kommunikation zwischen BI-Plattform-Komponenten”.
- “Überblick zum Thema Sicherheit”
- Falls Sie Drittherstellerauthentifizierung verwenden möchten, lesen Sie “Authentifizierungsoptionen in der BI-Plattform”
- Lesen Sie nach der Installation “Arbeiten mit dem Verwaltungsbereich "Server" in der CMC”

Weitere Informationen zur Installation der BI-Plattform finden Sie im *Installationshandbuch für SAP BusinessObjects Business Intelligence*. Um Ihre Anforderungen zu beurteilen und eine Implementierungsarchitektur zu gestalten, die optimal für Ihre Anforderungen geeignet ist, lesen Sie das *Planungshandbuch zur Implementierung von SAP BusinessObjects Business Intelligence*.

Weitere Informationen

Überblick über die Architektur [Seite 32]
Kommunikation zwischen BI-Plattform-Komponenten [Seite 186]
Überblick zum Thema Sicherheit [Seite 153]
Authentifizierungsoptionen in der BI-Plattform [Seite 220]
Arbeiten mit dem Verwaltungsbereich "Server" in der CMC [Seite 365]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2.2.3.2 Konfigurieren der Implementierung

Wenn Sie die Installation der BI-Plattform gerade abgeschlossen haben und erste Konfigurationsaufgaben wie Firewall-Konfiguration und Benutzerverwaltung ausführen möchten, sollten Sie die folgenden Abschnitte lesen:

Weitere Informationen

Einführung in den Systemkonfigurationsassistenten [Seite 87]
Kommunikation zwischen BI-Plattform-Komponenten [Seite 186]
Überblick zum Thema Sicherheit [Seite 153]
Informationen zur Überwachung [Seite 666]

2.2.3.3 Optimieren der Systemleistung

Zur Bewertung und Anpassung der Effizienz Ihrer Implementierung, um Ressourcen zu maximieren, lesen Sie die folgenden Abschnitte:

- Wenn Sie eine Implementierungsvorlage zur Konfiguration Ihres Systems verwenden möchten, lesen Sie den Abschnitt “Einführung in den Systemkonfigurationsassistenten”.
- Wenn Sie eine Systemüberwachung für Ihr vorhandenes System einrichten möchten, lesen Sie den Abschnitt “Überwachung”.
- Informationen zu täglichen Wartungsarbeiten und Vorgehensweisen bei der Arbeit mit Servern in der CMC finden Sie im Abschnitt “Arbeiten mit dem Verwaltungsbereich "Server" in der CMC”.

Weitere Informationen

Einführung in den Systemkonfigurationsassistenten [Seite 87]
Informationen zur Überwachung [Seite 666]
Arbeiten mit dem Verwaltungsbereich "Server" in der CMC [Seite 365]

2.2.3.4 Arbeiten mit Objekten in der CMC

Objekte sind Dokumente und Dateien, die in der BI-Plattform oder in einer anderen Software erstellt und dann im BI-Plattform-Repository gespeichert und verwaltet werden. Wenn Sie mit Objekten in der CMC arbeiten, sollten Sie die folgenden Abschnitte lesen:

- Informationen über das Einrichten von Benutzern und Gruppen in der CMC finden Sie unter “Übersicht über die Kontoverwaltung”.
- Informationen zum Einstellen der Sicherheit für Objekte finden Sie unter “Funktionsweise von Rechten in der BI-Plattform”.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Allgemeine Informationen zum Arbeiten mit Objekten finden Sie im *Benutzerhandbuch für SAP BusinessObjects Business Intelligence*.

Weitere Informationen

Übersicht über die Kontoverwaltung [Seite 100]
Funktionsweise von Rechten in der BI-Plattform [Seite 124]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3 Architektur

3.1 Überblick über die Architektur

In diesem Abschnitt werden die gesamte Plattformarchitektur sowie System- und Dienstkomponenten erläutert, aus denen sich SAP BusinessObjects Business Intelligence zusammensetzt. Die Informationen sollen Administratoren helfen, die Grundlagen des Systems zu verstehen und einen Plan für die Implementierung, Verwaltung und Wartung des Systems zu entwickeln.

> **Hinweis**
>
> Eine Liste der unterstützten Plattformen, Sprachen, Datenbanken, Webanwendungsserver, Webserver und weiterer von diesem Release unterstützten Systeme finden Sie in der *Product Availability Matrix* (PAM) unter der Verknüpfung "Supported Platforms/PAR" auf dem SAP Support Portal: *http://service.sap.com/bosap-support*.

> **Hinweis**
>
> Da die PAM fortlaufend aktualisiert wird, rufen Sie immer die Online-Version der PAM ab, statt eine lokale Kopie zu verwenden.

Die Business-Intelligence-Plattform (BI) ist für hohe Leistung über ein breites Spektrum von Benutzer- und Implementierungsszenarios hinweg ausgelegt. Sie können prozessorintensive Zeitsteuerungs- und Verarbeitungsaufgaben verlagern, indem Sie dedizierte Server zum Hosten von spezifischen Diensten erstellen. Die Architektur ist so konzipiert, dass sie die Anforderungen praktisch jeder BI-Implementierung erfüllt und flexibel mitwächst – von einigen Benutzern mit einem Tool bis hin zu Tausenden Benutzern mit mehreren Tools und Benutzeroberflächen.

Entwickler können die BI-Plattform in andere Technologiesysteme ihres Unternehmens über Webdienste oder APIs (Application Programming Interfaces) für Java und .NET integrieren.

Endbenutzer können unter anderem über die folgenden spezialisierten Tools und Anwendungen auf Berichte zugreifen sowie Berichte erstellen, bearbeiten und mit ihnen interagieren:

- Vom Installationsprogramm der Clienttools der BI-Plattform installierte Clients:
  - Web-Intelligence-Rich-Client
  - Business View Manager
  - Berichtskonvertierungstool
  - Universe-Design-Tool
  - Query as a Web Service
  - Information-Design-Tool (früher Information Designer)
  - Übersetzungsmanagement-Tool (früher Übersetzungsmanager)
  - Widgets (früher BI Widgets)
- Separat erhältliche Clients:
  - SAP Crystal Reports
  - SAP BusinessObjects Dashboards (früher Xcelsius)
  - SAP BusinessObjects Analysis (früher Voyager)

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- BI-Arbeitsbereiche (früher Dashboard Builder)

IT-Abteilungen können Daten- und Systemverwaltungstools mit folgenden Komponenten verwenden:

- Berichtsviewer
- Central Management Console (CMC)
- Central Configuration Manager (CCM)
- Repository Diagnostic Tool (RDT)
- Datenföderations-Administrationstool
- Upgrade-Management-Tool (früher eine Funktion des Import-Assistenten)
- Universe-Design-Tool (früher Universe Designer)
- SAP BusinessObjects Mobile

Um für Flexibilität, Zuverlässigkeit und Skalierbarkeit zu sorgen, können BI-Plattform-Komponenten auf einem oder über mehrere Rechner verteilt installiert werden. In gewissen Fällen können Sie sogar zwei verschiedene Versionen der BI-Plattform gleichzeitig auf demselben Computer installieren. Diese Konfiguration wird jedoch nur im Rahmen des Upgrade-Prozesses oder zu Testzwecken empfohlen.

Serverprozesse können aus Kostenersparnisgründen vertikal skaliert werden (wobei auf einem Computer mehrere oder alle serverseitigen Prozesse ausgeführt werden), oder sie können zur Leistungssteigerung horizontal skaliert werden (wobei Serverprozesse auf zwei oder mehr Netzwerkrechner verteilt werden). Es können auch mehrere redundante Versionen desselben Serverprozesses auf mehr als einem Rechner ausgeführt werden, so dass die Verarbeitung fortgesetzt werden kann, wenn beim Primärprozess Probleme auftreten.

Hinweis

Es kann zwar eine Kombination aus Windows- und Unix-Plattformen verwendet werden, von der Verwendung unterschiedlicher Betriebssysteme für CMS-Prozesse wird jedoch abgeraten.

3.1.1 Komponentendiagramm

SAP BusinessObjects Business Intelligence ist eine BI-Plattform (Business Intelligence), die Analyse- und Berichterstellungstools auf Unternehmensebene zur Verfügung stellt, um so die Bereitstellung von Informationen zu vereinfachen. Daten können aus einer Vielzahl unterstützter Datenbanksysteme analysiert werden (einschließlich Text- oder mehrdimensionalen OLAP-Systemen), und BI-Berichte können in vielen verschiedenen Formaten in zahlreichen Publikationssystemen veröffentlicht werden.

Im Architekturdiagramm im SAP Community Network werden die Komponenten der BI-Plattform, wie Server und Clienttools, sowie zusätzliche Analyseprodukte, Webanwendungskomponenten und Datenbanken veranschaulicht, die Bestandteil einer BI-Plattform-Landschaft sein können: *http://scn.sap.com/docs/DOC-43663*.

Die BI-Plattform stellt Berichte über eine schreibgeschützte Verbindung mit den Datenbanken Ihres Unternehmens zur Verfügung und verwendet eigene Datenbanken, in denen seine Konfigurations-, Überwachungs- und andere operative Daten gespeichert werden. Die vom System erstellten BI-Berichte können an eine Vielzahl von Zielen, z.B. Dateisysteme und E-Mail, gesendet oder über Websites oder Portale aufgerufen werden.

Die BI-Plattform ist ein eigenständiges System, das auf einem Einzelrechner (z.B. einer kleinen Entwicklungs- oder Testumgebung im Vorfeld der Produktion) installiert oder auf einem Cluster von zahlreichen Rechnern, auf

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

denen unterschiedliche Komponenten ausgeführt werden (z.B. als umfangreiche Produktionsumgebung), verteilt werden kann.

3.1.2 Architekturschichten

SAP BusinessObjects Business Intelligence kann als eine Reihe von theoretischen Schichten verstanden werden:

Clientschicht

Die Clientschicht enthält alle Desktop-Clientanwendungen, die mit der BI-Plattform interagieren, um eine Vielzahl von Berichts-, Analyse- und Verwaltungsfunktionen bereitzustellen. Beispiele sind der Central Configuration Manager (BI-Plattform-Installationsprogramm), das Information-Design-Tool (Installationsprogramm für BI-Plattform-Clienttools) und SAP Crystal Reports (getrennt verfügbar und installiert).

Webschicht

Die Webschicht enthält Webanwendungen, die auf einem Java-Webanwendungsserver implementiert wurden. Webanwendungen bieten Endbenutzern über einen Webbrowser BI-Plattform-Funktionalität. Beispiele von Webanwendungen sind die administrative Webschnittstelle Central Management Console (CMC) und BI-Launchpad.

Außerdem enthält die Webschicht Webdienste. Webdienste bieten Softwaretools BI-Plattform-Funktionalität über den Webanwendungsserver, beispielsweise Sitzungsauthentifizierung, Verwaltung von Benutzerrechten, zeitgesteuerte Verarbeitung, Suchen, Administration, Berichterstellung und Abfragemanagement. Beispielsweise ist Live Office ein Produkt, das mit Webdiensten das BI-Plattform-Reporting in Microsoft Office-Produkte integriert.

Verwaltungsschicht

Die Verwaltungsschicht (auch Intelligence-Schicht genannt) koordiniert und steuert alle Komponenten, aus denen sich die BI-Plattform zusammensetzt. Sie besteht aus dem Central Management Server (CMS) und dem Event Server sowie zugehörigen Diensten. Der CMS enthält Sicherheits- und Konfigurationsinformationen, leitet Dienstanforderungen an Server weiter, verwaltet die Überwachung und pflegt die CMS-Systemdatenbank. Der Event Server verwaltet dateibasierte Ereignisse, die in einer definierten Speicherschicht auftreten.

Speicherschicht

Die Speicherschicht ist für die Verwaltung von Dateien, z.B. Dokumente und Berichte, zuständig.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Der Input File Repository-Server verwaltet Dateien, die Daten für Berichte enthalten. Diese Dateien können beispielsweise von folgenden Dateitypen sein: `.rpt`, `.car`, `.exe`, `.bat`, `.js`, `.xls`, `.doc`, `.ppt`, `.rtf`, `.txt`, `.pdf`, `.wid`, `.rep`, `.unv`, `.unx`.

> **Hinweis**
>
> Die Größe des Dateispeichers des Input File Repository-Servers wird nicht durch das System verwaltet. Stattdessen sollte ein Administrator die Monitoring- und Wartungsplanung übernehmen.

Der Output File Repository-Server verwaltet vom System erstellte Berichte wie die folgenden Dateitypen: `.rpt`, `.csv`, `.xls`, `.doc`, `.rtf`, `.txt`, `.pdf`, `.wid`, `.rep`.

Die Speicherschicht übernimmt außerdem das Berichtscaching, um Systemressourcen zu sparen, wenn Benutzer auf Berichte zugreifen.

Verarbeitungsschicht

Die Verarbeitungsschicht analysiert Daten und erzeugt Berichte und andere Ausgabearten. Dies ist die einzige Schicht, die auf die Datenbanken zugreift, die Berichtsdaten enthalten. Diese Schicht besteht aus dem Adaptive Job Server, Connection Server (32- und 64-Bit-Versionen) und Verarbeitungsservern wie dem Adaptive Processing Server oder Crystal Reports Processing Server.

Datenschicht

Die Datenschicht besteht aus den Datenbankservern, die die CMS-Systemdatenbank und den Audit-Datenspeicher hosten. Außerdem besteht sie aus jeglichen Datenbankservern, die relationale, OLAP- oder andere Datentypen für Berichterstellungs- und Analyseanwendungen enthalten.

3.1.3 Datenbanken

Die BI-Plattform verwendet mehrere unterschiedliche Datenbanken.

- Reporting-Datenbank

  Dies bezieht sich auf die Daten Ihres Unternehmens. Es handelt sich um die Quelldaten, die von Produkten der SAP BusinessObjects Business Intelligence Suite analysiert und in Berichten erfasst werden. Meist sind diese Daten in einer relationalen Datenbank gespeichert, sie können aber auch in Textdateien, Microsoft Office-Dokumenten oder OLAP-Systemen vorliegen.
- CMS-Systemdatenbank

  In der CMS-Systemdatenbank werden BI-Plattform-Informationen gespeichert, zum Beispiel zu Benutzern, Servern, Ordnern, Dokumenten, Konfigurationen und Authentifizierungen. Sie wird vom Central Management Server (CMS) verwaltet und manchmal als *System-Repository* bezeichnet.
- Audit-Datenspeicher

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Im Audit-Datenspeicher werden Informationen zu verfolgbaren Ereignissen gespeichert, die in der BI-Plattform auftreten. Anhand dieser Informationen können Sie die Nutzung von Systemkomponenten, die Benutzeraktivität oder andere Aspekte des täglichen Betriebs überwachen.

- Lifecycle-Management-Datenbank

  Mit der Lifecycle-Management-Datenbank werden Konfigurations- und Versionsinformationen in Zusammenhang mit einer BI-Plattform-Installation sowie Aktualisierungen verfolgt.

- Überwachungsdatenbank

  Die Überwachung speichert mit der Java Derby-Datenbank Systemkonfigurations- und Komponenteninformationen für die SAP-Unterstützbarkeit.

Wenn Sie nicht über einen Datenbankserver zur Verwendung mit der CMS-System- und der Audit-Datenspeicherdatenbank verfügen, kann ein Server vom BI-Plattform-Installationsprogramm installiert und konfiguriert werden. Es empfiehlt sich, die Unternehmensanforderungen auf Basis der Informationen des Datenbankserverproviders zu bewerten. So können Sie feststellen, welche der unterstützten Datenbanken die Anforderungen am besten erfüllt.

> **Hinweis**
>
> Die Standard-SQL-Anywhere-Datenbank wird für Produktionssysteme nicht empfohlen.

3.1.4 Server, Hosts und Cluster

Die BI-Plattform besteht aus Servergruppen, die auf einem oder mehreren Hosts ausgeführt werden. Kleine Installationen (wie beispielsweise Test- oder Entwicklungssysteme) können einen einzelnen Host für einen Webanwendungsserver, einen Datenbankserver und sämtliche BI-Plattform-Server verwenden.

Mittlere und große Installationen können über Server verfügen, die auf mehreren Hosts ausgeführt werden. So kann ein Webanwendungsserver-Host in Kombination mit einem BI-Plattform-Serverhost verwendet werden. Dadurch werden Ressourcen auf dem BI-Plattform-Serverhost freigesetzt, sodass dieser mehr Informationen verarbeiten kann, als wenn er zusätzlich den Webanwendungsserver hostet.

Große Installationen können über mehrere BI-Plattform-Serverhosts verfügen, die in einem Cluster zusammenarbeiten. Wenn eine Organisation beispielsweise über eine große Anzahl an SAP-Crystal-Reports-Benutzern verfügt, können Crystal Reports Processing Server auf mehreren BI-Plattform-Serverhosts erstellt werden, um zu gewährleisten, dass ausreichend Ressourcen zur Verarbeitung von Clientanforderungen verfügbar sind.

Die Verwendung mehrerer Server bietet unter anderem folgende Vorteile:

- Optimierte Leistung

  Mehrere BI-Plattform-Serverhosts können eine Warteschlange von Reporting-Informationen schneller verarbeiten als ein einzelner BI-Plattform-Serverhost.

- Lastausgleich

  Wenn ein Server hoher Last ausgesetzt ist, verteilt der CMS neue Aufgaben automatisch an andere Server im Cluster.

- Höhere Verfügbarkeit

  Wenn auf einem Server ein unerwarteter Fehlerzustand eintritt, leitet der CMS die Aufträge automatisch an andere Server um, bis der Fehlerzustand korrigiert wurde.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3.1.5 Webanwendungsserver

Ein Webanwendungsserver fungiert als Übersetzungsschicht zwischen Webbrowsern oder Rich-Anwendungen und der BI-Plattform. Webanwendungsserver unter Windows, Unix und Linux werden unterstützt.

Eine ausführliche Liste der unterstützten Webanwendungsserver finden Sie im Dokument *Supported Platforms/PARs* unter *https://service.sap.com/bosap-support*.

Wenn kein Webanwendungsserver für den Einsatz mit der BI-Plattform vorhanden ist, kann das Installationsprogramm einen Tomcat-Webanwendungsserver für Sie installieren und konfigurieren. Es empfiehlt sich, die eigenen Anforderungen mit den Informationen von Ihrem Anbieter für Webanwendungsserver abzugleichen, um unter den unterstützten Webanwendungsservern den für Ihre Geschäftsanforderungen geeignetsten Server zu finden.

> **Hinweis**
>
> Wenn Sie eine Produktionsumgebung konfigurieren, wird empfohlen, den Webanwendungsserver auf einem separaten System zu hosten. Wenn die BI-Plattform und ein Webanwendungsserver in einer Produktionsumgebung auf demselben Host ausgeführt werden, können Leistungseinbußen nicht ausgeschlossen werden.

3.1.5.1 Web Application Container Server (WACS)

Zum Hosten von BI-Plattform-Webanwendungen ist ein Webanwendungsserver erforderlich.

Wenn Sie ein erfahrener Administrator von Java-Webanwendungsservern mit erweiterten Verwaltungsanforderungen sind, hosten Sie BI-Plattform-Webanwendungen mithilfe eines unterstützten Java-Webanwendungsservers. Wenn Sie zum Hosten der BI-Plattform ein unterstütztes Windows-Betriebssystem verwenden und einen einfachen Installationsprozess für den Webanwendungsserver bevorzugen oder nicht die zur Verwaltung eines Java-Webanwendungsservers benötigten Ressourcen besitzen, können Sie bei der Installation der BI-Plattform einen Web Application Container Server (WACS) installieren.

WACS ist ein BI-Plattform-Server, der die Ausführung von BI-Plattform-Webanwendungen, wie z.B. Central Management Console (CMC), BI-Launchpad und Webdiensten, ermöglicht, ohne dass vorher ein Java-Webanwendungsserver installiert werden muss.

Die Verwendung des WACS bietet eine Reihe von Vorteilen:

- Der WACS erfordert nur ein Minimum an Installations-, Wartungs- und Konfigurationsschritten. Er wird vom BI-Plattform-Installationsprogramm installiert und konfiguriert. Es sind keine weiteren Schritte erforderlich, um ihn verwenden zu können.
- Die Verwendung eines WACS setzt keine Kenntnisse in der Verwaltung und Wartung eines Java-Anwendungsservers voraus.
- Der WACS bietet eine Verwaltungsoberfläche, die mit der anderer BI-Plattform-Server übereinstimmt.
- Der WACS kann wie andere BI-Plattform-Server auf einem dedizierten Host installiert werden.

> **Hinweis**
>
> Wenn ein WACS anstelle eines dedizierten Java-Webanwendungsservers verwendet wird, sind einige Einschränkungen gegeben:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Der WACS ist nur auf unterstützten Windows-Betriebssystemen verfügbar.
- Benutzerdefinierte Webanwendungen können nicht auf dem WACS implementiert werden, da dieser nur die mit der BI-Plattform installierten Webanwendungen unterstützt.
- Der WACS kann nicht mit einem Apache-Lastausgleichsmodul eingesetzt werden.

Zusätzlich zum WACS kann ein dedizierter Webanwendungsserver verwendet werden. Der dedizierte Webanwendungsserver kann dann benutzerdefinierte Webanwendungen hosten, während die CMC und andere Webanwendungen der BI-Plattform vom WACS gehostet werden.

3.1.6 Software Development Kits

Mithilfe eines Software Development Kits (SDK) können Entwickler Elemente von SAP BusinessObjects Business Intelligence in unternehmenseigene Anwendungen und Systeme einbinden.

Die BI-Plattform bietet SDKs für die Softwareentwicklung auf Java- und .NET-Plattformen.

Hinweis

Die .NET-SDKs der BI-Plattform werden nicht standardmäßig installiert, sondern müssen von SAP Service Marketplace heruntergeladen werden.

Folgende SDKs werden von der BI-Plattform unterstützt:

- Java SDK und .NET SDK für die BI-Plattform

  Mit den SDKs der BI-Plattform können Anwendungen verschiedene Aufgaben ausführen, darunter die Authentifizierung, Sitzungsverwaltung, Arbeit mit Repository-Objekten, zeitgesteuerte Verarbeitung von Berichten, Berichtsveröffentlichung und Serververwaltung.

  Hinweis

  Verwenden Sie das Java SDK, um vollen Zugriff auf Sicherheits-, Serververwaltungs- und Auditingfunktionen zu erhalten.

- RESTful-Webdienste-SDK für die BI-Plattform

  Das RESTful-Webdienste-SDK für die BI-Plattform ermöglicht Ihnen den Zugriff auf die BI-Plattform über das HTTP-Protokoll. Mit diesem SDK können Sie sich bei der BI-Plattform anmelden, zum BI-Plattform-Repository navigieren, auf Ressourcen zugreifen und grundlegende Ressourcenplanung durchführen. Sie können auf dieses SDK zugreifen, indem Sie Anwendungen entwickeln, die eine beliebige Programmiersprache verwenden, die das HTTP-Protokoll unterstützt, oder indem Sie ein beliebiges Tool verwenden, das HTTP-Anforderungen unterstützt.
- Java Consumer SDK und .NET Consumer SDK für die BI-Plattform

  Eine Implementierung von SOAP-basierten Webdiensten, mit deren Hilfe Sie die Benutzerauthentifizierung und Sicherheit, den Zugriff auf Dokumente und Berichte, die zeitgesteuerte Verarbeitung, Veröffentlichungen und die Serververwaltung handhaben können.

  BI-Plattform-Webdienste verwenden Standards wie XML, SOAP, AXIS 2.0 und WSDL. Die Plattform erfüllt die Webdienstspezifikation WS-Interoperability Basic Profile 1.0.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Webdienstanwendungen werden derzeit nur mit den folgenden Konfigurationen für den Lastausgleich unterstützt:
>
> 1. Persistenz der Quell-IP-Adresse
> 2. Persistenz der Quell-IP und des Zielports (nur auf Cisco Content Services Switch verfügbar)
> 3. SSL-Persistenz
> 4. Cookie-basierte Sitzungspersistenz

> **Hinweis**
>
> Die SSL-Persistenz kann in einigen Webbrowsern zu Problemen in Bezug auf Sicherheit und Zuverlässigkeit führen. Wenden Sie sich an Ihren Netzwerkadministrator, um zu ermitteln, ob SSL-Persistenz für Ihr Unternehmen geeignet ist.

- Datenzugriffstreiber- und Verbindungs-Java-SDKs

  Mit diesen SDKs können Sie Datenbanktreiber für den Connection Server erstellen und Datenbankverbindungen verwalten.
- Semantic Layer Java SDK

  Mit dem Semantic Layer Java SDK können Sie eine Java-Anwendung entwickeln, die Administrations- und Sicherheitsaufgaben für Universen und Verbindungen ausführt. Sie können beispielsweise Dienste für die Veröffentlichung eines Universums auf einem Repository oder zum Abrufen einer gesicherten Verbindung von einem Repository in ihrem Arbeitsbereich implementieren. Diese Anwendung kann in BI-Plattform-Lösungen eingebettet werden, die die BI-Plattform als OEM integrieren.
- Report Application Server Java SDK und .NET SDK

  Dank der SDKs von Report Application Server können Anwendungen vorhandene Crystal-Reports-Berichte öffnen, erstellen und ändern. Dies umfasst unter anderem des Festlegen von Parameterwerten, das Ändern von Datenquellen und den Export in andere Formate wie XML, PDF, Microsoft Word und Microsoft Excel.
- Java- und .NET-Crystal-Reports-Viewer

  Mithilfe der Viewer können Anwendungen Crystal-Reports-Berichte anzeigen und exportieren. Folgende Viewer stehen zur Verfügung:

  - Viewer für DHTML-Berichtseiten: Stellt Daten dar und ermöglicht Drilldowns, Seitennavigation, Zoomen, Eingabeaufforderungen, Suchvorgänge, Hervorhebungen, Export und Druck.
  - Viewer für Berichtbestandteile: Bietet die Möglichkeit, einzelne Bestandteile eines Berichts wie Diagramme, Text und Felder anzuzeigen.
- Report Engine Java SDK und .NET SDK

  Die Report Engine-SDKs ermöglichen Anwendungen die Interaktion mit Berichten, die mit SAP BusinessObjects Web Intelligence erstellt wurden.

  Diese SDKs beinhalten Bibliotheken, mit deren Hilfe sich ein Designtool für Webberichte erstellen lässt. Die mit den SDKs erstellten Anwendungen können eine Vielzahl verschiedener Web-Intelligence-Dokumente anzeigen, erstellen oder ändern. Benutzer können Dokumente bearbeiten, indem sie Objekte wie Tabellen, Diagramme, Bedingungen und Filter hinzufügen, entfernen und ändern.
- Plattformsuche-SDK: Das Plattformsuche-SDK ist die Schnittstelle zwischen der Clientanwendung und dem Plattformsuchdienst. Die Plattformsuche unterstützt das Public SDK, das mit dem Plattformsuche-SDK ausgeliefert wird.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wenn ein Suchanfrageparameter über die Clientanwendung an die SDK-Schicht gesendet wird, konvertiert die SDK-Schicht den Anfrageparameter in ein XML-codiertes Format und übermittelt ihn an den Plattformsuchdienst.

Die SDKs können in Kombination verwendet werden, um Anwendungen mit einer breiten Palette an BI-Funktionen auszustatten. Weitere Informationen über diese SDKs, einschließlich Entwicklerhandbüchern und API-Referenzen, finden Sie unter *http://help.sap.com*.

3.1.7 Datenquellen

3.1.7.1 Universen

Ein Universum ist eine semantische Schicht, die eine Abstraktion von komplexen Daten bietet, indem statt einer Datensprache eine Geschäftssprache verwendet wird, um auf Daten zuzugreifen, sie zu bearbeiten und zu organisieren. Diese Geschäftssprache wird in Form von Objekten in einer Universumsdatei gespeichert. Web Intelligence, Crystal Reports und weitere Anwendungen verwenden Universen, um den Prozess der Benutzererstellung zu vereinfachen, der für einfache und komplexe Endbenutzerabfragen und -analysen erforderlich ist.

Universen sind eine zentrale Komponente der BI-Plattform. Alle Universumsobjekte und -verbindungen werden vom Connection Server im zentralen Repository gespeichert und gesichert. Kunden-Tools zum Entwickeln von Universen müssen sich bei der BI-Plattform anmelden, um auf das System zuzugreifen und Universen zu erstellen. Der Zugriff auf Universen und die Sicherheit auf Zeilen-/Spaltenebene können auch auf Ebene von Gruppen oder einzelnen Benutzern innerhalb der Entwurfsumgebung verwaltet werden.

Die semantische Ebene ist die Voraussetzung dafür, dass Web Intelligence Dokumente unter Verwendung mehrerer synchronisierter Datenprovider, einschließlich OLAP-Datenquellen (Online Analytical Processing) und CWM-Datenquellen (Common Warehousing Metamodel), bereitstellen kann.

3.1.7.2 Business Views

Business Views vereinfachen die Berichterstellung und Interaktion, indem die Komplexität von Daten für Berichtsentwickler abstrahiert wird. Business Views helfen, Datenverbindungen, Datenzugriff, Business Elements und Zugriffskontrolle zu trennen.

Business Views können nur von Crystal-Reports-Berichten verwendet werden und vereinfachen den Datenzugriff und die Sicherheit zur Ansichtszeit, die für die Erstellung von Crystal-Reports-Berichten erforderlich ist. Business Views unterstützen die Kombination mehrerer Datenquellen in einer einzelnen Ansicht. Business Views werden in der BI-Plattform vollständig unterstützt.

3.1.8 Authentifizierung und Einzelanmeldung

Die Systemsicherheit wird vom Central Management Server (CMS), von Sicherheits-Plugins und von Authentifizierungstools von Drittherstellern verwaltet, z.B. SiteMinder oder Kerberos. Diese Komponenten

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

steuern die Authentifizierung von Benutzern und den Benutzerzugriff auf die BI-Plattform sowie die zugehörigen Ordner und weitere Objekte.

Folgende Sicherheits-Plugins für die Einzelanmeldungs-Benutzerauthentifizierung stehen zur Verfügung:

- Enterprise (Standard), einschließlich Unterstützung für vertrauenswürdige Authentifizierung zur Verwendung mit Authentifizierungsmethoden wie SAML, X.509, SAP NW SSO und anderen, von Ihrem Anwendungsserver unterstützten Methoden.
- LDAP
- Windows Active Directory (AD)

Bei Verwendung eines ERP-Systems (Enterprise Resource Planning) werden Benutzer-Zugriffsberechtigungen auf das ERP-System über die Einzelanmeldung gesteuert, sodass Berichte die ERP-Daten nutzen können. Für ERP-Systeme werden folgende Einzelanmeldungs-Benutzerauthentifizierungsarten unterstützt:

- SAP ERP und Business Warehouse (BW)
- Oracle E-Business Suite (EBS)
- Siebel Enterprise
- JD Edwards Enterprise One
- PeopleSoft Enterprise

3.1.8.1 Sicherheits-Plugins

Sicherheits-Plugins automatisieren die Kontoerstellung und -verwaltung, da Sie Benutzerkonten und Gruppen aus Drittherstellersystemen der BI-Plattform zuweisen können. Sie können Benutzerkonten von Drittherstellern vorhandenen Enterprise-Benutzerkonten zuordnen oder neue Enterprise-Benutzerkonten erstellen, die jedem zugeordneten Eintrag im externen System entsprechen.

Die Sicherheits-Plugins verwalten die Benutzer- und Gruppenlisten des Drittherstellers dynamisch. Nachdem Sie eine LDAP-Gruppe (Lightweight Directory Access Protocol) oder AD-Gruppe (Windows Active Directory) der BI-Plattform zugeordnet haben, können sich alle Benutzer, die zu dieser Gruppe gehören, an der BI-Plattform anmelden. Nachfolgende Änderungen an Gruppenmitgliedschaften des Drittherstellerprodukts werden automatisch weitergegeben.

Die BI-Plattform unterstützt folgende Sicherheits-Plugins:

- Enterprise-Sicherheits-Plugin

  Der Central Management Server (CMS) verwaltet Sicherheitsdaten, z.B. Benutzerkonten, Gruppenmitgliedschaften und Objektrechte, die Benutzer- und Gruppenberechtigungen definieren. Dies wird als Enterprise-Authentifizierung bezeichnet.

  Die Enterprise-Authentifizierung ist immer aktiviert und kann nicht deaktiviert werden. Verwenden Sie die vom System vorgegebene Enterprise-Authentifizierung, wenn Sie für die Verwendung mit der BI-Plattform eindeutige Konten und Gruppen erstellen möchten oder noch keine Benutzer- und Gruppenhierarchie auf einem LDAP- oder Windows-AD-Server erstellt wurde.
  Die vertrauenswürdige Authentifizierung gehört zur Enterprise-Authentifizierung und ist in Einzelanmeldungslösungen von Drittherstellern integriert, einschließlich Java Authentication and Authorization Service (JAAS). Anwendungen, die eine Vertrauensstellung beim Central Management Server haben, können die vertrauenswürdige Authentifizierung verwenden, damit sich Benutzer ohne Angabe ihrer Kennwörter anmelden können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- LDAP-Sicherheits-Plugin
- Windows AD

> **Hinweis**
>
> Obwohl ein Benutzer die Windows-AD-Authentifizierung für die BI-Plattform und benutzerdefinierte Anwendungen über die CMC konfigurieren kann, unterstützen die CMC und BI-Launchpad selbst keine Windows-AD-Authentifizierung mit NTLM. Die einzigen Authentifizierungsmethoden, die von der CMC und BI-Launchpad unterstützt werden, sind Windows AD mit Kerberos, LDAP, Enterprise und die vertrauenswürdige Authentifizierung.

3.1.8.2 ERP-Integration (Enterprise Resource Planning)

ERP-Anwendungen unterstützen die wesentlichen Funktionen der Prozesse einer Organisation, indem sie Echtzeitdaten über tägliche Geschäftsoperationen erfassen. Die BI-Plattform unterstützt die Einzelanmeldung und Berichterstellung aus folgenden ERP-Systemen:

- SAP ERP und Business Warehouse (BW)
- Siebel Enterprise
- Oracle E-Business Suite
- JD Edwards EnterpriseOne
- PeopleSoft Enterprise

> **Hinweis**
>
> - Die SAP ERP- und BW-Unterstützung ist standardmäßig installiert. Mit der Installationsoption *Benutzerdefiniert/Erweitert* können Sie die Auswahl der SAP-Integrationsunterstützung aufheben, wenn Sie keine Unterstützung für SAP ERP oder BW wünschen.
> - Die Unterstützung für Siebel Enterprise, Oracle E-Business Suite, JD Edwards EnterpriseOne oder PeopleSoft ist standardmäßig nicht installiert. Mit der Installationsoption *Benutzerdefiniert/Erweitert* können Sie die Integration für SAP-fremde ERP-Systeme auswählen und installieren.

Einzelheiten zu den spezifischen, von der BI-Plattform unterstützten Versionen finden Sie im Dokument *Supported Platforms/PARs* unter *https://service.sap.com/bosap-support*.

Informationen zur Konfiguration der ERP-Integration finden Sie im Kapitel *Ergänzende Konfigurationen für ERP-Umgebungen* dieses Handbuchs.

3.1.9 SAP-Integration

Die BI-Plattform ist in die folgenden SAP-Tools in der vorhandenen SAP-Infrastruktur integriert:

- SAP System Landscape Directory (SLD)

  System Landscape Directory von SAP NetWeaver ist die zentrale Quelle von Systemlandschaftsinformationen, die für die Verwaltung des Softwarelebenszyklus relevant sind. Durch

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Bereitstellung eines Verzeichnisses, das Informationen über die gesamte von SAP verfügbare installierbare Software sowie automatisch aktualisierte Daten über die bereits in einer Landschaft installierten Systeme enthält, erhalten Sie die Grundlage für die Toolunterstützung zur Planung von Softwarelebenszyklusaufgaben in der Systemlandschaft.

Das Installationsprogramm der BI-Plattform registriert die Hersteller- und Produktnamen, Versionen, Server- und Frontend-Komponentennamen, Versionen und den Speicherort bei SLD.

- SAP Solution Manager

  SAP Solution Manager ist eine Plattform, die integrierte Inhalte, Tools und Methodiken zur Implementierung, zur Unterstützung, zum Betrieb und zur Überwachung von SAP-Systemen und anderen Systemen zur Verfügung stellt.

  Software, die nicht von SAP stammt und eine von SAP zertifizierte Integration beinhaltet, wird in ein zentrales Repository eingetragen und automatisch in SAP System Landscape Directory (SLD) übertragen. SAP-Kunden können einfach ermitteln, welche Version der Drittanbieter-Produktintegration von SAP innerhalb der SAP-Systemumgebung zertifiziert wurde. Dieser Dienst bietet neben unseren Onlinekatalogen für Drittherstellerprodukte zusätzliche Informationen zu Drittherstellerprodukten.
  SAP Solution Manager steht SAP-Kunden ohne zusätzliche Gebühren zur Verfügung und ermöglicht direkten Zugang zum SAP Support und zu Informationen über SAP-Produkt-Upgrade-Verzeichnisse. Weitere Informationen zu SLD finden Sie unter “Registrierung der BI-Plattform in der Systemlandschaft”.
- Change and Transport System (CTS+)

  Mit dem CTS können Sie Entwicklungsprojekte in der ABAP Workbench und im Customizing organisieren und dann die Änderungen zwischen den SAP-Systemen in der Systemlandschaft transportieren. Wie ABAP-Objekte können Sie auch Java-Objekte (J2EE, JEE) und SAP-spezifische Nicht-ABAP-Technologien (z.B. Web Dynpro Java oder SAP NetWeaver Portal) in der Landschaft transportieren.
- Überwachen mit CA Wily Introscope

  CA Wily Introscope ist ein Webanwendungsmanagement-Produkt, mit dem Leistungsprobleme überwacht und diagnostiziert werden können, die in Java-basierten SAP-Modulen in der Produktion auftreten können. Dazu gehören die Transparenz von benutzerdefinierten Java-Anwendungen und Verbindungen zu Backendsystemen. Außerdem können Sie Leistungsengpässe in NetWeaver-Modulen, einschließlich einzelner Servlets, JSPs, EJBs, JCOs, Klassen und Methoden, isolieren. Das Produkt bietet Echtzeitüberwachung mit geringem Overhead, End-to-End-Transaktionstransparenz, historische Daten für Analysen oder Kapazitätsplanung, anpassbare Dashboards, automatisierte Grenzwertalarme und eine offene Architektur für eine über NetWeaver-Umgebungen hinausgehende Überwachung.

3.1.10 Integrierte Versionskontrolle

Die Dateien, aus denen sich die BI-Plattform auf einem Serversystem zusammensetzt, unterliegen jetzt der Versionskontrolle. Das Installationsprogramm installiert und konfiguriert das Subversion-Versionskontrollsystem. Sie können stattdessen auch Details zur Verwendung eines vorhandenen Subversion- oder ClearCase-Versionskontrollsystems eingeben.

Versionskontrollsysteme dienen der Speicherung und dem Wiederherstellen verschiedener Revisionen von Konfigurations- und anderen Dateien, d.h. das System kann in einen bekannten Status in der Vergangenheit zurückversetzt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3.1.11 Upgrade-Pfad

Es ist möglich, ein Upgrade von einem vorherigen Release von SAP BusinessObjects Enterprise (z.B. XI 3.x durchzuführen. Dafür müssen Sie jedoch zunächst SAP BusinessObjects Business Intelligence 4.x installieren und dann die Einstellungen und Daten vom bestehenden System mithilfe des Upgrade-Management-Tools migrieren.

Informationen zum Durchführen eines Upgrades aus einer früheren Version finden Sie im *Aktualisierungshandbuch für SAP BusinessObjects Business Intelligence*.

3.2 Server, Dienste, Knoten und Hosts

Die BI-Plattform verwendet die Begriffe Server und Dienst zur Bezeichnung von zwei Softwarevarianten, die auf einem BI-Plattform-Computer ausgeführt werden.

Als "Server" wird ein Prozess auf Betriebssystemebene bezeichnet (auf manchen Systemen wird dies Daemon) genannt), auf dem ein oder mehrere Dienste gehostet werden. Der Central Management Server (CMS) und der Adaptive Processing Server sind beispielsweise Server. Ein Server wird unter einem bestimmten Betriebssystemkonto ausgeführt und verfügt über eine eigene Prozess-ID (PID).

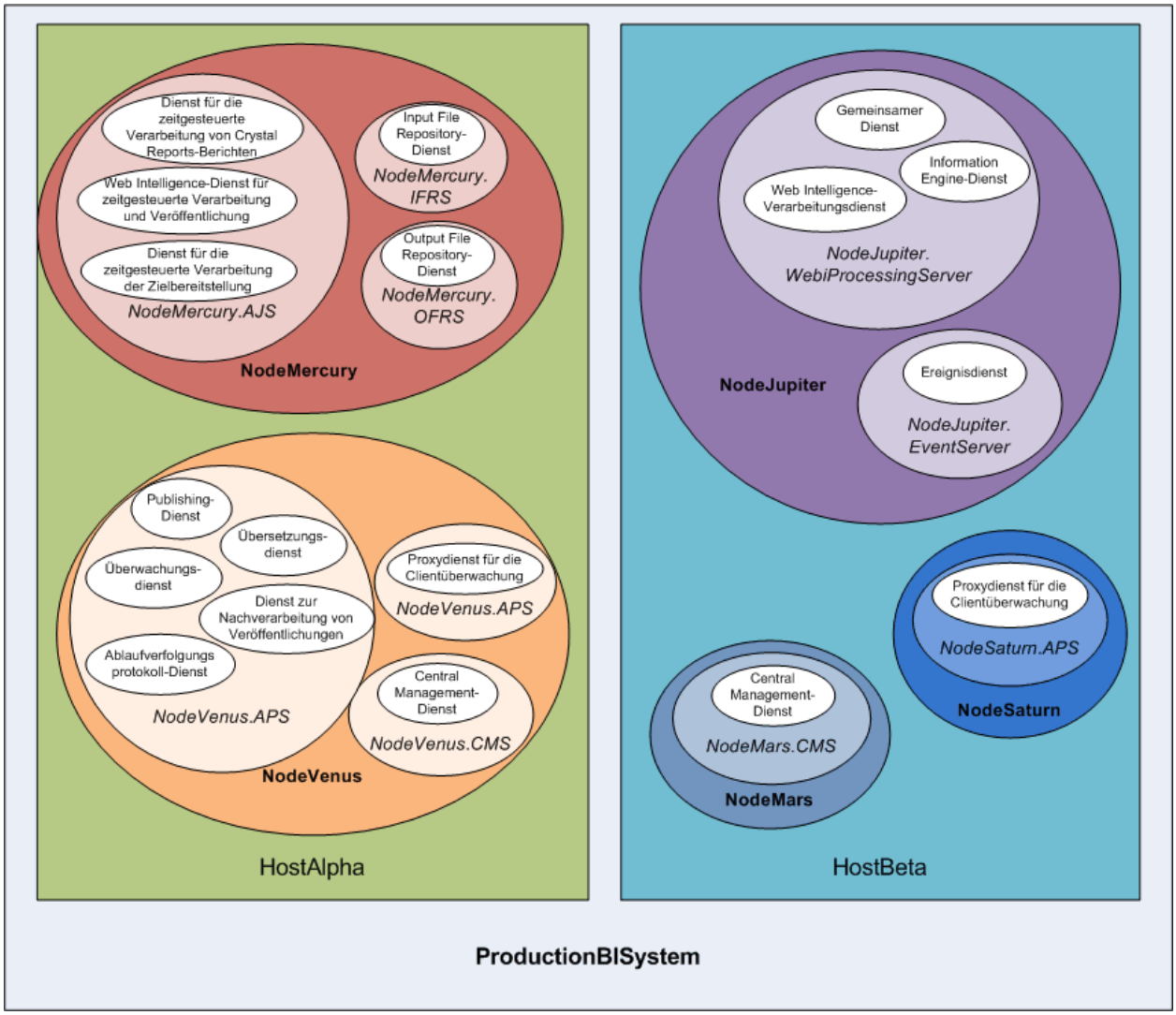
Ein Dienst ist ein Server-Untersystem, das eine bestimmte Funktion ausführt. Der Dienst wird im Speicherbereich des zugehörigen Servers und unter der Prozess-ID des übergeordneten Containers (Servers) ausgeführt. Der Dienst zur zeitgesteuerten Verarbeitung von Web Intelligence ist beispielsweise ein Untersystem, das innerhalb des Adaptive Job Server ausgeführt wird.

Ein Knoten entspricht einer Gruppe von BI-Plattform-Servern, die auf demselben Host ausgeführt und von einem einzelnen Server Intelligence Agent (SIA) verwaltet werden. Auf einem einzelnen Host können sich ein oder mehrere Knoten befinden.

Die BI-Plattform kann auf einem Einzelrechner installiert, über verschiedene Computer in einem Intranet verteilt oder in einem Wide Area Network (WAN) installiert werden.

Das folgende Diagramm zeigt eine hypothetische Installation der BI-Plattform an. Die Anzahl an Hosts, Knoten, Servern und Diensten – sowie die Server- und Diensttypen – weichen in echten Installationen davon ab.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.



Zwei Hosts bilden ein Cluster mit der Bezeichnung ProductionBISystem:

- Auf dem Host mit der Bezeichnung HostAlpha ist die BI-Plattform installiert und für zwei Knoten konfiguriert:
  - NodeMercury enthält einen Adaptive Job Server (`NodeMercury.AJS`) mit Diensten zum zeitgesteuerten Verarbeiten und Veröffentlichen von Berichten, einen Input File Repository Server (`NodeMercury.IFRS`) mit einem Dienst zum Speichern von Eingabeberichten sowie einen Output File Repository Server (`NodeMercury.OFRS`) mit einem Dienst zum Speichern der Berichtsausgabe.
  - NodeVenus enthält einen Adaptive Processing Server (`NodeVenus.APS`) mit Diensten zur Bereitstellung von Veröffentlichungs-, Überwachungs- und Übersetzungsfunktionen, einen Adaptive Processing Server (`NodeVenus.APS2`) mit einem Dienst für das Client-Auditing und einen Central Management Server (`NodeVenus.CMS`) mit einem Dienst zur Bereitstellung der CMS-Dienste.
- Auf dem Host mit der Bezeichnung HostBeta ist die BI-Plattform installiert und für drei Knoten konfiguriert:
  - NodeMars enthält einen Central Management Server (`NodeMars.CMS`) mit einem Dienst zur Bereitstellung der CMS-Dienste. Da der CMS auf zwei Rechnern installiert ist, stehen Lastausgleich, Abwehr- und Failover-Fähigkeiten zur Verfügung.
  - NodeJupiter: enthält einen Web Intelligence Processing Server (`NodeJupiter.Web Intelligence`) mit einem Dienst zur Bereitstellung von Web-Intelligence-Berichterstellungsfunktionen und einen Event

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Server (`NodeJupiter.EventServer`) zur Bereitstellung von Funktionen zur Überwachung von Berichten.

- NodeSaturn enthält einen Adaptive Processing Server (`NodeSaturn.APS`) mit einem Dienst zur Bereitstellung von Client-Audits.

3.2.1 Serveränderungen seit XI 3.1

In der Tabelle unten sind die Hauptänderungen an den BI-Plattform-Servern seit XI 3.1 aufgeführt, unter anderem folgende:

- Server, deren Name sich von Version zu Version geändert hat, obgleich dieselbe oder ähnliche Funktionalität bereitgestellt wird
- Server, die nicht mehr in neueren Versionen zur Verfügung stehen
- Gemeinsame oder verwandte Dienste, die in den Adaptive Servern konsolidiert wurden

  Beispielsweise wurden die Dienste für die zeitgesteuerte Verarbeitung, die von einzelnen Job Servern in XI 3.1 bereitgestellt wurden, ab der 4.0-Version in den Adaptive Job Server verschoben.
- Neu eingeführte Server

Tabelle 1: Serveränderungen

XI 3.1	4.0	4.0 Feature Pack 3	4.1
Connection Server [1]	Connection Server Connection Server 32	Connection Server Connection Server 32	Connection Server Connection Server 32
Crystal Reports Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Crystal Reports Processing Server	Crystal Reports 2011 Processing Server Crystal Reports Processing Server (für SAP-Crystal-Reports-für-Enterprise-Berichte)	Crystal Reports 2011 Processing Server Crystal Reports Processing Server (für SAP-Crystal-Reports-für-Enterprise-Berichte)	Crystal Reports 2013 Processing Server Crystal Reports Processing Server (für SAP-Crystal-Reports-für-Enterprise-Berichte)
Dashboard Server (Dashboard Builder) [2]	Dashboard Server (BI-Arbeitsbereiche)	Ab 4.0 Feature Pack 3 nicht mehr verfügbar	In 4.1 nicht verfügbar
Dashboard Analytics Server (Dashboard Builder) [2]	Dashboard Analytics Server (BI-Arbeitsbereiche)	Ab 4.0 Feature Pack 3 nicht mehr verfügbar	In 4.1 nicht verfügbar
Desktop Intelligence Cache Server [3]	Ab 4.0 nicht mehr verfügbar	Ab 4.0 nicht mehr verfügbar	In 4.1 [3] nicht verfügbar
Desktop Intelligence Job Server [3]	Ab 4.0 nicht mehr verfügbar	Ab 4.0 nicht mehr verfügbar	In 4.1 [3] nicht verfügbar
Desktop Intelligence Processing Server [3]	Ab 4.0 nicht mehr verfügbar	Ab 4.0 nicht mehr verfügbar	In 4.1 [3] nicht verfügbar

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

XI 3.1	4.0	4.0 Feature Pack 3	4.1
Destination Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
List of Values Server (LOV)	Web Intelligence Processing Server	Web Intelligence Processing Server	Web Intelligence Processing Server
Multi-Dimensional Analysis Services Server	Adaptive Processing Server	Adaptive Processing Server	Adaptive Processing Server
Program Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2013 Report Application Server (RAS)
Web Intelligence Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Xcelsius-Cache-Server [4]	Dashboard Design Cache Server (Xcelsius) [5]	Dashboards Cache Server (Xcelsius)	Dashboards Cache Server (Xcelsius)
Xcelsius-Verarbeitungsserver [4]	Dashboard Design Processing Server (Xcelsius) [5]	Dashboards Processing Server (Xcelsius)	Dashboards Processing Server (Xcelsius)

- [1] In 4.0 ist Connection Server 32 ein 32-Bit-Server, der Verbindungen speziell mit Datenquellen herstellt, die 64-Bit-Middleware nicht unterstützen. Connection Server ist ein 64-Bit-Server, der Verbindungen mit allen anderen Datenquellen herstellen kann. Weitere Informationen finden Sie im *Datenzugriffshandbuch*.
- [2] Der Dashboard Server und der Dashboard Analytics Server wurden aus 4.0 Feature Pack 3 entfernt. Für die BI-Arbeitsbereichfunktionalität ist keine Serverkonfiguration mehr nötig (früher Dashboard Builder in XI 3.1).
- [3] Desktop Intelligence war in Version 4.0 und in 4.0-Wartungspaketen nicht verfügbar. Die Desktop-Intelligence-Clientanwendung ist in Version 4.1 verfügbar, Desktop-Intelligence-Server jedoch nicht. Desktop-Intelligence-Berichte können mithilfe des Berichtskonvertierungstools in Web-Intelligence-Dokumente konvertiert werden.
- Die Cache- und Verarbeitungsdienste von Xcelsius wurden mit XI 3.1 Service Pack 3 eingeführt, um Query-as-a-Web-Service-Anforderungen für relationale Datenquellen aus Xcelsius zu optimieren. Äquivalente Cache- und Verarbeitungsdienste stehen auf dem Dashboards Cache Server und dem Dashboards Processing Server ab 4.0 Feature Pack 3 zur Verfügung.
- [5] Dashboard Design Server aus 4.0 wurden in 4.0 Feature Pack 3 in “Dashboards” umbenannt, um die Produktnamensänderung in SAP BusinessObjects Dashboards widerzuspiegeln.

3.2.2 Dienste

Beim Hinzufügen von Servern müssen Sie verschiedene Dienste auf dem Adaptive Job Server einbeziehen, beispielsweise den Dienst für die zeitgesteuerte Verarbeitung der Zielbereitstellung.

> **Hinweis**
>
> In künftigen Wartungsversionen können neue Dienst- oder Servertypen hinzugefügt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Dienst	Dienstkategorie	Servertyp	Dienstbeschreibung
Adaptiver Konnektivitätsdienst	Konnektivitätsdienste	Adaptive Processing Server	Stellt Konnektivitätsdienste für Java-basierte Treiber bereit
Dienst für die zeitgesteuerte Verarbeitung von Authentifizierungsaktualisierungen	Kerndienste	Adaptive Job Server	Stellt Synchronisierung von Updates für Sicherheits-Plugins von Drittherstellern bereit
BEx-Web-Applications-Dienst	Analysis Services	Adaptive Processing Server	Ermöglicht die Integration von SAP Business Warehouse (BW) Business Explorer (BEx) Web Applications in BI-Launchpad
BOE-Webanwendungsdienst	Kerndienste	Web Application Container Server	Stellt Webanwendungen für den WACS bereit, z.B. die Central Management Console (CMC), BI-Launchpad und OpenDocument
Business Process BI-Dienst	Kerndienste	Web Application Container Server	Stellt Business-Process-BI-Webdienste für den WACS bereit und ermöglicht so die Einbindung von BI-Technologie in Webanwendungen. Der Business Process BI-Dienst ist veraltet.
Central Management Service	Kerndienste	Central Management Server	Stellt Server-, Benutzer- und Sitzungsverwaltung sowie Sicherheitsverwaltung (Zugriffsrechte und Authentifizierung) zur Verfügung. Für ein funktionsfähiges Cluster muss mindestens ein Central Management Service zur Verfügung stehen.
Proxydienst für die Clientüberwachung	Kerndienste	Adaptive Processing Server	Sammelt Auditing-Ereignisse von Clients und leitet sie an den CMS-Server weiter
Crystal Reports 2013-Verarbeitungsdienst	Crystal-Reports-Dienste	Crystal Reports Processing Server	Akzeptiert und verarbeitet Crystal-Reports-2013-Berichte und

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Dienst	Dienstkategorie	Servertyp	Dienstbeschreibung
			kann Daten in Berichten gemeinsam nutzen, um die Anzahl der Datenbankzugriffe zu verringern
Dienst für die zeitgesteuerte Verarbeitung von Crystal Reports 2013-Berichten	Crystal-Reports-Dienste	Adaptive Job Server	Führt zeitgesteuerte Crystal-Reports-Aufträge älterer Versionen aus und veröffentlicht die Ergebnisse an einem Ausgabespeicherort
Anzeige- und Änderungsdienst von Crystal Reports 2013	Crystal-Reports-Dienste	Report Application Server (RAS)	Verarbeitet Anzeige- und Modifizierungsanfragen für Berichte von Crystal Reports 2013
Crystal-Reports-Cache-Dienst	Crystal-Reports-Dienste	Crystal Reports Cache Server	Begrenzt die Anzahl der durch Crystal-Reports-Berichte verursachte Datenbankzugriffe und beschleunigt die Berichtserstellung durch Verwaltung eines Berichts-Caches
Dienst für die Verarbeitung von Crystal-Reports-Berichten	Crystal-Reports-Dienste	Crystal Reports Processing Server	Akzeptiert und verarbeitet Crystal-Reports-Berichte und kann Daten in Berichten gemeinsam nutzen, um die Anzahl der Datenbankzugriffe zu verringern
Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-Berichten	Crystal-Reports-Dienste	Adaptive Job Server	Führt zeitgesteuerte neue Crystal-Reports-Aufträge aus und veröffentlicht die Ergebnisse an einem Ausgabespeicherort
Benutzerdefinierter Datenzugriffsdienst	Web-Intelligence-Dienste	Adaptive Processing Server	Bereitstellen dynamischer Verbindungen zu Datenquellen, die keinen Connection Server benötigen. Dieser Dienst ermöglicht den Abruf und die Regenerierung von Berichten, die mit einem bestimmten per-

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Dienst	Dienstkategorie	Servertyp	Dienstbeschreibung
			sönlichen Datenprovider erstellt wurden, wie z. B. CSV-Dateien. Weitere Informationen zum Erstellen einer Abfrage oder Regenerieren eines Dokuments auf Basis einer Textdatei finden Sie im *Benutzerhandbuch für den Web-Intelligence-Rich-Client von SAP BusinessObjects*.
Dashboard-Cache-Dienst	Dashboards-Dienste	Dashboards Cache Server	Begrenzt die Anzahl der durch Dashboards-Inhalte verursachten Datenbankzugriffe und beschleunigt die Erstellung von Berichten durch einen verwalteten Berichts-Cache.
Dashboards-Verarbeitungsdienst	Dashboards-Dienste	Dashboards Processing Server	Akzeptiert und verarbeitet Dashboards-Inhalte und kann Daten in Berichten gemeinsam nutzen, um die Anzahl der Datenbankzugriffe zu verringern
Datenföderations-Dienst	Datenföderations-Dienste	Adaptive Processing Server	Fragt die zugrunde liegenden Datenquellen für ein Universum mit mehreren Quellen ab und verarbeitet sie
Dienst für die zeitgesteuerte Verarbeitung der Zielbereitstellung	Kerndienste	Adaptive Job Server	Führt zeitgesteuerte Aufträge aus und veröffentlicht die Ergebnisse an einem Ausgabespeicherort, z.B. dem Dateisystem, FTP-Server, E-Mail-Client oder Posteingang eines Benutzers **Hinweis** Beim Hinzufügen von Servern müssen Sie

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Dienst	Dienstkategorie	Servertyp	Dienstbeschreibung
			verschiedene Adaptive-Job-Server-Dienste einbeziehen, einschließlich diesen Dienst
Dokument-Wiederherstellungsdienst	Web-Intelligence-Dienste	Adaptive Processing Server	Automatisches Speichern und Wiederherstellen von Web-Intelligence-Dokumenten
DSL-Bridge-Dienst	Web-Intelligence-Dienste	Adaptive Processing Server	Sitzungsunterstützung der dimensionalen semantischen Ebene (DSL)
Ereignisdienst	Kerndienste	Event Server	Überwacht Dateiereignisse auf einem File Repository Server (FRS) und löst bei Bedarf die Ausführung von Berichten aus
Excel-Datenzugriffsdienst	Web-Intelligence-Dienste	Adaptive Processing Server	Unterstützt Excel-Dateien, die zur BI-Plattform als Datenquellen hochgeladen wurden. Weitere Informationen zum Erstellen einer Abfrage oder Regenerieren eines Dokuments auf Basis einer Excel-Datei finden Sie im *Benutzerhandbuch für den Web-Intelligence-Rich-Client von SAP BusinessObjects*.
Information Engine-Dienst	Web-Intelligence-Dienste	Web Intelligence Processing Server	Erforderlicher Dienst zur Verarbeitung von Web-Intelligence-Dokumenten
Input-Dateispeicherdienst	Kerndienste	Input File Repository Server	Verwaltet veröffentlichte Berichts- und Programmobjekte, mit denen beim Empfang einer Eingabedatei neue Berichte generiert werden können

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Dienst	Dienstkategorie	Servertyp	Dienstbeschreibung
Dienst "Insight to Action"	Kerndienste	Adaptive Processing Server	Ermöglicht das Aufrufen von Aktionen und bietet Unterstützung für RRI
Lifecycle-Management-ClearCase-Dienst	Lifecycle-Management-Dienste	Adaptive Processing Server	Bietet ClearCase-Unterstützung für LCM
Lifecycle-Management-Dienst für die zeitgesteuerte Verarbeitung	Lifecycle-Management-Dienste	Adaptive Job Server	Führt zeitgesteuerte Lifecycle-Management-Aufträge aus
Lifecycle-Management-Dienst	Lifecycle-Management-Dienste	Adaptive Processing Server	Lifecycle-Management-Kerndienst
Überwachungsdienst	Kerndienste	Adaptive Processing Server	Stellt Überwachungsfunktionen bereit
Multi Dimensional Analysis Service	Analysis Services	Adaptive Processing Server	Stellt Zugriff auf mehrdimensionale Online-Analytical-Processing-Daten (OLAP-Daten) bereit und konvertiert die Rohdaten in das XML-Format zur Ausgabe in Excel, als PDF oder als Advanced-Analysis-Kreuztabellen und -Diagramme (früher Voyager)
Systemeigener Konnektivitätsdienst	Konnektivitätsdienste	Connection Server	Stellt systemeigene Konnektivitätsdienste für 64-Bit-Architekturen bereit
Systemeigener Konnektivitätsdienst (32-Bit)	Konnektivitätsdienste	Connection Server	Stellt systemeigene Konnektivitätsdienste für 32-Bit-Architekturen bereit
Output-Dateispeicherdienst	Kerndienste	Output File Repository Server	Verwaltet eine Sammlung abgeschlossener Dokumente
Dienst zur zeitgesteuerten Verarbeitung der Plattformsuche	Kerndienste	Adaptive Job Server	Führt eine zeitgesteuerte Suche zur Indizierung des gesamten Inhalts des Central-Management-Server-Repositorys (CMS-Repositorys) durch

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Dienst	Dienstkategorie	Servertyp	Dienstbeschreibung
Plattformsuchdienst	Kerndienste	Adaptive Processing Server	Stellt der BI-Plattform Suchfunktionalität bereit.
Dienst für die zeitgesteuerte Verarbeitung von Diagnosen	Kerndienste	Adaptive Job Server	Stellt zeitgesteuerte Diagnoseaufträge bereit und veröffentlicht die Ergebnisse an einem Ausgabespeicherort
Dienst zur zeitgesteuerten Verarbeitung von Programmen	Kerndienste	Adaptive Job Server	Führt Programme aus, die für einen bestimmten Zeitpunkt terminiert wurden
Dienst zur zeitgesteuerten Verarbeitung von Veröffentlichungen	Kerndienste	Adaptive Job Server	Führt zeitgesteuerte Veröffentlichungsaufträge aus und veröffentlicht die Ergebnisse an einem Ausgabespeicherort
Dienst zur Nachverarbeitung von Veröffentlichungen	Kerndienste	Adaptive Processing Server	Führt Aktionen für abgeschlossene Berichte aus, z.B. das Senden eines Berichts an einen Ausgabespeicherort
Publishing-Dienst	Kerndienste	Adaptive Processing Server	Kooperiert mit dem Dienst zur Nachverarbeitung von Veröffentlichungen und dem Destination Job Server, um Berichte an einem Ausgabespeicherort wie einem Dateisystem, FTP-Server, E-Mail-Client oder Posteingang eines Benutzers zu veröffentlichen
Rebean-Dienst	Web-Intelligence-Dienste	Adaptive Processing Server	Von Web Intelligence und Explorer verwendetes SDK
Replikationsdienst	Kerndienste	Adaptive Job Server	Führt zeitgesteuerte Datenföderations-Aufträge aus, um Inhalte zwischen föderierten Websites zu replizieren

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Dienst	Dienstkategorie	Servertyp	Dienstbeschreibung
RESTful-Webdienst	Kerndienste	Web Application Container Server (WACS)	Stellt Sitzungsverarbeitung für Anforderungen des RESTful-Webdiensts bereit
Dienst zur zeitgesteuerten Verarbeitung von Sicherheitsabfragen	Kerndienste	Adaptive Job Server	Führt die zeitgesteuerte Verarbeitung von Sicherheitsabfragen-Aufträgen aus
Sicherheitstokendienst	Kerndienste	Adaptive Processing Server	Unterstützung für SAP-Einzelanmeldung
Übersetzungsdienst	Kerndienste	Adaptive Processing Server	Übersetzt InfoObjects mit Eingaben vom Übersetzungsmanager-Client
Dienst für die zeitgesteuerte Verarbeitung des Benutzer- und Gruppenimports	Kerndienste	Adaptive Job Server	Ermöglicht die Einplanung von Prinzipal-Dateiimporten
Dienst zur zeitgesteuerten Verarbeitung für den grafischen Vergleich	Lifecycle-Management-Dienste	Adaptive Job Server	Führt zeitgesteuerte Aufträge für den grafischen Vergleich (Lifecycle-Management) aus und veröffentlicht die Ergebnisse an einem Ausgabespeicherort
Grafischer Vergleichsdienst	Lifecycle-Management-Dienste	Adaptive Processing Server	Ermittelt, ob Dokumente grafisch identisch für die Hochstufung von Dokumenten und das Lifecycle-Management sind
Visualisierungsdienst	Web-Intelligence-Dienste	Adaptive Processing Server	Von Web Intelligence verwendeter gemeinsamer Visualisierungsdienst für Objektmodelle
Gemeinsamer Web-Intelligence-Dienst	Web-Intelligence-Dienste	Web Intelligence Processing Server	Unterstützt die Verarbeitung von Web-Intelligence-Dokumenten
Web-Intelligence-Kerndienst	Web-Intelligence-Dienste	Web Intelligence Processing Server	Unterstützt die Verarbeitung von Web-Intelligence-Dokumenten
Web-Intelligence-Verarbeitungsdienst	Web-Intelligence-Dienste	Web Intelligence Processing Server	Akzeptiert und verarbeitet Web-Intelligence-Dokumente

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Dienst	Dienstkategorie	Servertyp	Dienstbeschreibung
Web-Intelligence-Dienst für zeitgesteuerte Verarbeitung	Web-Intelligence-Dienste	Adaptive Job Server	Bietet Unterstützung für zeitgesteuerte Web-Intelligence-Aufträge
Web Services SDK und QaaWS	Kerndienste	Web Application Container Server	Webdienste auf dem WACS

3.2.3 Dienstkategorien

Hinweis

In künftigen Wartungsversionen können neue Dienst- oder Servertypen hinzugefügt werden.

Dienstkategorie	Dienst	Servertyp
Analysis Services	BEx-Web-Applications-Dienst	Adaptive Processing Server
Analysis Services	Multi Dimensional Analysis Service	Adaptive Processing Server
Konnektivitätsdienste	Adaptiver Konnektivitätsdienst	Adaptive Processing Server
Konnektivitätsdienste	Systemeigener Konnektivitätsdienst	Connection Server
Konnektivitätsdienste	Systemeigener Konnektivitätsdienst (32-Bit)	Connection Server
Kerndienste	Dienst für die zeitgesteuerte Verarbeitung von Authentifizierungsaktualisierungen	Adaptive Job Server
Kerndienste	Central Management Service	Central Management Server
Kerndienste	Proxydienst für die Clientüberwachung	Adaptive Processing Server
Kerndienste	Dashboard-Dienst	Dashboard Server
Kerndienste	Dienst für Zielkonfiguration*	Adaptive Job Server
Kerndienste	Dienst für die zeitgesteuerte Verarbeitung der Zielbereitstellung	Adaptive Job Server
Kerndienste	Ereignisdienst	Event Server
Kerndienste	Dienst "Insight to Action"	Adaptive Processing Server
Kerndienste	Input-Dateispeicherdienst	Input File Repository Server
Kerndienste	Überwachungsdienst	Adaptive Processing Server
Kerndienste	Output-Dateispeicherdienst	Output File Repository Server

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Dienstkategorie	Dienst	Servertyp
Kerndienste	Dienst zur zeitgesteuerten Verarbeitung der Plattformsuche	Adaptive Job Server
Kerndienste	Plattformsuchdienst	Adaptive Processing Server
Kerndienste	Dienst für die zeitgesteuerte Verarbeitung von Diagnosen	Adaptive Job Server
Kerndienste	Dienst zur zeitgesteuerten Verarbeitung von Programmen	Adaptive Job Server
Kerndienste	Dienst zur zeitgesteuerten Verarbeitung von Veröffentlichungen	Adaptive Job Server
Kerndienste	Dienst zur Nachverarbeitung von Veröffentlichungen	Adaptive Processing Server
Kerndienste	Publishing-Dienst	Adaptive Processing Server
Kerndienste	Replikationsdienst	Adaptive Job Server
Kerndienste	RESTful-Webdienst	Web Application Container Server
Kerndienste	Dienst zur zeitgesteuerten Verarbeitung von Sicherheitsabfragen	Adaptive Job Server
Kerndienste	Sicherheitstokendienst	Adaptive Processing Server
Kerndienste	Einzelanmeldungsdienst*	Central Management Server, Connection Server, Crystal Reports Processing Server, RAS, Dashboards Processing Server und Web Intelligence Processing Server
Kerndienste	Ablaufverfolgungsprotokoll-Dienst	Beliebiger Server
Kerndienste	Übersetzungsdienst	Adaptive Processing Server
Kerndienste	Dienst für die zeitgesteuerte Verarbeitung des Benutzer- und Gruppenimports*	Adaptive Job Server
Kerndienste	Webanwendungs-Containerdienst*	Web Application Container Server
Crystal-Reports-Dienste	Crystal Reports 2013-Verarbeitungsdienst	Crystal Reports Processing Server
Crystal-Reports-Dienste	Dienst für die zeitgesteuerte Verarbeitung von Crystal Reports 2013-Berichten	Adaptive Job Server
Crystal-Reports-Dienste	Anzeige- und Änderungsdienst von Crystal Reports 2013	Report Application Server (RAS)
Crystal-Reports-Dienste	Crystal-Reports-Cache-Dienst	Crystal Reports Cache Server
Crystal-Reports-Dienste	Dienst für die Verarbeitung von Crystal-Reports-Berichten	Crystal Reports Processing Server

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Dienstkategorie	Dienst	Servertyp
Crystal-Reports-Dienste	Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-Berichten	Adaptive Job Server
Dashboards-Dienste	Dashboard-Cache-Dienst	Dashboards Cache Server
Dashboards-Dienste	Dashboards-Verarbeitungsdienst	Dashboards Processing Server
Datenföderations-Dienste	Datenföderations-Dienst	Adaptive Processing Server
Lifecycle-Management-Dienste	LifeCycle-Management-ClearCase-Dienst	Adaptive Processing Server
Lifecycle-Management-Dienste	Lifecycle-Management-Dienst für die zeitgesteuerte Verarbeitung	Adaptive Job Server
Lifecycle-Management-Dienste	Lifecycle-Management-Dienst	Adaptive Processing Server
Lifecycle-Management-Dienste	Dienst zur zeitgesteuerten Verarbeitung für den grafischen Vergleich	Adaptive Job Server
Lifecycle-Management-Dienste	Grafischer Vergleichsdienst	Adaptive Processing Server
Web-Intelligence-Dienste	Benutzerdefinierter Datenzugriffsdienst	Adaptive Processing Server
Web-Intelligence-Dienste	Dokument-Wiederherstellungsdienst	Adaptive Processing Server
Web-Intelligence-Dienste	DSL-Bridge-Dienst	Adaptive Processing Server
Web-Intelligence-Dienste	Excel-Datenzugriffsdienst	Adaptive Processing Server
Web-Intelligence-Dienste	Information Engine-Dienst	Web Intelligence Processing Server
Web-Intelligence-Dienste	Rebean-Dienst	Adaptive Processing Server
Web-Intelligence-Dienste	Visualisierungsdienst	Adaptive Processing Server
Web-Intelligence-Dienste	Gemeinsamer Web-Intelligence-Dienst	Web Intelligence Processing Server
Web-Intelligence-Dienste	Web-Intelligence-Kerndienst	Web Intelligence Processing Server
Web-Intelligence-Dienste	Web-Intelligence-Überwachungsdienst*	Adaptive Processing Server
Web-Intelligence-Dienste	Web-Intelligence-Verarbeitungsdienst	Web Intelligence Processing Server
Web-Intelligence-Dienste	Web-Intelligence-Dienst für zeitgesteuerte Verarbeitung	Adaptive Job Server

3.2.4 Servertypen

Ein Sternchen neben einem Dienstnamen gibt an, dass es sich um einen sekundären Dienst handelt. Einige sekundäre Dienste werden automatisch erstellt. Nachdem Sie den primären Dienst, von dem ein sekundärer

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Dienst abhängig ist, ausgewählt haben, müssen Sie jedoch auswählen, ob andere sekundäre Dienste eingeschlossen werden sollen.

> **Hinweis**
>
> In künftigen Wartungsversionen können neue Dienst- oder Servertypen hinzugefügt werden.

Servertyp	Dienst	Dienstkategorie
Beliebiger Server	Ablaufverfolgungsprotokoll-Dienst	Kerndienste
Adaptive Job Server	Dienst für die zeitgesteuerte Verarbeitung von Authentifizierungsaktualisierungen	Kerndienste
Adaptive Job Server	Dienst für die zeitgesteuerte Verarbeitung von Crystal Reports 2013-Berichten	Crystal-Reports-Dienste
Adaptive Job Server	Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-Berichten	Crystal-Reports-Dienste
Adaptive Job Server	Dienst für Zielkonfiguration*	Kerndienste
Adaptive Job Server	Dienst für die zeitgesteuerte Verarbeitung der Zielbereitstellung	Kerndienste
Adaptive Job Server	Lifecycle-Management-Dienst für die zeitgesteuerte Verarbeitung	Lifecycle-Management-Dienste
Adaptive Job Server	Dienst zur zeitgesteuerten Verarbeitung der Plattformsuche	Kerndienste
Adaptive Job Server	Dienst für die zeitgesteuerte Verarbeitung von Diagnosen	Kerndienste
Adaptive Job Server	Dienst zur zeitgesteuerten Verarbeitung von Programmen	Kerndienste
Adaptive Job Server	Dienst zur zeitgesteuerten Verarbeitung von Veröffentlichungen	Kerndienste
Adaptive Job Server	Replikationsdienst	Kerndienste
Adaptive Job Server	Dienst zur zeitgesteuerten Verarbeitung von Sicherheitsabfragen	Kerndienste
Adaptive Job Server	Dienst für die zeitgesteuerte Verarbeitung des Benutzer- und Gruppenimports*	Kerndienste
Adaptive Job Server	Dienst zur zeitgesteuerten Verarbeitung für den grafischen Vergleich	Lifecycle-Management-Dienste
Adaptive Job Server	Web-Intelligence-Dienst für zeitgesteuerte Verarbeitung	Web-Intelligence-Dienste

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Servertyp	Dienst	Dienstkategorie
Adaptive Processing Server	Adaptiver Konnektivitätsdienst	Konnektivitätsdienste
Adaptive Processing Server	BEx-Web-Applications-Dienst	Analysis Services
Adaptive Processing Server	Proxydienst für die Clientüberwachung	Kerndienste
Adaptive Processing Server	Benutzerdefinierter Datenzugriffsdienst	Web-Intelligence-Dienste
Adaptive Processing Server	Datenföderations-Dienst	Datenföderations-Dienste
Adaptive Processing Server	Dokument-Wiederherstellungsdienst	Web-Intelligence-Dienste
Adaptive Processing Server	DSL-Bridge-Dienst	Web-Intelligence-Dienste
Adaptive Processing Server	Excel-Datenzugriffsdienst	Web-Intelligence-Dienste
Adaptive Processing Server	Dienst "Insight to Action"	Kerndienste
Adaptive Processing Server	Lifecycle-Management-ClearCase-Dienst	Lifecycle-Management-Dienste
Adaptive Processing Server	Lifecycle-Management-Dienst	Lifecycle-Management-Dienste
Adaptive Processing Server	Überwachungsdienst	Kerndienste
Adaptive Processing Server	Multi Dimensional Analysis Service	Analysis Services
Adaptive Processing Server	Plattformsuchdienst	Kerndienste
Adaptive Processing Server	Dienst zur Nachverarbeitung von Veröffentlichungen	Kerndienste
Adaptive Processing Server	Publishing-Dienst	Kerndienste
Adaptive Processing Server	Rebean-Dienst	Web-Intelligence-Dienste
Adaptive Processing Server	Sicherheitstokendienst	Kerndienste
Adaptive Processing Server	Übersetzungsdienst	Kerndienste
Adaptive Processing Server	Grafischer Vergleichsdienst	Lifecycle-Management-Dienste
Adaptive Processing Server	Visualisierungsdienst	Web-Intelligence-Dienste
Adaptive Processing Server	Web-Intelligence-Überwachungsdienst*	Web-Intelligence-Dienste
Central Management Server	Central Management Service	Kerndienste
Central Management Server	Einzelanmeldungsdienst*	Kerndienste
Connection Server	Systemeigener Konnektivitätsdienst	Konnektivitätsdienste
Connection Server	Systemeigener Konnektivitätsdienst (32-Bit)	Konnektivitätsdienste
Connection Server	Einzelanmeldungsdienst*	Kerndienste

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Servertyp	Dienst	Dienstkategorie
Crystal Reports Cache Server	Crystal-Reports-Cache-Dienst	Crystal-Reports-Dienste
Crystal Reports Processing Server	Crystal Reports 2013-Verarbeitungsdienst	Crystal-Reports-Dienste
Crystal Reports Processing Server	Dienst für die Verarbeitung von Crystal-Reports-Berichten	Crystal-Reports-Dienste
Crystal Reports Processing Server	Einzelanmeldungsdienst*	Kerndienste
Dashboards Cache Server	Dashboard-Cache-Dienst	Dashboards-Dienste
Dashboards Processing Server	Dashboards-Verarbeitungsdienst	Dashboards-Dienste
Dashboards Processing Server	Einzelanmeldungsdienst*	Kerndienste
Dashboard Server	Dashboard-Dienst	Kerndienste
Event Server	Ereignisdienst	Kerndienste
Input File Repository Server	Input-Dateispeicherdienst	Kerndienste
Output File Repository Server	Output-Dateispeicherdienst	Kerndienste
Report Application Server (RAS)	Anzeige- und Änderungsdienst von Crystal Reports 2013	Crystal-Reports-Dienste
RAS	Einzelanmeldungsdienst*	Kerndienste
Web Application Container Server	RESTful-Webdienst	Kerndienste
Web Application Container Server	Webanwendungs-Containerdienst*	Kerndienste
Web Intelligence Processing Server	Information Engine-Dienst	Web-Intelligence-Dienste
Web Intelligence Processing Server	Einzelanmeldungsdienst*	Kerndienste
Web Intelligence Processing Server	Gemeinsamer Web-Intelligence-Dienst	Web-Intelligence-Dienste
Web Intelligence Processing Server	Web-Intelligence-Kerndienst	Web-Intelligence-Dienste
Web Intelligence Processing Server	Web-Intelligence-Verarbeitungsdienst	Web-Intelligence-Dienste

Servertyp	Dienst	Dienstkategorie
Adaptive Job Server	Dienst für die zeitgesteuerte Verarbeitung von Authentifizierungsaktualisierungen	Kerndienste
Adaptive Job Server	Dienst für die zeitgesteuerte Verarbeitung von Crystal Reports 2013-Berichten	Crystal-Reports-Dienste
Adaptive Job Server	Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-Berichten	Crystal-Reports-Dienste

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Servertyp	Dienst	Dienstkategorie
Adaptive Job Server	Dienst für die zeitgesteuerte Verarbeitung der Zielbereitstellung	Kerndienste
Adaptive Job Server	Lifecycle-Management-Dienst für die zeitgesteuerte Verarbeitung	Lifecycle-Management-Dienste
Adaptive Job Server	Dienst zur zeitgesteuerten Verarbeitung der Plattformsuche	Kerndienste
Adaptive Job Server	Dienst für die zeitgesteuerte Verarbeitung von Diagnosen	Kerndienste
Adaptive Job Server	Dienst zur zeitgesteuerten Verarbeitung von Programmen	Kerndienste
Adaptive Job Server	Dienst zur zeitgesteuerten Verarbeitung von Veröffentlichungen	Kerndienste
Adaptive Job Server	Replikationsdienst	Kerndienste
Adaptive Job Server	Dienst zur zeitgesteuerten Verarbeitung von Sicherheitsabfragen	Kerndienste
Adaptive Job Server	Dienst zur zeitgesteuerten Verarbeitung für den grafischen Vergleich	Lifecycle-Management-Dienste
Adaptive Job Server	Web-Intelligence-Dienst für zeitgesteuerte Verarbeitung	Web-Intelligence-Dienste
Adaptive Processing Server	Adaptiver Konnektivitätsdienst	Konnektivitätsdienste
Adaptive Processing Server	BEx-Web-Applications-Dienst	Analysis Services
Adaptive Processing Server	Proxydienst für die Clientüberwachung	Kerndienste
Adaptive Processing Server	Benutzerdefinierter Datenzugriffsdienst	Web-Intelligence-Dienste
Adaptive Processing Server	Datenföderations-Dienst	Datenföderations-Dienste
Adaptive Processing Server	Dokument-Wiederherstellungsdienst	Web-Intelligence-Dienste
Adaptive Processing Server	DSL-Bridge-Dienst	Web-Intelligence-Dienste
Adaptive Processing Server	Excel-Datenzugriffsdienst	Web-Intelligence-Dienste
Adaptive Processing Server	Dienst "Insight to Action"	Kerndienste
Adaptive Processing Server	Lifecycle-Management-ClearCase-Dienst	Lifecycle-Management-Dienste
Adaptive Processing Server	Lifecycle-Management-Dienst	Lifecycle-Management-Dienste
Adaptive Processing Server	Überwachungsdienst	Kerndienste
Adaptive Processing Server	Multi Dimensional Analysis Service	Analysis Services
Adaptive Processing Server	Plattformsuchdienst	Kerndienste

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Servertyp	Dienst	Dienstkategorie
Adaptive Processing Server	Dienst zur Nachverarbeitung von Veröffentlichungen	Kerndienste
Adaptive Processing Server	Publishing-Dienst	Kerndienste
Adaptive Processing Server	Rebean-Dienst	Web-Intelligence-Dienste
Adaptive Processing Server	Sicherheitstokendienst	Kerndienste
Adaptive Processing Server	Übersetzungsdienst	Kerndienste
Adaptive Processing Server	Grafischer Vergleichsdienst	Lifecycle-Management-Dienste
Adaptive Processing Server	Visualisierungsdienst	Web-Intelligence-Dienste
Central Management Server	Central Management Service	Kerndienste
Connection Server	Systemeigener Konnektivitäts-dienst	Konnektivitätsdienste
Connection Server	Systemeigener Konnektivitäts-dienst (32-Bit)	Konnektivitätsdienste
Crystal Reports Cache Server	Crystal-Reports-Cache-Dienst	Crystal-Reports-Dienste
Crystal Reports Processing Server	Crystal Reports 2013-Verarbei-tungsdienst	Crystal-Reports-Dienste
Crystal Reports Processing Server	Dienst für die Verarbeitung von Crystal-Reports-Berichten	Crystal-Reports-Dienste
Dashboards Cache Server	Dashboard-Cache-Dienst	Dashboards-Dienste
Dashboards Processing Server	Dashboards-Verarbeitungsdienst	Dashboards-Dienste
Dashboard Server	Dashboard-Dienst	Kerndienste
Event Server	Ereignisdienst	Kerndienste
Input File Repository Server	Input-Dateispeicherdienst	Kerndienste
Output File Repository Server	Output-Dateispeicherdienst	Kerndienste
Report Application Server (RAS)	Anzeige- und Änderungsdienst von Crystal Reports 2013	Crystal-Reports-Dienste
Web Application Container Server	RESTful-Webdienst	Kerndienste
Web Intelligence Processing Server	Information Engine-Dienst	Web-Intelligence-Dienste
Web Intelligence Processing Server	Gemeinsamer Web-Intelligence-Dienst	Web-Intelligence-Dienste
Web Intelligence Processing Server	Web-Intelligence-Kerndienst	Web-Intelligence-Dienste
Web Intelligence Processing Server	Web-Intelligence-Verarbeitungs-dienst	Web-Intelligence-Dienste

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3.2.5 Server

Server sind Zusammenstellungen von Diensten, die unter einem Server Intelligence Agent (SIA) auf einem Host ausgeführt werden. Der Servertyp wird durch die auf diesem ausgeführten Dienste festgelegt. Server können in der Central Management Console (CMC) erstellt werden. In der folgenden Tabelle sind die verschiedenen Servertypen aufgeführt, die in der CMC erstellt werden können.

Server	Beschreibung
Adaptive Job Server	Ein allgemeiner Server, der zeitgesteuerte Aufträge verarbeitet. Wenn Sie dem BI-Plattform-System einen Job Server hinzufügen, können Sie den Job Server für die Verarbeitung von Berichten, Dokumenten, Programmen oder Veröffentlichungen konfigurieren und die Ergebnisse an verschiedene Ziele senden.
Adaptive Processing Server	Generischer Server, auf dem Dienste für die Verarbeitung von Anforderungen aus unterschiedlichen Quellen gehostet werden. Mit dem Installationsprogramm wird ein Adaptive Processing Server (APS) pro Hostsystem installiert. Je nach installierten Funktionen kann dieser APS eine große Anzahl von Diensten hosten, beispielsweise den Überwachungsdienst, Lifecycle-Management-Dienst, Multi-Dimensional Analysis Service (MDAS), Veröffentlichungsdienst und andere. Für Produktions- oder Testsysteme besteht die optimale Vorgehensweise darin, zusätzliche APS zu erstellen und diese gemäß Ihren Geschäftsanforderungen zu konfigurieren. Weitere Informationen finden Sie unter *Einführung in den Systemkonfigurationsassistenten* [Seite 87] und *Konfigurieren von Adaptive Processing Servern für Produktionssysteme* [Seite 388].
Central Management Server (CMS)	Verwaltet eine Datenbank mit Informationen zum BI-Plattform-System (in der CMS-Systemdatenbank) und auditierte Benutzeraktionen (im Audit-Datenspeicher). Alle Plattformdienste werden über den CMS verwaltet. Der CMS steuert auch den Zugriff auf die Systemdateien, in denen Dokumente gespeichert sind, und auf Informationen über Benutzer, Benutzergruppen, Sicherheitsebenen (einschl. Authentifizierung) und Inhalte.
Connection Server	Ermöglicht den Datenbankzugriff auf Quelldaten. Bietet Unterstützung für relationale Datenbanken sowie OLAP und andere Formate. Der Connection Server ist für die Verbindung und die Interaktion mit den unterschiedlichen Datenquellen und die Bereitstellung eines gemeinsamen Funktionssatzes für die Clients zuständig.
Crystal Reports Cache Server	Fängt Berichtsanforderungen ab, die von Clients an den Page Server gesendet werden. Wenn der Cache Server die Anforderung nicht mit einer zwischengespeicherten Berichtseite erfüllen kann, übergibt er die Anforderung an

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Server	Beschreibung
	den Crystal Reports Processing Server, der den Bericht ausführt und Ergebnisse zurückgibt. Der Cache Server führt eine Zwischenspeicherung der Berichtsseite für eine mögliche spätere Verwendung aus.
Crystal Reports Processing Server	Beantwortet Seitenanforderungen, indem Berichte verarbeitet und EPF-Seiten (Encapsulated Page Format) erzeugt werden. Der Hauptvorteil von EPF besteht darin, dass es den Zugriff auf Berichtsseiten auf Abruf unterstützt, sodass nur die angeforderte Seite, aber nicht der gesamte Bericht zurückgegeben wird. Dadurch wird die Leistung erhöht und unnötiger Netzwerkdatenverkehr bei umfangreichen Berichten reduziert.
Dashboards Cache Server	Fängt Berichtsanforderungen ab, die von Clients an den Dashboard Server gesendet werden. Wenn der Cache Server die Anforderung nicht mit einer zwischengespeicherten Berichtseite erfüllen kann, übergibt er die Anforderung an den Dashboard Server, der den Bericht ausführt und Ergebnisse zurückgibt. Der Cache Server führt eine Zwischenspeicherung der Berichtsseite für eine mögliche spätere Verwendung aus.
Dashboards Processing Server	Beantwortet Dashboards-Anforderungen, indem Berichte verarbeitet und EPF-Seiten (Encapsulated Page Format) erzeugt werden. Der Hauptvorteil von EPF besteht darin, dass es den Zugriff auf Berichtsseiten auf Abruf unterstützt, sodass nur die angeforderte Seite, aber nicht der gesamte Bericht zurückgegeben wird. Dadurch wird die Leistung erhöht und unnötiger Netzwerkdatenverkehr bei umfangreichen Berichten reduziert.
Event Server	Überwacht das System auf Ereignisse, die als Trigger für die Berichtsausführung dienen können. Wenn Sie einen Ereignis-Trigger einrichten, überwacht der Event Server dessen Status und benachrichtigt den CMS, wenn das Ereignis eingetreten ist. Anschließend kann der CMS alle Aufträge starten, die bei Eintreten des Ereignisses ausgeführt werden sollen. Der Event Server verwaltet dateibasierte Ereignisse, die auf der Speicherschicht eintreten.
File Repository Server	Verantwortlich für die Erstellung von Dateisystemobjekten, z.B. exportierten Berichten und importierten Dateien in systemfremden Formaten. Ein Input FRS speichert Berichts- und Programmobjekte, die von Administratoren oder Endbenutzern auf dem System veröffentlicht wurden. Ein Output FRS speichert alle vom Job Server generierten Berichtsinstanzen.
Web Intelligence Processing Server	Verarbeitet Dokumente von SAP BusinessObjects Web Intelligence.
Report Application Server	Bietet Ad-hoc-Berichterstellungsfunktionen, mit denen Benutzer Crystal-Reports-Berichte über das SAP Crystal Reports Server Embedded Software Development Kit (SDK) erstellen und ändern können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3.3 Clientanwendungen

Sie können über zwei Hauptarten von Clientanwendungen mit der BI-Plattform interagieren:

- Desktopanwendungen

  Diese Anwendungen müssen unter einem unterstützten Microsoft Windows-Betriebssystem installiert sein und ermöglichen die lokale Datenverarbeitung und Berichtserstellung.

  > **Hinweis**
  >
  > Das Installationsprogramm der BI-Plattform installiert keine Desktop-Anwendungen mehr. Verwenden Sie zur Installation von Desktop-Anwendungen auf einem Server das eigenständige Installationsprogramm der Clienttools von SAP BusinessObjects Business Intelligence.

  Desktopclients ermöglichen es Ihnen, bestimmte BI-Berichtsverarbeitungsvorgänge auf einzelne Clientcomputer auszulagern. Die meisten Desktop-Anwendungen greifen direkt über Treiber, die auf dem Desktop installiert sind, auf die Daten des Unternehmens zu und kommunizieren über CORBA oder verschlüsseltes CORBA SSL mit Ihrer BI-Plattform-Implementierung.
  Beispiele für diesen Anwendungstyp sind Crystal Reports und Live Office.

  > **Hinweis**
  >
  > Obwohl es sich bei Live Office um eine Anwendung mit vielfältiger Funktionalität handelt, kommuniziert sie über HTTP mit BI-Plattform-Webdiensten.

- Webanwendungen

  Diese Anwendungen werden von einem Webanwendungsserver gehostet und sind über einen unterstützten Webbrowser unter Windows-, Macintosh-, Unix- und Linux-Betriebssystemen zugänglich.

  Auf diese Weise haben große Benutzergruppen Zugriff auf Business Intelligence (BI), ohne dass Desktop-Softwareprodukte implementiert werden müssen. Die Kommunikation erfolgt über HTTP mit oder ohne SSL-Verschlüsselung (HTTPS).
  Beispiele für diesen Anwendungstyp sind BI-Launchpad, SAP BusinessObjects Web Intelligence, die Central Management Console (CMC) und Berichtsviewer.

3.3.1 Installiert mit Clienttools von SAP BusinessObjects Business Intelligence

3.3.1.1 Web-Intelligence-Rich-Client

Web-Intelligence-Rich-Client ist ein Ad-hoc-Analyse- und Berichterstellungs-Tool für Geschäftsbenutzer mit oder ohne Zugriff auf die BI-Plattform.

Es ermöglicht Geschäftsbenutzern den Zugriff auf Daten über Universen (.unv und .unx), BEx Queries und andere Quellen und verwendet gängige Geschäftstermini in einer Drag-und-Drop-Oberfläche. Workflows ermöglichen die Analyse sehr weit- oder enggefasster Fragen sowie das Stellen weiterer Fragen zu einem beliebigen Zeitpunkt im Analyseworkflow.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Web-Intelligence-Rich-Client-Benutzer können weiterhin mit Web-Intelligence-Dokumentdateien (.wid) arbeiten, auch wenn sie keine Verbindung zum Central Management Server (CMS) herstellen können.

3.3.1.2 Business View Manager

Mit Business View Manager können Benutzer Objekte der semantischen Ebene erstellen, durch die die Komplexität der zugrunde liegenden Datenbank vereinfacht wird.

Business View Manager kann normale und dynamische Datenverbindungen, Datengrundlagen, Business Elements, Business Views und relationale Ansichten erstellen. Es bietet Ihnen außerdem die Möglichkeit, detaillierte Spalten- und Zeilensicherheit für die Objekte in einem Bericht festzulegen.

Designer können Verbindungen zu mehreren Datenquellen, Verknüpfungstabellen und Aliasfeldnamen erstellen, berechnete Felder erzeugen und anschließend diese vereinfachte Struktur als Business View verwenden. Berichtsdesigner und Benutzer haben dann die Möglichkeit, die Business View als Basis für ihre Berichte einzusetzen, anstatt ihre eigenen Abfragen für die Daten direkt zu erstellen.

3.3.1.3 Berichtskonvertierungstool

Das Berichtskonvertierungstool konvertiert Berichte in das Web-Intelligence-Format und veröffentlicht die Berichte auf einem Central Management Server (CMS).

Berichte können aus den CMS-Ordnern `Öffentlich`, `Favoriten` oder `Posteingang` abgerufen werden. Nach der Konvertierung werden Berichte entweder im selben Ordner wie die ursprünglichen Web-Intelligence-Berichte oder in einem anderen Ordner veröffentlicht. Das Tool konvertiert nicht alle Web-Intelligence-Funktionen und -Berichte. Wie viel konvertiert wird, hängt von den Funktionen im Originalbericht ab. Bestimmte Funktionen verhindern eine vollständige Konvertierung eines Berichts. Andere wiederum werden beim Konvertieren durch das Tool geändert, neu implementiert oder entfernt.

Außerdem dient das Berichtskonvertierungstool auch zum Überwachen der konvertierten Berichte. Auf diese Weise können Sie Berichte identifizieren, die vom Berichtskonvertierungstool nicht vollständig konvertiert werden konnten, und die Ursachen analysieren.

3.3.1.4 Universe-Design-Tool

Mit dem Universe-Design-Tool (früher Universe Designer) können Datendesigner Daten aus mehreren Quellen auf einer semantischen Ebene kombinieren, die die komplexe Datenbankstruktur für die Endbenutzer ausblendet. Sie abstrahiert komplexe Daten durch die Verwendung einer Geschäftssprache anstelle einer technischen Sprache, um auf Daten zuzugreifen, sie zu bearbeiten und zu organisieren.

Mit seiner grafischen Benutzeroberfläche ermöglicht das Universe-Design-Tool die Auswahl und Anzeige von Tabellen in einer Datenbank. Die Datenbanktabellen werden als Tabellensymbole in einem Schema dargestellt. Designer können diese Oberfläche zum Bearbeiten von Tabellen, Erstellen von Joins zwischen Tabellen, Aliastabellen und Kontexten sowie zur Schleifenunterdrückung in einem Schema verwenden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Sie können Universen auch aus Metadatenquellen erstellen. Das Universe-Design-Tool wird für die Universumsgenerierung am Ende des Erstellungsprozesses verwendet.

3.3.1.5 Query as a Web Service

Query as a Web Service ist eine assistentenähnliche Anwendung, mit der Abfragen in einem Webdienst erstellt und in webfähige Anwendungen integriert werden können. Abfragen können gespeichert werden, um einen Katalog von Standardabfragen zu erstellen, die dann von Anwendungserstellern nach Bedarf ausgewählt werden können.

BI-Inhalte (Business Intelligence) sind normalerweise an eine bestimmte Benutzeroberfläche von BI-Tools gebunden. Query as a Web Service ändert dieses Verhalten, indem es zulässt, dass BI-Inhalt an jede Benutzeroberfläche gesendet werden kann, die Webdienste unterstützt.

Query as a Web Service wurde so konzipiert, dass es wie andere Webdienste auf Microsoft-Windows-Anwendungen aufsetzt. Query as a Web Service basiert auf den W3C-Webdienst-Spezifikationen SOAP, SDL und XML. Es besteht aus zwei Hauptkomponenten:

- Serverkomponente

  Die (im Lieferumfang der BI-Plattform enthaltene) Serverkomponente speichert den Katalog von Query as a Web Service und hostet die veröffentlichten Webdienste.
- Clienttool

  Wird von Geschäftsbenutzern verwendet, um Abfragen als Webdienst auf dem Server zu erstellen und zu veröffentlichen. Das Clienttool kann auf mehreren Rechnern installiert werden, die dann auf denselben auf dem Server gespeicherten Katalog zugreifen und diesen gemeinsam nutzen können. Das Clienttool kommuniziert über Webdienste mit den Serverkomponenten.

Durch Query as a Web Service können Webabfragen als Teil unterschiedlicher Clientlösungen verwendet werden. Dazu gehören:

- Microsoft Office, Excel und InfoPath
- SAP NetWeaver
- OpenOffice
- Geschäftsregeln und Prozessverwaltungsanwendungen
- Enterprise-Dienst-Bus-Plattformen

3.3.1.6 Information-Design-Tool

Das Information-Design-Tool (früher Information Designer) ist eine Metadaten-Entwicklungsumgebung, in der Designer Metadaten aus relationalen und OLAP-Quellen extrahieren, definieren und bearbeiten können, um SAP-BusinessObjects-Universen zu erstellen und zu implementieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3.3.1.7 Übersetzungsmanagement-Tool

Die BI-Plattform bietet Unterstützung für mehrsprachige Dokumente und Universen. Ein mehrsprachiges Dokument enthält lokalisierte Versionen von Universum-Metadaten und Dokumentaufforderungen. Benutzer können Berichte erstellen, z.B. von einem einzigen Universum, aber in ausgewählten Sprachen.

Mit dem Übersetzungsmanagement-Tool (früher Übersetzungsmanager) werden mehrsprachige Universen definiert und die Übersetzung von Universen und anderen Berichts- und analytischen Ressourcen im CMS-Repository definiert.

Übersetzungsmanagement-Tool:

- Übersetzt Universen oder Dokumente für ein mehrsprachiges Publikum.
- Definiert sprachbezogene Metadaten eines Dokuments und der entsprechenden Übersetzung. Generiert das externe XLIFF-Format und importiert XLIFF-Dateien mit den Übersetzungen.
- Zeigt die Struktur des zu übersetzenden Universums oder Dokuments an.
- Sie können die Metadaten über die Benutzeroberfläche oder ein externes Übersetzungstool übersetzen, indem Sie XLIFF-Dateien importieren und exportieren.
- Erstellt mehrsprachige Dokumente.

3.3.1.8 Datenföderations-Administrationstool

Das Datenföderations-Administrationstool (früher Data Federator) ist eine Rich-Client-Anwendung mit benutzerfreundlichen Funktionen zur Verwaltung des Datenföderations-Dienstes.

Der Datenföderations-Dienst ist in die BI-Plattform integriert und ermöglicht durch die Verteilung von Abfragen auf verschiedene Datenquellen die Erstellung von Universen mit mehreren Quellen. Darüber hinaus können Sie mit diesem Dienst Daten durch eine einzelne Datengrundlage föderieren.

Mit dem Datenföderations-Administrationstool können Sie Datenföderations-Abfragen optimieren und die Datenföderations-Abfrage-Engine zur bestmöglichen Leistung abstimmen.

Mit dem Datenföderations-Administrationstool können Sie folgende Aufgaben ausführen:

- Testen von SQL-Abfragen.
- Anzeigen von Optimierungsplänen, die genaue Informationen darüber enthalten, wie föderierte Abfragen auf die einzelnen Quellen verteilt werden.
- Berechnen von *Statistiken* und Festlegen von Systemparametern zur Feineinstellung der Datenföderations-Dienste und eine bestmögliche Leistung.
- Verwalten der Eigenschaften zur Steuerung der Abfragenausführung in jeder einzelnen Datenquelle auf Connector-Ebene.
- Überwachen von SQL-Abfragen, die aktuell ausgeführt werden.
- Den Verlauf ausgeführter Abfragen durchsuchen

3.3.1.9 Widgets für die BI-Plattform

Widgets sind Minianwendungen, die schnellen und einfachen Zugriff auf häufig verwendete Funktionen ermöglichen und visuelle Informationen auf Ihrem Desktop anzeigen. Mit Widgets für die BI-Plattform (früher BI

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Widgets) kann Ihre Organisation den Zugriff auf vorhandene BI-Inhalte (Business Intelligence) auf der BI-Plattform bereitstellen, oder Sie können Web-Dynpro-Anwendungen, die als XBCML-Widgets (Extensible Business Client Markup Language) registriert sind, auf SAP NetWeaver Application Servern als Desktop-Widgets hinzufügen.

Die XBCML-Widgets werden mit SAP Web Dynpro Flex Client auf dem Desktop des Benutzers gerendert. SAP Web Dynpro Flex Client ist eine auf Adobe Flex, das zum Rendern von Widgets verwendet wird, basierende Rendering-Engine. Einzelheiten zum Konfigurieren von Web Dynpro-Anwendungen finden Sie unter dem Thema *Aktivieren von Widgets auf dem SAP NetWeaver Application Server* im *Widgets für SAP BusinessObjects-Benutzerhandbuch.*

> **Hinweis**
>
> Die SAP Web Dynpro Flex Client-Unterstützung für XBCML-Widgets ist ab Release 7.0 EhP2 SP3 verfügbar. Die Flex Client-Warteschlangenunterstützung ist auf Flex Client-Probleme beschränkt, die in VBCML-Widgets in den angegebenen Releases auftreten.

Mit Widgets können Sie nach vorhandenen Inhalten suchen, z.B. nach Web-Intelligence-Dokumenten, Dashboards-Modellen sowie Web-Dynpro-Anwendungen, und die Informationen anschließend auf dem Desktop einfügen, damit sie bei Bedarf sofort verfügbar sind.

Als Widget übernehmen die Inhalte folgende Funktionen aus dem Widget-Framework:

- Benutzergesteuerte Größe und Positionierung
- Automatische Regenerierung
- Optionale Einstellung als oberstes Anwendungsfenster
- Umfassende BI-Plattform-Sicherheit (nur für Web-Intelligence-Berichtsteile und Dashboards-Modelle)
- Gespeicherte Anzeige
- Gespeicherter Datenkontextstatus (nur Web-Intelligence-Berichtsteile)
- Web-Intelligence-OpenDocument-Verknüpfungen zu detaillierten Berichten (nur Web-Intelligence-Berichte)
- Registerkarten-Ansichten (nur Dashboards-Modelle)

3.3.2 Installiert mit SAP BusinessObjects Business Intelligence

3.3.2.1 Central Configuration Manager (CCM)

Der Central Configuration Manager (CCM) ist ein Tool für die Fehlerbehebung auf Servern und die Knotenverwaltung, das in zwei Varianten bereitgestellt wird. In einer Microsoft Windows-Umgebung können Sie mit dem CCM lokale Server und Remoteserver über die grafische Benutzeroberfläche oder über eine Befehlszeile verwalten. In einer UNIX-Umgebung können Sie mit dem CCM-Shell-Skript (`ccm.sh`) Server über eine Befehlszeile verwalten.

Sie können mit dem CCM Knoten erstellen und konfigurieren und den Webanwendungsserver starten oder stoppen, sofern es sich um den gebündelten, standardmäßigen Tomcat-Webanwendungsserver handelt. Unter Windows ermöglicht er Ihnen auch die Konfiguration von Netzwerkparametern, z.B. der SSL-Verschlüsselung (Secure Socket Layer). Diese Parameter gelten für alle Server innerhalb eines Knotens.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Die meisten Serververwaltungsaufgaben werden nun über die CMC und nicht im CCM ausgeführt. Ab sofort wird der CCM für die Fehlerbehebung und die Knotenkonfiguration verwendet.

3.3.2.2 Upgrade-Management-Tool

Das Upgrade-Management-Tool (früher eine Funktion des Import-Assistenten) wird als Teil der BI-Plattform installiert und führt Administratoren durch den Prozess des Imports von Benutzern, Gruppen und Ordnern aus früheren Versionen der BI-Plattform. Außerdem können mit dem Tool Ereignisse, Servergruppen, Repository-Objekte und Kalender importiert und aktualisiert werden.

Informationen über das Upgrade von einer früheren Version der BI-Plattform finden Sie im *Aktualisierungshandbuch für SAP BusinessObjects Business Intelligence*.

3.3.2.3 Repository Diagnostic Tool

Mit dem Repository Diagnostic Tool (RDT) können Sie Inkonsistenzen zwischen der CMS-Systemdatenbank und dem FRS-Dateispeicher (File Repository Server) suchen, diagnostizieren und reparieren.

Das RDT kann zudem den Reparaturstatus und durchgeführte Aktionen melden. Um die Synchronisierung zwischen dem Dateisystem und der Datenbank zu ermitteln, sollte RDT erst verwendet werden, nachdem der Benutzer ein Hot-Backup ausgeführt hat. Das Tool kann auch nach einer Wiederherstellung und vor dem Start der BI-Plattform-Dienste verwendet werden. Der Benutzer kann einen Grenzwert für die Anzahl der Fehler festlegen, die das RDT vor Ende der Ausführung findet und repariert.

3.3.3 Separat erhältliche Anwendungen

3.3.3.1 SAP BusinessObjects Analysis, Edition für Microsoft Office

SAP BusinessObjects Analysis, Edition für Microsoft Office ist eine hervorragende Alternative zu Business Explorer (BEx) und bietet Business-Analysten die Möglichkeit, mehrdimensionale OLAP-Daten (Online Analytical Processing) zu durchsuchen.

Analysten können Geschäftsfragen rasch beantworten und ihre Auswertung und den Arbeitsbereich anschließend gemeinsam mit anderen als *Analysen* nutzen.

Mit SAP BusinessObjects Analysis, Edition für Microsoft Office können Analysten Folgendes ausführen:

- Aufdecken von Trends, Ausreißern und Details in den Finanzsystemen ohne die Hilfe eines Datenbankadministrators.
- Beantwortung von Geschäftsfragen beim effizienten Anzeigen großer oder kleiner mehrdimensionaler Datensätze.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Zugriff auf sämtliche OLAP-Datenquellen innerhalb der Organisation und gemeinsame Nutzung der Ergebnisse über eine einfache, intuitiv zu bedienende Oberfläche.
- Zugriff auf mehrere unterschiedliche OLAP-Quellen in derselben Analyse für eine umfassende Übersicht über das Unternehmen und die Art und Weise, wie sich die verschiedenen Trends gegenseitig beeinflussen.
- Abfragen, analysieren, vergleichen und prognostizieren von Einflussfaktoren.
- Verwendung einer breit gefächerten Auswahl von Geschäfts- und Zeitberechnungen.

3.3.3.2 SAP Crystal Reports

Mit der Software SAP Crystal Reports können Benutzer interaktive Berichte aus einer Datenquelle erstellen.

3.3.3.3 SAP BusinessObjects Dashboards

SAP BusinessObjects Dashboards (vormals Xcelsius) ist ein Tool zur Datenvisualisierung und zur Erstellung von dynamischen, interaktiven Dashboards. Daten und Formeln werden importiert oder direkt in ein eingebettetes Excel-Arbeitsblatt eingegeben. Eine Flash-Oberfläche stellt einen Grafikbereich bereit, in dem eine Vielzahl von Analysen und Dashboards angezeigt werden können.

Die Daten lassen sich dynamisch aus der BI-Plattform aktualisieren und dann in viele unterschiedliche Formate exportieren, sodass Nutzer der Daten diese in Standardformaten wie PowerPoint, PDF oder Flash anzeigen können.

3.3.3.4 SAP BusinessObjects Explorer

SAP BusinessObjects Explorer ist eine Datensuchanwendung, die anhand einer leistungsstarken Suchfunktion schnell und direkt Antworten auf Geschäftsfragen aus Ihren Unternehmensdaten abruft.

Wenn Sie SAP BusinessObjects Explorer installieren, werden folgende Server zum Central Configuration Manager (CCM) und zur Central Management Console (CMC) der BI-Plattform hinzugefügt:

- Explorer-Masterserver: Verwaltet alle Explorer-Server.
- Explorer-Indizierungsserver: Ermöglicht und verwaltet das Indizieren von Information-Space-Daten und Metadaten.
- Explorer-Suchserver: Verarbeitet Suchanfragen und gibt die Ergebnisse zurück.
- Explorer-Explorationsserver: Ermöglicht und verwaltet die Funktionen zur Information-Space-Exploration und -Analyse einschließlich der Datensuche, Filterung und Aggregation.

3.3.4 Webanwendungsclients

Webanwendungsclients befinden sich auf einem Webanwendungsserver. Der Zugriff auf sie erfolgt über einen Client-Webbrowser. Webanwendungen werden bei der Installation der BI-Plattform automatisch implementiert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Auf Webanwendugen kann einfach über einen Webbrowser zugegriffen werden. Die Kommunikation erfolgt mit SSL-Verschlüsselung, wenn Sie planen, Benutzern den Zugriff von außerhalb des Unternehmens zu ermöglichen.

Java-Webanwendungen können Sie auch nach der Erstinstallation neu konfigurieren oder implementieren, indem Sie das gebündelte WDeploy-Befehlszeilenwerkzeug verwenden, mit dem Sie Webanwendungen auf zwei verschiedene Arten auf einem Webanwendungsserver implementieren können:

1. Eigenständiger Modus

   Alle Webanwendungsressourcen werden auf einem Webanwendungsserver implementiert, der sowohl dynamische als auch statische Inhalte verarbeitet. Diese Vorgehensweise eignet sich für kleine Installationen.
2. Split-Modus

   Der statische Inhalt der Webanwendung (HTML, Bilder, CSS) wird auf einem dedizierten Webserver implementiert, während der dynamische Inhalt (JSPs) auf einem Webanwendungsserver implementiert wird. Diese Vorgehensweise eignet sich für größere Installationen, die davon profitieren, dass der Webanwendungsserver von der Verwaltung statischer Webinhalte befreit wird.

Weitere Informationen zu WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.

3.3.4.1 Central Management Console (CMC)

Die Central Management Console (CMC) ist ein webbasiertes Tool, mit dem Sie administrative Aufgaben (z.B. Benutzer-, Inhalt- und Serververwaltung) ausführen und Sicherheitseinstellungen konfigurieren können. Da es sich bei der CMC um eine webbasierte Anwendung handelt, können Sie alle administrativen Aufgaben in einem Webbrowser auf jedem Computer ausführen, der eine Verbindung mit dem Webanwendungsserver herstellen kann.

Verwaltungseinstellungen können nur von Mitgliedern der Gruppe "Administratoren" geändert werden, es sei denn, anderen Benutzern werden diese Rechte explizit gewährt. In der CMC können Rollen zugewiesen werden, um Benutzerrechte für die Ausführung kleinerer administrativer Aufgaben zu gewähren, z.B. Verwalten der Benutzer in Ihrer Gruppe oder Verwalten von Berichten in Ordnern, die Ihrem Team gehören.

3.3.4.2 BI-Launchpad

BI-Launchpad (früher InfoView) ist eine webbasierte Schnittstelle, auf die Endbenutzer zugreifen, um veröffentlichte BI-Berichte anzuzeigen, zeitgesteuert zu verarbeiten und zu verfolgen. BI-Launchpad ist in der Lage, auf jeden Business-Intelligence-Dokumenttyp zuzugreifen, diesen zu exportieren und damit zu interagieren, einschließlich Berichte, Analysen und Dashboards.

Mit BI-Launchpad können Benutzer Folgendes durchführen:

- Navigation und Suche im BI-Inhalt
- Zugriff auf BI-Inhalt (Erstellen, Bearbeiten, Anzeigen)
- Zeitgesteuerte Verarbeitung und Veröffentlichung von BI-Inhalt

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3.3.4.3 BI-Arbeitsbereiche

Mithilfe von BI-Arbeitsbereichen (früher Dashboard Builder) können Sie Ihre Geschäftsaktivitäten und Ihre Leistung verfolgen. Hierzu kommen Module (Vorlagen für Daten) und BI-Arbeitsbereiche (Anzeige von Daten in einem oder mehreren Modulen) zum Einsatz. Module und BI-Arbeitsbereiche stellen die nötigen Informationen bereit, die zum Anpassen von Geschäftsregeln an wechselnde Bedingungen erforderlich sind. Die BI-Arbeitsbereiche und -Module für die Verwaltung helfen Ihnen dabei, wichtige Geschäftsdaten zu verfolgen und zu analysieren. Diese Produkte vereinfachen auch die Entscheidungsfindung und Analyseprozesse innerhalb von Gruppen, indem sie integrierte Funktionen für Zusammenarbeit und Workflows bieten. BI-Arbeitsbereiche stellen die folgenden Funktionen bereit:

- Auf Registerkarten basierende Suche
- Seitenerstellung: Verwalten von BI-Arbeitsbereichen und -Modulen
- Anwendungs-Generator mit Zeigen- und Klicken-Funktionen
- Inhaltsverknüpfung zwischen Modulen für eine ausführliche Datenanalyse

> **Hinweis**
>
> BI-Arbeitsbereiche sind ein integraler Bestandteil der BI-Launchpad-Anwendung. Zur Nutzung der Funktionen von BI-Arbeitsbereichen erwerben Sie daher eine Lizenz für SAP BusinessObjects Business Intelligence, in der BI-Launchpad als Teil der Softwarelizenzvereinbarung enthalten ist.

3.3.4.4 Berichtsviewer

Jeder Berichtsviewer unterstützt eine andere Plattform und einen anderen Browser. Die Einstellungen können in BI-Launchpad und der Central Management Console (CMC) festgelegt werden. Zur Auswahl stehen zwei Viewer-Kategorien:

- Zero-Client-Berichtsviewer (DHTML-Viewer)

  Zero-Client-Berichtsviewer befinden sich auf dem Webanwendungsserver. Wenn ein Benutzer einen Bericht anfordert, ruft der Webanwendungsserver die Berichtsseiten von der BI-Plattform ab und erstellt DHTML-Seiten, die im Webbrowser angezeigt werden. Um den Zero-Client-Berichtsviewer (DHTML) zu wählen, wählen Sie **Einstellungen** > **Crystal Reports** > **Web (kein Download erforderlich)**.
- Clientseitige Berichtsviewer (Active X-Viewer, Java-Viewer)

  Clientseitige Berichtsviewer werden mithilfe des Browsers des Benutzers heruntergeladen und installiert. Bei Anforderung eines Berichts durch einen Benutzer verarbeitet der Anwendungsserver die Anforderung und ruft die Berichtsseiten von der BI-Plattform ab. Der Webanwendungsserver übergibt die Berichtsseiten anschließend an den clientseitigen Viewer, der diese verarbeitet und direkt im Webbrowser anzeigt. Um einen clientseitigen Berichtsviewer zu wählen, wählen Sie **Einstellungen** > **Crystal Reports** > **Web ActiveX (ActiveX erforderlich)** oder **Web Java (Java erforderlich)** aus.

Alle Berichtsviewer verarbeiten Berichtsanforderungen und stellen Berichtsseiten dar, die im Webbrowser angezeigt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Für den Online-Zugriff auf Crystal Reports über die Central Management Console (CMC) wird empfohlen, den Standard-DHTML-Webviewer zu verwenden. Vermeiden Sie, den veralteten Java-Viewer zu verwenden, da dieser nicht die gleichen Funktionen wie der DHTML-Viewer bietet.

Weitere Informationen zur Unterstützung von Funktionen oder Plattformen durch dieBerichtsviewer finden Sie im *Benutzerhandbuch für BI-Launchpad*, im *Report Application Server .NET SDK Developer Guide* oder im *Entwicklerhandbuch für das Viewer-Java-SDK*.

3.3.4.5 SAP BusinessObjects Web Intelligence

SAP BusinessObjects Web Intelligence ist ein webbasiertes Tool, das Abfrage-, Berichterstellungs- und Analysefunktionen für relationale Datenquellen in einem einzigen webbasierten Produkt liefert.

Sie ermöglicht Benutzern, Berichte zu erstellen, Ad-hoc-Analysen auszuführen, Daten zu analysieren und Berichte in einer Drag-and-Drop-Oberfläche zu formatieren. Web Intelligence kaschiert die Komplexität zugrunde liegender Datenquellen.

Berichte können mithilfe von SAP BusinessObjects Live Office in einem unterstützten Webportal oder in Microsoft Office-Anwendungen veröffentlicht werden.

3.3.4.6 SAP BusinessObjects Analysis, Edition für OLAP

SAP BusinessObjects Analysis, Edition für OLAP (früher Voyager) ist ein OLAP-Tool ((Online Analytical Processing) im BI-Launchpad-Portal, mit dem mehrdimensionale Daten bearbeitet werden können. Darüber hinaus kann es Informationen aus unterschiedlichen OLAP-Datenquellen in einem einzigen Arbeitsbereich kombinieren. Zu den unterstützten OLAP-Providern gehören SAP BW und Microsoft Analysis Services.

Der OLAP-Funktionssatz von Analysis kombiniert Elemente von SAP Crystal Reports (direkter Datenzugriff auf OLAP-Cubes zur Produktionsberichterstellung) und von SAP BusinessObjects Web Intelligence (analytische Ad-hoc-Berichterstellung mit Universen aus OLAP-Datenquellen). Er bietet eine Reihe von Geschäfts- und Zeitberechnungen und umfasst Features wie Zeitspannen, mit denen die Analyse von OLAP-Daten so einfach wie möglich gestaltet wird.

> **Hinweis**
>
> Die Webanwendung von Analysis, Edition für OLAP, ist nur als Java-Webanwendung verfügbar. Für .NET ist keine entsprechende Anwendung verfügbar.

3.3.4.7 SAP BusinessObjects Mobile

Mit SAP BusinessObjects Mobile können Ihre Benutzer über ein drahtloses Gerät remote auf die gleichen BI-Berichte, -Metriken und -Echtzeitdaten zugreifen wie über den Desktop-Client. Der Inhalt ist für mobile Geräte

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

optimiert, damit die Benutzer auf einfache Weise und ohne zusätzliches Training auf vertraute Berichte zugreifen, in diesen navigieren und sie analysieren können.

Mit SAP BusinessObjects Mobile bleiben Führungskräfte und Mitarbeiter immer auf dem neuesten Stand. So können sie Entscheidungen stets aufgrund der neuesten Informationen treffen. Vertriebs- und Außendienstmitarbeiter liefern die richtigen Kunden-, Produkt- und Auftragsinformationen wo und wann diese benötigt werden.

SAP BusinessObjects Mobile unterstützt eine breite Palette von mobilen Geräten, darunter BlackBerry, Windows Mobile und Symbian.

Informationen zur Mobile-Installation, -Konfiguration und -Implementierung finden Sie im *Installations- und Implementierungshandbuch für SAP BusinessObjects Mobile*. Informationen zur Verwendung von SAP BusinessObjects Mobile finden Sie im *Benutzerhandbuch für SAP BusinessObjects Mobile*.

3.4 Prozess-Workflows

Bei der Ausführung von Aufgaben wie der Anmeldung und der zeitgesteuerte Verarbeitung oder Anzeige von Berichten fließen Informationen durch das System und die Server kommunizieren miteinander. Im folgenden Abschnitt werden einige Prozessabläufe beschrieben, so wie sie in der BI-Plattform vorkommen könnten.

Um zusätzliche Prozess-Workflows mit visuellen Hilfsmitteln anzuzeigen, sehen Sie sich die offiziellen Produktlernprogramme von SAP BusinessObjects Business Intelligence 4.x unter folgender Adresse an: *http://scn.sap.com/docs/DOC-8292*

3.4.1 Start und Authentifizierung

3.4.1.1 Anmelden bei der BI-Plattform

Dieser Workflow beschreibt die Anmeldung eines Benutzers an einer Webanwendung der BI-Plattform über einen Webbrowser. Dieser Workflow lässt sich auf Webanwendungen wie BI-Launchpad und der Central Management Console (CMC) übertragen.

1. Der Browser (Webclient) sendet die Anmeldeanforderung über den Webserver an den Webanwendungsserver, auf dem die Webanwendung ausgeführt wird.
2. Der Webanwendungsserver stellt fest, ob es sich bei der Anforderung um eine Anmeldeanforderung handelt. Der Webanwendungsserver sendet den Benutzernamen, das Kennwort und den Authentifizierungstyp zur Authentifizierung an den CMS.
3. Der CMS validiert den Benutzernamen und das Kennwort bezüglich der geeigneten Datenbank. In diesem Fall wird die Enterprise-Authentifizierung verwendet, und die Anmeldedaten werden bezüglich der CMS-Systemdatenbank authentifiziert.
4. Nach erfolgreicher Überprüfung erstellt der CMS eine Benutzersitzung im Arbeitsspeicher.
5. Der CMS sendet eine Antwort an den Webanwendungsserver, um ihm mitzuteilen, dass die Überprüfung erfolgreich war.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6. Der Webanwendungsserver generiert ein Anmeldetoken für die Benutzersitzung im Arbeitsspeicher. Im weiteren Verlauf dieser Sitzung verwendet der Webanwendungsserver das Anmeldetoken, um den Benutzer gegenüber dem CMS zu authentifizieren. Der Webanwendungsserver generiert die nächste, an den Webclient zu sendende Webseite.
7. Der Webanwendungsserver sendet die nächste Webseite an den Webserver.
8. Der Webanwendungsserver sendet die Webseite an den Webclient, auf dem sie im Browser des Benutzers gerendert wird.

3.4.1.2 Starten von SIA

Ein Server Intelligence Agent (SIA) kann so konfiguriert werden, dass er automatisch mit dem Hostbetriebssystem gestartet wird, oder kann manuell mit dem Central Configuration Manager (CCM) gestartet werden.

Ein SIA ruft von einem Central Management Server (CMS) Informationen über die von ihm verwalteten Server ab. Verwendet der SIA einen lokalen CMS, und wird dieser CMS nicht ausgeführt, startet der SIA den CMS. Verwendet ein SIA einen Remote-CMS, versucht er, eine Verbindung zum CMS herzustellen.

Nach dem Start eines SIA wird die folgende Reihe von Ereignissen ausgeführt.

1. Der SIA sucht einen CMS in seinem Cache.
   a) Wenn der SIA für den Start eines lokalen CMS konfiguriert und dieser nicht ausgeführt wird, startet der SIA den CMS in seinem Cache und stellt die Verbindung her.
   b) Wenn der SIA für die Verwendung eines CMS (lokal oder remote) konfiguriert ist, der ausgeführt wird, versucht er, eine Verbindung zum ersten CMS in seinem Cache herzustellen. Wenn der CMS gerade nicht verfügbar ist, versucht er, eine Verbindung zum nächsten CMS im Cache herzustellen. Wenn keiner der CMS im Cache verfügbar ist, wartet der SIA so lange, bis einer verfügbar wird.
2. Der CMS bestätigt die Identität des SIA, um dessen Gültigkeit sicherzustellen.
3. Nachdem der SIA die Verbindung zu einem CMS hergestellt hat, fordert er eine Liste der zu verwaltenden Server an.

   Hinweis

   Ein SIA speichert keine Informationen über die Server, die er verwaltet. Die Konfigurationsinformationen, die vorgeben, welcher Server von einem SIA verwaltet wird, sind in der CMS-Systemdatenbank gespeichert und werden vom SIA bei dessen Start vom CMS abgerufen.

4. Der CMS fragt eine Liste der vom SIA verwalteten Server aus der CMS-Systemdatenbank ab. Außerdem wird die Konfiguration der einzelnen Server abgerufen.
5. Der CMS gibt die Liste der Server und ihre Konfiguration an den SIA zurück.
6. Der SIA startet jeden für den automatischen Start konfigurierten Server mit der entsprechenden Konfiguration und überwacht seinen Status. Alle vom SIA gestarteten Server sind so konfiguriert, dass sie den gleichen CMS wie der SIA verwenden.

   Sämtliche nicht für den automatischen Start mit dem SIA konfigurierten Server werden nicht gestartet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3.4.1.3 Herunterfahren von SIA

Der Server Intelligence Agent (SIA) stoppt automatisch, wenn Sie das Host-Betriebssystem herunterfahren. Sie können den SIA auch manuell im Central Configuration Manager (CCM) stoppen.

Wenn der SIA heruntergefahren wird, werden folgende Schritte durchgeführt.

Der SIA benachrichtigt den CMS, dass er heruntergefahren wird.

a) Falls der SIA gestoppt wird, weil das Betriebssystem des Hosts heruntergefahren wird, fordert der SIA seine Server zum Stopp auf. Die Beendigung von Servern, die nicht innerhalb von 25 Sekunden gestoppt werden, wird erzwungen.

b) Wenn der SIA manuell gestoppt wird, wartet er, bis der verwaltete Server mit der Verarbeitung vorhandener Aufträge fertig ist. Die verwalteten Server akzeptieren keine neuen Aufträge. Wenn alle Aufträge abgeschlossen sind, werden die Server gestoppt. Nachdem alle Server gestoppt wurden, wird auch der SIA gestoppt.

Beim erzwungenen Herunterfahren sendet der SIA eine Aufforderung zum sofortigen Stoppen an alle verwalteten Server.

3.4.2 Programmobjekte

3.4.2.1 Festlegen der zeitgesteuerten Verarbeitung für ein Programmobjekt

Dieser Workflow beschreibt, wie ein Benutzer ein Programmobjekt zeitgesteuert verarbeitet, sodass es zu einem späteren Zeitpunkt von einer Webanwendung, z.B. der Central Management Console (CMC) oder dem BI-Launchpad, ausgeführt wird.

1. Der Benutzer sendet die Anforderung zur zeitgesteuerten Verarbeitung vom Webclient über den Webserver an den Webanwendungsserver.
2. Der Webanwendungsserver interpretiert die Anforderung und stellt fest, ob es sich um eine Anforderung zur zeitgesteuerten Verarbeitung handelt. Der Webanwendungsserver sendet den Zeitpunkt für die zeitgesteuerte Verarbeitung, Werte für die Datenbankanmeldung, Parameterwerte, Ziel und Format an den angegebenen Central Management Server (CMS).
3. Der CMS stellt sicher, dass der Anwender zur zeitgesteuerten Verarbeitung des Objekts berechtigt ist. Wenn der Benutzer über die erforderlichen Rechte verfügt, fügt der CMS der CMS-Systemdatenbank einen neuen Datensatz hinzu und fügt die Instanz zu seiner Liste der ausstehenden Zeitsteuerungen hinzu.
4. Der CMS sendet eine Antwort an den Webanwendungsserver, die beinhaltet, dass der Zeitsteuerungsvorgang erfolgreich ausgeführt wurde.
5. Der Webanwendungsserver generiert die nächste HTML-Seite und sendet sie über den Webserver an den Webclient.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3.4.2.2 Ausführen eines zeitgesteuert verarbeiteten Programmobjekts

Mit diesem Workflow wird der Prozess eines zeitgesteuert verarbeiteten Programmobjekts beschrieben, das zu einer eingeplanten Zeit ausgeführt wird. Der Adaptive Job Server und der Input File Repository Server müssen ebenfalls ausgeführt werden.

> **Hinweis**
>
> Für diesen Workflow ist es erforderlich, dass CMS, Adaptive Job Server und Input File Repository Server ausgeführt werden.

1. Der Central Management Server (CMS) prüft die CMS-Systemdatenbank, um festzustellen, ob momentan ein zeitgesteuert verarbeiteter SAP-Crystal-Reports-Bericht ausgeführt werden muss.
2. Kurz vor der zeitgesteuerten Verarbeitung sucht der CMS einen verfügbaren Dienst zur zeitgesteuerten Verarbeitung von Programmen, der auf einem Adaptive Job Server ausgeführt wird. Der CMS sendet die Auftragsinformationen an den Dienst zur zeitgesteuerten Verarbeitung von Programmen.
3. Der Dienst zur zeitgesteuerten Verarbeitung von Programmen kommuniziert mit dem Input File Repository Server (FRS), um das Programmobjekt abzurufen.

   > **Hinweis**
   >
   > Dieser Schritt setzt zudem die Kommunikation mit dem CMS voraus, damit die erforderlichen Server und Objekte gesucht werden können.

4. Der Dienst zur zeitgesteuerten Verarbeitung von Programmen startet das Programm.
5. Der Dienst zur zeitgesteuerten Verarbeitung von Programmen aktualisiert regelmäßig den Auftragsstatus auf dem CMS. Der aktuelle Status ist "Verarbeitung".
6. Der Dienst zur zeitgesteuerten Verarbeitung von Programmen sendet eine Protokolldatei an den Output FRS. Der Output FRS benachrichtigt den Dienst zur zeitgesteuerten Verarbeitung von Programmen durch Senden einer Objektprotokolldatei darüber, dass das Objekt erfolgreich zeitgesteuert verarbeitet wurde.

   > **Hinweis**
   >
   > Dieser Schritt setzt zudem die Kommunikation mit dem CMS voraus, damit die erforderlichen Server und Objekte gesucht werden können.

7. Der Dienst zur zeitgesteuerten Verarbeitung von Programmen aktualisiert den Auftragsstatus auf dem CMS. Der aktuelle Status ist "Erfolg".
8. Der CMS aktualisiert den Auftragsstatus in seinem Arbeitsspeicher und schreibt die Instanzinformationen dann in die CMS-Systemdatenbank.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3.4.3 Crystal Reports

3.4.3.1 Anzeigen einer zwischengespeicherten SAP-Crystal-Reports-Berichtsseite

Dieser Workflow beschreibt, wie ein Benutzer eine Seite in einem SAP-Crystal-Reports-Bericht (z.B. vom Bericht-Viewer in BI-Launchpad) anfordert, wenn die Berichtsseite bereits auf einem Cache Server vorliegt. Dieser Workflow gilt sowohl für SAP Crystal Reports 2013 als auch für SAP Crystal Reports für Enterprise.

> **Hinweis**
>
> Für diesen Workflow müssen der CMS und der Crystal Reports Cache Server ausgeführt werden.

1. Der Webclient sendet in einer URL eine Anforderung zur Anzeige über den Webserver an den Webanwendungsserver.
2. Der Webanwendungsserver interpretiert die Anforderung und stellt fest, dass es sich um eine Anforderung zum Anzeigen einer ausgewählten Berichtsseite handelt. Der Webanwendungsserver sendet eine Anforderung an den Central Management Server (CMS), um sicherzustellen, dass der Benutzer über ausreichende Rechte zum Anzeigen des Berichts verfügt.
3. Der CMS prüft die CMS-Systemdatenbank, um festzustellen, ob der Benutzer über ausreichende Rechte zum Anzeigen des Berichts verfügt.
4. Der CMS sendet eine Antwort an den Webanwendungsserver, um zu bestätigen, dass der Benutzer über die ausreichende Rechte zum Anzeigen des Berichts verfügt.
5. Der Webanwendungsserver sendet eine Anforderung an den Crystal Reports Cache Server, in der die erste Seite des Berichts (`.epf`-Datei) angefordert wird.
6. Der Crystal Reports Cache Server stellt fest, ob die angeforderte `.epf`-Datei im Cache-Verzeichnis vorhanden ist. In diesem Beispiel wird die `.epf`-Datei gefunden.
7. Der Crystal Reports Cache Server sendet die angeforderte Seite an den Webanwendungsserver.
8. Der Webanwendungsserver sendet die Seite über den Webserver an den Webclient, auf dem sie gerendert und angezeigt wird.

3.4.3.2 Anzeigen einer nicht zwischengespeicherten Seite eines SAP-Crystal-Reports-2013-Berichts

Dieser Workflow beschreibt, wie ein Benutzer eine Seite in einem SAP-Crystal-Reports-2013-Bericht (z. B. vom Berichtsviewer in BI-Launchpad) anfordert, wenn die Datei noch nicht auf einem Cache Server vorhanden ist.

> **Hinweis**
>
> Für diesen Workflow ist es erforderlich, dass CMS, Crystal Reports Cache Server, Crystal Reports 2013 Processing Server und Output File Repository Server ausgeführt werden.

1. Der Benutzer sendet die Anzeigeanforderung über den Webserver an den Webanwendungsserver.
2. Der Webanwendungsserver interpretiert die Anforderung, bestimmt, dass es sich um eine Anforderung zum Anzeigen einer bestimmten Berichtsseite handelt und sendet eine Anfrage an den Central Management

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Server (CMS), um sicherzustellen, dass der Benutzer über die erforderlichen Berechtigungen zum Anzeigen des Berichts verfügt.

3. Der CMS prüft die CMS-Systemdatenbank, um festzustellen, ob der Benutzer über ausreichende Rechte zum Anzeigen des Berichts verfügt.
4. Der CMS sendet eine Antwort an den Webanwendungsserver, um zu bestätigen, dass der Benutzer über die ausreichende Rechte zum Anzeigen des Berichts verfügt.
5. Der Webanwendungsserver sendet eine Anforderung an den Crystal Reports Cache Server, in der die erste Seite des Berichts (`.epf`-Datei) angefordert wird.
6. Der Crystal Reports Cache Server stellt fest, ob die angeforderte Datei im Cacheverzeichnis vorhanden ist. In diesem Beispiel befindet sich die angeforderte `.epf`-Datei nicht im Cacheverzeichnis.
7. Der Crystal Reports Cache Server sendet die Anforderung an den Crystal Reports 2013 Processing Server.
8. Der Crystal Reports 2013 Processing Server fragt die erforderliche Berichtsinstanz vom Output File Repository Server (FRS) ab, und der Output FRS sendet die angeforderte Berichtsinstanz an den Crystal Reports 2013 Processing Server.

   Hinweis

   Dieser Schritt setzt zudem die Kommunikation mit dem CMS voraus, damit die erforderlichen Server und Objekte gesucht werden können.

9. Der Crystal Reports 2013 Reporting Server öffnet die Berichtsinstanz und überprüft, ob der Bericht Daten enthält.

   Der Crystal Reports 2013 Reporting Server stellt fest, ob der Bericht Daten enthält, und erstellt die `.epf`-Datei für die angeforderte Berichtsseite. Dazu muss keine Verbindung mit der Produktionsdatenbank hergestellt werden.
10. Der Crystal Reports 2013 Processing Server sendet die `.epf`-Datei an den Crystal Reports Cache Server.
11. Der Crystal Reports Cache Server schreibt die `.epf`-Datei in das Cache-Verzeichnis.
12. Der Crystal Reports Cache Server sendet die angeforderte EPF-Seite an den Webanwendungsserver.
13. Der Webanwendungsserver sendet die Seite über den Webserver an den Webclient, auf dem sie gerendert und angezeigt wird.

3.4.3.3 Anzeigen eines SAP-Crystal-Reports-2013-Berichts auf Abruf

Mit diesem Workflow wird der Prozess beschrieben, bei dem ein Benutzer eine Berichtsseite von SAP Crystal Reports 2013 auf Abruf anfordert, um die aktuellen Daten anzuzeigen, beispielsweise aus dem Bericht-Viewer im BI-Launchpad.

Hinweis

Für diesen Workflow ist es erforderlich, dass CMS, Crystal Reports Cache Server, Crystal Reports 2013 Processing Server und Input File Repository Server ausgeführt werden.

1. Der Benutzer sendet die Anzeigeanforderung über den Webserver an den Webanwendungsserver.
2. Der Webanwendungsserver interpretiert die Anforderung und stellt fest, dass es sich um eine Anforderung zum Anzeigen einer ausgewählten Berichtsseite handelt. Der Webanwendungsserver sendet eine

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Anforderung an den Central Management Server (CMS), um sicherzustellen, dass der Benutzer über ausreichende Rechte zum Anzeigen des Berichts verfügt.

3. Der CMS prüft die CMS-Systemdatenbank, um festzustellen, ob der Benutzer über ausreichende Rechte zum Anzeigen des Berichts verfügt.
4. Der CMS sendet eine Antwort an den Webanwendungsserver, um zu bestätigen, dass der Benutzer über die ausreichende Rechte zum Anzeigen des Berichts verfügt.
5. Der Webanwendungsserver sendet eine Anforderung an den Crystal Reports Cache Server, in der die erste Seite des Berichts (`.epf`-Datei) angefordert wird.
6. Der Crystal Reports Cache Server überprüft, ob die Seite bereits vorhanden ist. Der Crystal Reports Cache Server sendet eine Anforderung zum Generieren der Seite an den Crystal Reports 2013 Processing Server, es sei denn, der Bericht erfüllt die Bedingungen für die Freigabe von Berichten auf Abruf (innerhalb einer festgelegten Zeit einer anderen Auf-Abruf-Anforderung, Datenbankanmeldung oder anderer Parameter).
7. Der Crystal Reports 2013 Processing Server fordert das Berichtsobjekt vom Input File Repository Server (FRS) an. Der Input FRS übermittelt eine Kopie des Objekts in einem Datenstream an den Crystal Reports 2013 Processing Server.

   Hinweis

   Dieser Schritt setzt zudem die Kommunikation mit dem CMS voraus, damit die erforderlichen Server und Objekte gesucht werden können.

8. Der Crystal Reports 2013 Processing Server öffnet den Bericht in seinem Arbeitsspeicher und prüft, ob er Daten enthält. In diesem Beispiel sind keine Daten im Berichtsobjekt enthalten, sodass der Crystal Reports 2013 Processing Server eine Verbindung mit der Datenquelle herstellt, um Daten abzurufen und den Bericht zu generieren.
9. Der Crystal Reports 2013 Processing Server sendet die Seite (`.epf`-Datei) an den Crystal Reports Cache Server. Der Crystal Reports Cache Server speichert eine Kopie der `.epf`-Datei in seinem Cache-Verzeichnis, wo sie für neue Anzeigeanforderungen zur Verfügung steht.
10. Der Crystal Reports Cache Server sendet die angeforderte Seite an den Webanwendungsserver.
11. Der Webanwendungsserver sendet die Seite über den Webserver an den Webclient, auf dem sie gerendert und angezeigt wird.

3.4.3.4 Festlegen einer zeitgesteuerten Verarbeitung für einen Crystal-Reports-Bericht

Dieser Workflow beschreibt, wie ein Benutzer einen SAP-Crystal-Reports-Bericht zeitgesteuert verarbeitet, sodass dieser zu einem späteren Zeitpunkt von einer Webanwendung, z.B. der Central Management Console (CMC) oder BI-Launchpad, ausgeführt wird. Dieser Workflow gilt sowohl für SAP Crystal Reports 2013 als auch für SAP Crystal Reports für Enterprise.

1. Der Webclient sendet in einer URL eine Anforderung zur zeitgesteuerten Verarbeitung über den Webserver an den Webanwendungsserver.
2. Der Webanwendungsserver interpretiert die URL-Anforderung und stellt fest, ob es sich bei der Anforderung um eine Anforderung zur zeitgesteuerten Verarbeitung handelt. Der Webanwendungsserver sendet den Zeitpunkt für die zeitgesteuerte Verarbeitung, Werte für die Datenbankanmeldung, Parameterwerte, Ziel und Format an den angegebenen Central Management Server (CMS).

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Der CMS stellt sicher, dass der Anwender zur zeitgesteuerten Verarbeitung des Objekts berechtigt ist. Wenn der Benutzer über die erforderlichen Rechte verfügt, fügt der CMS der CMS-Systemdatenbank einen neuen Datensatz hinzu. Der CMS fügt die Instanz außerdem der Liste ausstehender zeitgesteuerter Verarbeitungen hinzu.
4. Der CMS sendet eine Antwort an den Webanwendungsserver, um ihm mitzuteilen, dass der Vorgang der zeitgesteuerten Verarbeitung erfolgreich war.
5. Der Webanwendungsserver generiert die nächste HTML-Seite und sendet sie über den Webserver an den Webclient.

3.4.3.5 Ausführen von zeitgesteuert verarbeiteten SAP-Crystal-Reports-2013-Berichten

Dieser Workflow beschreibt, wie ein zeitgesteuert verarbeiteter SAP-Crystal-Reports-2013-Bericht zu einem geplanten Zeitpunkt ausgeführt wird.

1. Der Central Management Server (CMS) prüft die CMS-Systemdatenbank, um festzustellen, ob momentan ein zeitgesteuert verarbeiteter SAP-Crystal-Reports-Bericht ausgeführt werden muss.
2. Kurz vor der zeitgesteuerten Verarbeitung sucht der CMS (auf der Grundlage des Werts **Maximal zulässige Anzahl von Aufträgen**, der für jeden Adaptive Job Server konfiguriert wird) einen verfügbaren Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-2013-Berichten, der auf einem Adaptive Job Server ausgeführt wird. Der CMS sendet die Auftragsinformationen (Bericht-ID, Format, Ziel, Anmeldeinformationen, Parameter und Auswahlformeln) an den Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-2013-Berichten.
3. Der Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-2013-Berichten kommuniziert mit dem Input File Repository Server (FRS), um entsprechend der angeforderten Bericht-ID eine Berichtsvorlage zu erhalten.

   Hinweis

   Dieser Schritt setzt zudem die Kommunikation mit dem CMS voraus, damit die erforderlichen Server und Objekte gesucht werden können.

4. Der Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-2013-Berichten startet den JobChildserver-Prozess.
5. Der untergeordnete Prozess (JobChildserver) startet bei Empfang der Vorlage vom Input File Repository Server die Datei `ProcReport.dll`. Die Datei `ProcReport.dll` enthält alle Parameter, die vom CMS an den Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-2013-Berichten übergeben wurden.
6. `ProcReport.dll` startet die Datei `crpe32.dll`, die den Bericht in Übereinstimmung mit den übergebenen Parametern verarbeitet.
7. Während der Bericht noch immer von `crpe32.dll` verarbeitet wird, werden Datensätze gemäß Definition im Bericht aus der Datenquelle abgerufen.
8. Der Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-2013-Berichten aktualisiert regelmäßig den Auftragsstatus auf dem CMS. Der aktuelle Status ist "Verarbeitung".
9. Nachdem der Bericht in den Arbeitsspeicher des Diensts für die zeitgesteuerte Verarbeitung von Crystal-Reports-2013-Berichten kompiliert wurde, muss er in ein anderes Format, z. B. Portable Document Format (PDF), exportiert werden. Beim Export in das PDF-Format wird `crxfpdf.dll` verwendet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10. Der Bericht mit den gespeicherten Daten wird an den geplanten Ort (z.B. E-Mail) und danach an den Output FRS gesendet.

> **Hinweis**
>
> Dieser Schritt setzt zudem die Kommunikation mit dem CMS voraus, damit die erforderlichen Server und Objekte gesucht werden können.

11. Der Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-2013-Berichten aktualisiert den Auftragsstatus auf dem CMS. Der aktuelle Status ist "Erfolg".
12. Der CMS aktualisiert den Auftragsstatus in seinem Arbeitsspeicher und schreibt die Instanzinformationen dann in die CMS-Systemdatenbank.

3.4.4 Web Intelligence

3.4.4.1 Anzeigen eines SAP BusinessObjects Web-Intelligence-Dokuments auf Abruf

Mit diesem Workflow wird der Prozess beschrieben, bei dem ein Benutzer ein SAP-BusinessObjects-Web-Intelligence-Dokument auf Abruf anfordert, um die aktuellen Daten anzuzeigen, beispielsweise aus dem Web-Intelligence-Viewer im BI-Launchpad.

1. Ein Webbrowser sendet die Anzeigeanforderung über den Webserver an den Webanwendungsserver.
2. Der Webanwendungsserver interpretiert die Anforderung und stellt fest, dass es sich um eine Anforderung zum Anzeigen eines Web-Intelligence-Dokuments handelt. Der Webanwendungsserver sendet eine Anforderung an den Central Management Server (CMS), um sicherzustellen, dass der Benutzer über die erforderlichen Rechte zum Anzeigen des Dokuments verfügt.
3. Der CMS prüft die CMS-Systemdatenbank, um zu verifizieren, dass der Benutzer über die erforderlichen Rechte zum Anzeigen des Berichts verfügt.
4. Der CMS sendet eine Antwort an den Webanwendungsserver, um zu bestätigen, dass der Benutzer über die erforderlichen Rechte zur Anzeige des Dokuments verfügt.
5. Der Webanwendungsserver sendet eine Anforderung für das Dokument an den Web Intelligence Processing Server.
6. Der Web Intelligence Processing Server fordert einerseits das Dokument vom Input File Repository Server (FRS) und andererseits die Universumsdatei an, auf der das angeforderte Dokumente basiert. Die Universumsdatei enthält Informationen der Metadatenschicht, einschließlich der Sicherheit auf Zeilen- und auf Spaltenebene.
7. Der Input FRS sendet eine Kopie des Dokuments sowie die Universumsdatei, auf der das angeforderte Dokument basiert, in einem Datenstream an den Web Intelligence Processing Server.

> **Hinweis**
>
> Dieser Schritt setzt zudem die Kommunikation mit dem CMS voraus, damit die erforderlichen Server und Objekte gesucht werden können.

8. Die Web Intelligence Report Engine (auf dem Web Intelligence Processing Server) öffnet das Dokument im Arbeitsspeicher und startet die Datei `QT.dll` und einen Connection Server im Prozess.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9. Die Datei `QT.dll` generiert, validiert und regeneriert den SQL-Code und stellt eine Verbindung mit der Datenbank her, um die Abfrage auszuführen. Der Connectoin Server verwendet den SQL-Code, um die Daten aus der Datenbank auf die Report Engine zu laden, wo das Dokument verarbeitet wird.
10. Der Web Intelligence Processing Server sendet die angeforderte anzeigbare Dokumentseite an den Webanwendungsserver.
11. Der Webanwendungsserver sendet die Dokumentseite über den Webserver an den Webclient, wo sie gerendert und angezeigt wird.

3.4.4.2 Festlegen der zeitgesteuerten Verarbeitung für ein SAP-BusinessObjects-Web-Intelligence-Dokument

Dieser Workflow beschreibt, wie ein Benutzer ein Dokument von SAP BusinessObjects Web Intelligence zeitgesteuert verarbeitet, sodass es zu einem späteren Zeitpunkt von einer Webanwendung, z.B. der Central Management Console (CMC) oder von BI-Launchpad, ausgeführt wird.

1. Der Webclient sendet in einer URL eine Anforderung zur zeitgesteuerten Verarbeitung über den Webserver an den Webanwendungsserver.
2. Der Webanwendungsserver interpretiert die URL-Anforderung und stellt fest, ob es sich bei der Anforderung um eine Anforderung zur zeitgesteuerten Verarbeitung handelt. Der Webanwendungsserver sendet den Zeitpunkt für die zeitgesteuerte Verarbeitung, Werte für die Datenbankanmeldung, Parameterwerte, Ziel und Format an den angegebenen Central Management Server (CMS).
3. Der CMS stellt sicher, dass der Anwender zur zeitgesteuerten Verarbeitung des Objekts berechtigt ist. Wenn der Benutzer über die erforderlichen Rechte verfügt, fügt der CMS der CMS-Systemdatenbank einen neuen Datensatz hinzu. Der CMS fügt die Instanz außerdem der Liste ausstehender zeitgesteuerter Verarbeitungen hinzu.
4. Der CMS sendet eine Antwort an den Webanwendungsserver, um ihm mitzuteilen, dass der Vorgang der zeitgesteuerten Verarbeitung erfolgreich war.
5. Der Webanwendungsserver generiert die nächste HTML-Seite und sendet sie über den Webserver an den Webclient.

3.4.4.3 Ausführen eines zeitgesteuert verarbeiteten Dokuments von SAP BusinessObjects Web Intelligence

Dieser Workflow beschreibt, wie ein zeitgesteuert verarbeitetes Dokument von SAP BusinessObjects Web Intelligence zu einem geplanten Zeitpunkt ausgeführt wird.

1. Der Central Management Server (CMS) überprüft die CMS-Systemdatenbank, um festzustellen, ob die zeitgesteuerte Ausführung eines Web-Intelligence-Dokuments geplant ist.
2. Kurz vor der zeitgesteuerten Verarbeitung sucht der CMS einen verfügbaren Web-Intelligence-Dienst für zeitgesteuerte Verarbeitung, der auf einem Adaptive Job Server ausgeführt wird. Der CMS sendet die Anforderung der zeitgesteuerten Verarbeitung und alle zugehörigen Informationen an den Web-Intelligence-Dienst für zeitgesteuerte Verarbeitung.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Der Web-Intelligence-Dienst für zeitgesteuerte Verarbeitung sucht auf der Grundlage des Werts **Maximale Verbindungen**, der für jeden Web Intelligence Processing Server konfiguriert wird, einen verfügbaren Web Intelligence Processing Server.
4. Der Web Intelligence Processing Server ermittelt den Speicherort des Input File Repository Servers (FRS), auf dem sich das Dokument und die dem Dokument zugrunde liegende Metalayer-Datei des Universums befinden. Der Web Intelligence Processing Server fordert daraufhin das Dokument vom Input FRS an. Der Input FRS sucht das Web Intelligence-Dokument sowie die Universumsdatei, auf der das Dokument basiert, und sendet diese in einem Datenstream an den Web Intelligence Processing Server.

   Hinweis

   Dieser Schritt setzt zudem die Kommunikation mit dem CMS voraus, damit die erforderlichen Server und Objekte gesucht werden können.
5. Das Web Intelligence-Dokument wird in einem temporären Verzeichnis auf dem Web Intelligence Processing Server abgelegt. Der Web Intelligence Processing Server öffnet das Dokument im Speicher, und `QT.dll` generiert die SQL auf Grundlage des Universums, das dem Dokument zugrunde liegt. Die im Web Intelligence Processing Server enthaltenen Connection-Server-Bibliotheken stellen eine Verbindung mit der Datenquelle her. Die Abfragedaten werden über `QT.dll` an die Report Engine im Web Intelligence Processing Server zurückgegeben, auf dem das Dokument verarbeitet wird. Eine neue erfolgreiche Instanz wird erstellt.
6. Der Web Intelligence Processing Server lädt die Dokumentinstanz auf den Output FRS.

   Hinweis

   Dieser Schritt setzt zudem die Kommunikation mit dem CMS voraus, damit die erforderlichen Server und Objekte gesucht werden können.
7. Der Web Intelligence Processing Server benachrichtigt den Web-Intelligence-Dienst für zeitgesteuerte Verarbeitung (auf dem Adaptive Job Server) über den Abschluss der Dokumenterstellung. Wenn das Dokument für die Weitergabe an ein Ziel (Dateisystem, FTP, SMTP oder Posteingang) geplant ist, ruft der Adaptive Job Server das verarbeitete Dokument vom Output FRS ab und sendet es an die angegebenen Ziele. In diesem Beispiel trifft dies nicht zu.
8. Der Web-Intelligence-Dienst für zeitgesteuerte Verarbeitung aktualisiert den Auftragsstatus auf dem CMS.
9. Der CMS aktualisiert den Auftragsstatus in seinem Arbeitsspeicher und schreibt die Instanzinformationen dann in die CMS-Systemdatenbank.

3.4.5 Analysis

3.4.5.1 Anzeigen eines Arbeitsbereichs von SAP BusinessObjects Analysis, Edition für OLAP

Mit diesem Workflow wird beschrieben, wie ein Benutzer einen Arbeitsbereich von SAP BusinessObjects Analysis, Edition für OLAP, über das BI-Launchpad anfordert, um diesen anzuzeigen.

Hinweis

Für diesen Workflow ist es erforderlich, dass CMS, Adaptive Processing Server (der den Multi-Dimensional Analysis Service (MDAS) umfasst) und Input File Repository Server ausgeführt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Der Webclient sendet eine Anforderung zur Anzeige eines neuen Arbeitsbereichs über den Webserver an den Webanwendungsserver. Der Webclient kommuniziert über die DHTML AJAX-Technologie (Asynchronous JavaScript and XML) mit dem Webanwendungsserver. Die AJAX-Technologie ermöglicht die teilweise Aktualisierung von Seiten, sodass nicht bei jeder neuen Anforderung eine neue Seite gerendert werden muss.
2. Der Webanwendungsserver übersetzt die Anforderung und sendet sie an den Central Management Server (CMS), um festzustellen, ob der jeweilige Benutzer zur Anzeige oder Erstellung eines neuen Arbeitsbereichs berechtigt ist.
3. Der CMS ruft die Anmeldedaten des Benutzers aus der CMS-Systemdatenbank ab.
4. Wenn der Benutzer berechtigt ist, einen Arbeitsbereich anzuzeigen oder zu erstellen, sendet der CMS eine Bestätigung an den Webanwendungsserver. Gleichzeitig sendet er eine Liste, die einen oder mehrere verfügbare Multi-Dimensional Analysis Services (MDAS) enthält.
5. Der Webanwendungsserver wählt einen MDAS aus der Liste aus und sendet eine CORBA-Anforderung an den Service, um die geeigneten OLAP-Server zum Erstellen eines neuen bzw. zum Regenerieren eines vorhandenen Arbeitsbereichs zu finden.
6. Um das richtige Arbeitsbereichsdokument mit Informationen zur zugrunde liegenden OLAP-Datenbank sowie einer gespeicherten ersten OLAP-Abfrage abzurufen, muss der MDAS mit dem Input File Repository Server (FRS) kommunizieren. Der Input FRS ruft den erforderlichen Analysis-Arbeitsbereich aus dem zugrunde liegenden Verzeichnis ab und sendet diesen Arbeitsbereich in einem Datenstream zurück an den MDAS.
7. Der MDAS öffnet den Arbeitsbereich, formuliert eine Abfrage und sendet sie an den OLAP-Datenbankserver. Der MDAS muss über einen geeigneten OLAP-Datenbankclient verfügen, der für die OLAP-Datenquelle konfiguriert ist. Die Webclient-Anfrage muss in die entsprechende OLAP-Abfrage übersetzt werden. Der OLAP-Datenbankserver sendet das Abfrageergebnis zurück an den MDAS.
8. Je nach Anforderung – d.h. Erstellung, Anzeige, Druck oder Export – rendert der MDAS vorab das Ergebnis, um die schnellere Darstellung auf dem Java-Webanwendungsserver zu ermöglichen. Der MDAS sendet XML-Pakete der gerenderten Ergebnisse zurück an den Webanwendungsserver.
9. Der Webanwendungsserver rendert den Arbeitsbereich und sendet die formatierte Seite oder Teilseite über den Webserver an den Webclient. Der Webclient zeigt die aktualisierte oder neu angeforderte Seite an. Dabei handelt es sich um eine Zero-Client-Lösung, von der keine Java- oder ActiveX-Komponenten heruntergeladen werden müssen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4 Systemkonfigurationsassistent

4.1 Einführung in den Systemkonfigurationsassistenten

Nachdem Sie SAP BusinessObjects Business Intelligence installiert haben, möchten Sie vermutlich die grundlegende Nachinstallationskonfiguration durchführen und beispielsweise eine Implementierungsvorlage und die SAP-BusinessObjects-Produkte auswählen, die Ihr Unternehmen nutzen wird. Um diese Konfiguration durchzuführen und die BI-Plattform möglichst schnell einzurichten, führen Sie den *Systemkonfigurationsassistenten* aus.

Wichtige Vorteile des Assistenten:

- Der Assistent führt Sie durch die Konfigurationsschritte, die Sie ausführen sollen.
- Durch die Verwendung des Assistenten wird das Risiko einer Systemfehlkonfiguration gesenkt.
- Der Assistent konfiguriert Einstellungen für Sie, wodurch die Systemkonfiguration beschleunigt wird.

Der Assistent ist standardmäßig so eingerichtet, dass er automatisch ausgeführt wird, wenn Sie sich an der Central Management Console (CMC) anmelden, Sie können ihn jedoch auch aus dem Bereich *Verwalten* in der CMC starten. Sie können den Assistenten jederzeit erneut ausführen, um Ihre Konfiguration anzupassen, und Sie können stets die Verwaltungsseite *Server* in der CMC verwenden, um Einstellungen zu optimieren, einschließlich der mit dem Assistenten vorgenommenen Einstellungen.

> **Hinweis**
>
> Zur Gewährleistung einer höheren Sicherheit können nur Mitglieder der Administratorengruppe auf den Assistenten zugreifen.

> **Hinweis**
>
> Um zu verhindern, dass der Assistent automatisch ausgeführt wird, kann der "Administrator"-Benutzer das Kontrollkästchen **Diesen Assistenten beim Starten der CMC nicht anzeigen** auf der ersten Seite des Assistenten aktivieren.

> **Hinweis**
>
> Falls Sie planen, Addons zu installieren oder Knoten zu Ihrer BI-Plattform-Implementierung hinzuzufügen, sollten Sie diese Schritte vor der Ausführung des Systemkonfigurationsassistenten ausführen.

4.2 Angeben der von Ihnen verwendeten Produkte

Sie können die Konfiguration von BI-Plattform-Servern vereinfachen, indem Sie die in Ihrer Organisation verwendeten Produkte angeben. Außerdem können Sie die Ressourcenallokation optimieren, indem Sie die Server für Produkte stoppen, die in Ihrer Organisation nicht verwendet werden. Wählen Sie dazu die Produkte auf der Seite *Produkte* aus. Wenn Sie die in Ihrer Organisation verwendeten Produkte angeben, startet der Assistent alle zum Ausführen dieser Produkte erforderlichen Server und Abhängigkeiten und konfiguriert die Server und

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Abhängigkeiten so, dass sie automatisch gestartet werden, wenn die BI-Plattform gestartet wird. Außerdem können Sie die Startzeit und die Resourcenauslastung der BI-Plattform optimieren, indem Sie nicht verwendete Produkte deaktivieren.

Wenn Sie z.B. das Produkt Crystal Reports auswählen, startet die BI-Plattform automatisch alle Crystal-Reports-Server und die entsprechenden Abhängigkeiten.

Um eine Liste aller Server anzuzeigen, die automatisch für ein Produkt gestartet werden, klicken Sie auf das Symbol**?** neben dem Namen des Produkts.

Der Assistent konfiguriert Produktserver wie folgt:

- Durch Auswahl eines Produkts werden alle zu diesem Server gehörenden Produkte sowie alle anderen für die ordnungsgemäße Funktionsweise dieses Produkts erforderlichen Server (Abhängigkeiten) gestartet, wenn der Assistent fertig ist. Durch Auswahl eines Produkts werden die Server dieses Produkts so eingestellt, dass sie automatisch mit der BI-Plattform gestartet werden. Wenn der Server Dienste von mehreren Produkten hostet, und eines dieser Produkte ausgewählt wird, wird der Server gestartet. Beachten Sie, dass einige Dienste von nicht ausgewählten Produkten möglicherweise ausgeführt werden, wenn sie von einem Server gehostet werden, der auch die Dienste von ausgewählten Produkten hostet.
- Wenn ein Produkt deaktiviert wird, werden die von diesem Produkt verwendeten Server gestoppt, vorausgesetzt, die Server hosten keine Dienste eines noch ausgewählten Produkts oder zur Kerndienstkategorie gehörende Dienste. Die gestoppten Produktserver sind nicht für einen automatischen Start mit der BI-Plattform eingerichtet. Wenn ein Server Dienste von aktivierten und deaktivierten Produkten hostet, wird er weiterhin ausgeführt.
- Die Deaktivierung eines Produkts kann auch zum Stoppen von Servern führen, die nicht zu dem deaktivierten Produkt gehören, falls es abhängige Dienste gibt, die ausschließlich von diesem deaktivierten Produkt verwendet werden. Dadurch werden Ressourcen freigegeben, da diese abhängigen Server nicht mehr benötigt werden.
- Wird ein Produkt aktiviert bzw. deaktiviert, werden alle Server, die zu der Kerndienstekategorie gehörende Dienste in der BI-Plattform hosten, (ausgenommen von WACS gehostete Dienste) automatisch gestartet. Der WACS verbleibt in seinem aktuellen Status.
- Durch Deaktivieren von Produkten werden keine Dateien für diese Produkte deinstalliert oder entfernt.

Wenn Sie die Seite *Produkte* öffnen, repräsentieren die Produktstatus auf der Seite den aktuellen Systemstatus.

Wenn alle Server für ein Produkt ausgeführt werden, ist das Kontrollkästchen für dieses Produkt aktiviert. Wenn alle Server für ein Produkt gestoppt werden, ist das Kontrollkästchen deaktiviert. Wenn nur einige Server für ein Produkt ausgeführt werden, während andere sich in anderen Status befinden, wie z.B. "Gestoppt", zeigt die Seite *Produkte* das Kontrollkästchen **Vorhandene Konfiguration beibehalten** an, um darauf hinzuweisen, dass das System außerhalb des Assistenten konfiguriert wurde. Sie können das Kontrollkästchen deaktivieren, wenn Sie den Assistenten zur Änderung der Konfiguration verwenden möchten.

Hinweis

Auf der Seite *Produkte* werden alle auf dem Cluster installierten Produkte angezeigt. Wenn z.B. auf Rechner A die Produkte P1 und P2 und auf Rechner B die Produkte P2 und P3 installiert sind, werden auf der Seite*Produkte* die Produkte P1, P2 und P3 angezeigt. Nicht installierte Produkte werden nicht auf der Seite *Produkte* angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Zur Vereinfachung der Implementierung muss die Konfiguration auf dieser Seite nicht für jeden Knoten wiederholt werden, stattdessen wird sie auf das gesamte Cluster angewendet.

> **Hinweis**
>
> Falls Einstellungen zuvor in der CMC geändert wurden, zeigt der Assistent eine Meldung an, die besagt, dass die Einstellungen außerhalb des Assistenten geändert wurden. Sie können die bestehende Konfiguration beibehalten oder die aktuellen Einstellungen überschreiben.

> **Hinweis**
>
> Änderungen, die Sie im Assistenten vornehmen, werden erst angewendet, nachdem Sie auf der Seite **Überprüfen** auf *Anwenden* geklickt haben.

Nachdem Sie die Änderungen vorgenommen haben, klicken Sie auf **Weiter**, um zur nächsten Seite des Assistenten zu wechseln. Sie können auch über den Navigationsbereich links direkt zu einer Seite wechseln, die sie bereits zuvor aufgerufen haben.

4.3 Auswählen von Implementierungsvorlagen

Die Standardinstallation der BI-Plattform konfiguriert eine kleine Implementierung, die für eine Demo-Umgebung auf eingeschränkter System-Hardware geeignet ist. Zur besseren Anpassung auf Ihre Hardware und den Anwendungsfall (beispielsweise die Vorbereitung eines Testsystem oder Produktivsystems) wählen Sie eine der vordefinierten Implementierungsvorlagen auf der Seite *Kapazität* aus. Diese Vorlagen sollen Ihnen dabei behilflich sein, Ihr BI-Plattform-System schnell einzurichten und auszuführen und die Zeit für die Erstimplementierung zu verkürzen.

Auch wenn die Auswahl einer geeigneten Implementierungsvorlage für die Erstkonfiguration nützlich ist und einen guten Ausgangspunkt bietet, stellt sie keinen Ersatz für die Größenanpassung und Optimierung des Systems dar, die weiterhin ausgeführt werden muss. Um eine optimale Leistung zu erzielen, sollten Sie zur Größenanpassung Ihres Systems ein Handbuch zur Größenanpassung verwenden: *http://www.sap.com/bisizing*.

Die Auswahl einer geeigneten Implementierungsvorlage ist aus mehreren Gründen wichtig:

- Die von Ihnen gewählte Implementierungsvorlage wirkt sich auf die Kapazität zur Verarbeitung von Anforderungen Ihres Systems aus. Eine größere Implementierung bietet mehr Kapazität zur Verarbeitung von Anforderungen oder von komplexeren Anforderungen. Für eine größere Implementierung sind jedoch mehr Systemressourcen erforderlich.
- Die Auswahl einer größeren Implementierung garantiert keine verbesserte Performance, insbesondere, wenn Sie nicht über ausreichende Hardware-Ressourcen verfügen.
- Die von Ihnen ausgewählte Implementierungsvorlage sollte Ihren Geschäftsanforderungen und Ihren verfügbaren Hardware-Ressourcen entsprechen. Die Systemkapazität und -Performance ist möglicherweise niedriger, wenn Sie eine Implementierungsvorlage wählen, die für Ihre Geschäftsanforderungen zu klein oder für die verfügbaren Hardware-Ressourcen zu groß ist.
- Größere Implementierungsvorlagen bieten eine bessere Kompartimentierung: Fehler in einem Produkt wirken sich mit niedrigerer Wahrscheinlichkeit auf andere Produkte aus. Wählen Sie eine Vorlage, die die Nutzung

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

und Performance von Ressourcen (RAM) ausgleicht. Wenn eine hohe RAM-Größe verfügbar ist, können Sie die größte für Ihren Arbeitsspeicher zulässige Implementierungsvorlage wählen. Dies führt zu einer besseren Systemkompartimentierung.

Sie können mit dem Schieberegler eine Implementierungsvorlage auswählen oder aus der Dropdown-Liste eine RAM-Größe wählen. Beachten Sie beim Ändern der Einstellung, dass der Indikator *Anzahl an Adaptive Processing Servern* sich ändert, um Ihnen anzuzeigen, wie Ihr System konfiguriert wird, wenn Sie diese Einstellung wählen.

Hinweis

Die von Ihnen ausgewählte Implementierungsvorlage wirkt sich nur auf die Adaptive Processing Server (APS) aus. Andere Server, beispielsweise der CMS oder Adaptive Job Server, bleiben unbeeinflusst.

Hinweis

"Erforderliches RAM" ist die RAM-Mindestgröße, die für BI-Plattform-Server benötigt wird. Wenn beispielsweise auf einem Rechner mit 16 GB RAM das Betriebssystem 1 GB RAM, der Datenbankserver ebenfalls 1 GB und die BI-Plattform-Server 10 GB benötigen, entspricht "Erforderliches RAM" 10 GB, nicht 12 GB oder 16 GB. Die Zahl in "Erforderliches RAM" stellt nur einen typischen Wert dar; für Ihr System könnte bei hoher Belastung mehr RAM erforderlich sein. Für eine optimale System-Performance sollten Sie stets die Systemgrößenanpassung durchführen.

Hinweis

Wenn Sie die Seite *Kapazität* öffnen, stellt die auf der Seite dargestellte Implementierungsvorlage den aktuellen Systemstatus dar, wenn dieser mit einer der vordefinierten Implementierungsvorlagen übereinstimmt. Wenn Sie beispielsweise unter Verwendung der CMC manuell einen zusätzlichen Adaptive Processing Server erstellt haben, entspricht der aktuelle Status Ihres Systems keiner der Implementierungsvorlagen, deshalb wird auf der Seite *Kapazität* das Kontrollkästchen **Vorhandene Konfiguration beibehalten** angezeigt, um anzugeben, dass das System außerhalb des Assistenten konfiguriert wurde. In einer Implementierung mit mehreren Knoten wird das Kontrollkästchen **Vorhandene Konfiguration beibehalten** auch dann angezeigt, wenn bei einem beliebigen Knoten die Anzahl an APS nicht mit der Implementierungsvorlage übereinstimmt oder wenn die Anzahl an APS auf verschiedenen Knoten unterschiedlich ist. Sie können das Kontrollkästchen deaktivieren, wenn Sie den Assistenten zur Änderung der Konfiguration verwenden möchten.

Hinweis

Um die Implementierung zu vereinfachen, wird die von Ihnen gewählte APS-Konfiguration auf alle Knoten angewendet (solange diese Knoten über einen installierten APS verfügen). Über je mehr Knoten Sie also verfügen, desto mehr Kapazität hat Ihr Cluster.

Hinweis

Addons (zum Beispiel Data Services oder Analysis Application Design Service (AADS)) werden nicht vom Assistenten verwalten. Dienste, die von den Addons erstellt wurden, werden nicht zu anderen APS vom Assistenten verschoben.

Beispiele:

- Wenn AADS von einem APS gehostet wird, der andere Dienste aus der BI-Plattform-Hauptinstallation hostet, und Sie den Assistenten zum Ändern der Implementierungsvorlagengröße von XS in M ändern,

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

erstellt der Assistent sieben neue APS und verschiebt alle Dienste auf die sieben APS, mit Ausnahme des AADS-Dienstes, der auf dem ersten APS verbleibt.

- Das Data-Services-Addon erstellt einen dedizierten APS. Der Assistent ändert diesen dedizierten APS nicht und zählt diesen APS nicht mit, wenn er die Anzahl der APS im System meldet.

Die Datei DeploymentTemplates.pdf

Um eine detaillierte Beschriftung der Einstellungen anzuzeigen, die der Assistent für alle verfügbaren Implementierungsvorlagen vornimmt, klicken Sie auf die Verknüpfung **Implementierungsvorlage** auf der Seite *Kapazität*, um die Datei `DeploymentTemplates.pdf` zu öffnen.

In der Datei `DeploymentTemplates.pdf` werden die Implementierungsvorlagen detailliert beschrieben. Beachten Sie, dass auf den Vorlagen nicht die Anzahl der Benutzer angegeben wird, die unterstützt werden können. Dies liegt daran, dass deren Anzahl von der Last abhängig ist. Sie sollten die Systemgrößenanpassung durchführen, um die Anzahl der zu unterstützenden Benutzer, die daraus resultierende erforderliche RAM-Größe, die CPU-Anforderungen usw. festzulegen.

4.4 Festlegen von Datenordnerspeicherorten

Verwenden Sie die Seite *Ordner*, um festzulegen, wo die BI-Plattform die Daten- und Protokolldateien speichert. Sie können Ordnerspeicherorte festlegen oder die aktuellen Speicherorte akzeptieren.

Wenn Ihre BI-Plattform-Implementierung mehrere Knoten aufweist, stehen Ihnen zur Definition der Ordnerspeicherorte zwei Optionen zur Verfügung:

- Wenn Sie dieselben Ordnerspeicherorte für alle Knoten konfigurieren möchten, wählen Sie die Option **Alle Knoten haben dieselben Ordnerspeicherorte**.
- Wenn die Server in Ihrem Cluster nicht identisch eingerichtet sind, haben sie möglicherweise unterschiedliche Installationspfade oder Dateiverzeichnisstrukturen. Sie können die Option **Die Knoten haben verschiedene Ordnerspeicherorte** wählen, um bestimmte Ordnerspeicherorte für jeden einzelnen Knoten zu konfigurieren.

Wenn der Assistent die Seite *Ordner* öffnet, werden die Ordnernamen folgendermaßen angezeigt:

- Wenn alle Knoten Ordner mit den genau identischen Werten aufweisen (das bedeutet, die Protokoll-Ordner auf allen Servern im Cluster sind identisch und die Daten-Ordner auf allen Servern im Cluster sind identisch usw.), ist die Option **Alle Knoten haben dieselben Ordnerspeicherorte** ausgewählt, und die aktuellen Ordnernamen werden angezeigt.
- Wenn alle Ordner eines bestimmten Typs (Protokoll, Daten, Audit, Input-Dateispeicher oder Output-Dateispeicher) innerhalb jedes einzelnen Knotens identisch sind, sich jedoch zwischen den Knoten unterscheiden, ist die Option **Die Knoten haben verschiedene Ordnerspeicherorte** ausgewählt, und die aktuellen Ordnernamen werden angezeigt.
- Wenn alle Ordner eines bestimmten Typs innerhalb jedes einzelnen Knotens nicht identisch sind und sich zwischen den Knoten unterscheiden, ist die Option **Die Knoten haben verschiedene Ordnerspeicherort** ausgewählt, die Ordnernamen sind jedoch leer.

Wenn Sie die Speicherorte der Ordner ändern, konfiguriert der Assistent das System so, dass die neuen Ordner verwendet werden. Mit Ausnahme des Audit-Datenordners kopiert oder verschiebt der Assistent die Inhalte der

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Originalordner nicht in die neuen Ordner. Wenn die neuen Ordner die richtigen Inhalte nicht bereits enthalten, oder wenn die Originalordner Daten umfassen, die Sie migrieren möchten, können Sie diese Daten in die neuen Ordner verschieben oder kopieren.

Wenn der neue Ordnerspeicherort leer ist, sollten sie für die Input-Dateispeicher-, Output-Dateispeicher- und Daten-Ordner die Dateien aus dem alten Ordnerspeicherort manuell in den neuen kopieren oder die Dateien aus einer Sicherung wiederherstellen. Kopieren Sie für den Protokoll-Ordner die Dateien aus dem alten Ordner nur dann, wenn der neue Ordner die Protokolldateien des alten Ordnerspeicherorts enthalten soll.

Tipp

Wenn Sie Dateien in die neuen Ordner kopieren oder darin wiederherstellen möchten, tun Sie dies vor dem Neustart der Knoten.

Beispielszenarien:

- Wenn Sie einen Ordnerspeicherort ändern und der Originalordner Berichte enthält, stehen diese Berichte in der BI-Plattform erst dann zur Verfügung, wenn Sie sie in den neuen Ordner kopiert und die Knoten neu gestartet haben.
- Wenn der Originalordner beschädigte oder modifizierte Berichte enthalten hat und Sie diese auf eine bekanntermaßen gute Sicherung zurücksetzen möchten, rufen Sie die Berichte aus der Sicherung ab, und platzieren Sie sie im neuen Ordner, anstatt die Inhalte aus dem Originalordner zu kopieren.
- Wenn sich Ihre Datendateien ursprünglich auf einer Festplatte mit dem Buchstaben X befunden haben und Sie den Buchstaben im Betriebssystem in Y ändern, müssen Sie die Datendateien nicht kopieren oder verschieben; Sie müssen lediglich den Ordnerspeicherort in der BI-Plattform ändern.

Wenn Sie einige Ordnerspeicherorte manuell geändert haben, sodass einige Server auf einem Knoten einen Satz von Ordnern verwenden während andere Server auf demselben Knoten andere Ordner verwenden, wird auf der Seite *Ordner* das Kontrollkästchen **Vorhandene Konfiguration beibehalten** angezeigt, um anzugeben, dass das System außerhalb des Assistenten konfiguriert wurde. Beispielsweise könnten Sie über zwei File Repository Server aus demselben Knoten verfügen, die für die Verwendung unterschiedlicher Protokoll-Ordnerpfade konfiguriert wurden. Sie können das Kontrollkästchen deaktivieren, wenn Sie den Assistenten zur Änderung der aktuellen Konfiguration verwenden möchten.

Für weitere Informationen zu den Typen der in den einzelnen Ordnern gespeicherten Dateien klicken Sie auf die **?**-Symbole.

Hinweis

Wenn Sie einen der folgenden Ordnerspeicherorte ändern, müssen Sie nach Beendigung des Assistenten alle Knoten manuell neu starten, damit die Änderungen übernommen werden:

- Input-Dateispeicher
- Output-Dateispeicher
- Protokoll-Ordner
- Daten-Ordner

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4.5 Überprüfen von Änderungen

Nachdem Sie die Auswahl der Konfigurationseinstellungen abgeschlossen haben, werden diese auf der Seite *Überprüfen* angezeigt, damit Sie sie prüfen können, bevor die Änderungen auf Ihr BI-Plattform-System angewandt werden. Für jede Kategorie von Einstellungen können Sie auf **Details** klicken, um eine detaillierte Beschreibung oder Auflistung der anzuwendenden Einstellungen und Änderungen anzuzeigen.

Wenn Sie eine beliebige Einstellung ändern möchten, können Sie direkt aus dem Navigationsmenü auf der linken Seite des Assistenten auf die einzelnen Seiten zugreifen.

Ihre Auswahl wird in einer Protokolldatei gespeichert, die Sie von der Seite "Abgeschlossen" herunterladen können.

Außerdem wird eine Antwortdatei generiert und gespeichert. Mithilfe der Antwortdatei können Sie die Systemkonfiguration automatisieren. Sie können auf die Schaltfläche **Herunterladen** klicken, um die Antwortdatei anzuzeigen oder auf einen lokalen Datenträger herunterzuladen.

Wenn Sie auf **Anwenden** klicken, werden Ihre Konfigurationseinstellungen auf Ihre BI-Plattform-Implementierung angewendet. Wenn der Assistent abgeschlossen ist, wird die Seite *Abgeschlossen* angezeigt, die die nächsten Schritte enthält, die Sie manuell ausführen sollen.

Weitere Informationen

Protokolldateien und Antwortdateien [Seite 93]

4.6 Protokolldateien und Antwortdateien

Auf der Seite *Abgeschlossen* wird der Status Ihrer Änderungen angezeigt, und Sie können die Protokoll- und Antwortdateien für Ihre Sitzung anzeigen.

Die Protokoll- und Antwortdateien werden automatisch im Ordner System Configuration Wizard angezeigt, auf den Sie über die CMC zugreifen können. Die Dateinamen enthalten einen Zeitstempel im Format `Jahr_Monat_Tag_Stunde_Minute_Sekunde`. Für Protokolldateien wird die Erweiterung `.log` verwendet, für Antwortdateien die Verwendung `.ini`.

Sie können auch auf **Download**-Schaltflächen klicken, um die Protokoll- und Antwortdateien anzuzeigen oder auf einen lokalen Datenträger herunterzuladen.

Die Protokolldatei enthält folgenden Inhalt:

- Einen Datensatz mit allen in dieser Sitzung von Ihnen vorgenommenen Änderungen.
- Den Speicherort der Antwortdatei.
- Eine Liste, in der die nächsten erforderlichen Schritte beschrieben werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Verwenden von Antwortdateien [Seite 94]

4.6.1 Verwenden von Antwortdateien

Jedes Mal, wenn der Assistent abgeschlossen ist, wird eine Antwortdatei gespeichert, die Ihre Auswahlen oder Antworten auf alle Fragen auf den Seiten des Assistenten enthält. Die Antwortdatei kann zum Konfigurieren von anderen Clustern in Ihrer BI-Plattform-Implementierung verwendet werden, ohne dass Sie für jedes einzelne Cluster die Schritte des Assistenten durchlaufen müssen, oder sie kann zu einem späteren Zeitpunkt verwendet werden, wenn Sie das System auf denselben Konfigurationsstatus setzen möchten. Mithilfe der Antwortdatei können Sie Ihre Implementierung automatisieren und vermeiden Bedienerfehler.

Um eine Antwortdatei zu verwenden, führen Sie ein Skript aus, das die Antwortdatei als Parameter verwendet. Suchen Sie zuerst die zu verwendende Antwortdatei, und speichern Sie sie auf der Festplatte. Antwortdateien werden automatisch im Ordner Systemkonfigurationsassistent gespeichert, auf den Administratoren über die CMC zugreifen können. Die Dateinamen enthalten einen Zeitstempel im Format `Jahr_Monat_Tag_Stunde_Minute_Sekunde` und haben die Erweiterung `.ini`. Sie können die Antwortdatei über die CMC anzeigen und auf Festplatte speichern, oder Sie können dazu die Menübefehle **Organisieren** > **Senden** > **Dateispeicherort** verwenden.

Sie können die Antwortdatei auch für Ihre aktuelle Assistentensitzung von der Seite *Überprüfen* oder *Abgeschlossen* herunterladen und auf Festplatte speichern.

Wenn Sie die Einstellungen in der Antwortdatei ändern möchten, bevor Sie sie verwenden, können Sie sie in einem Texteditor bearbeiten. Einzelheiten finden Sie in der Beispielantwortdatei unten.

Ausführen des Skripts

Nachdem Sie über die entsprechende Antwortdatei verfügen, verwenden Sie die Datei als Befehlszeilenparameter für die Skripte, die den Assistenten ausführen:

- Führen Sie unter Windows die Batch-Datei `SCW.bat` aus.
- Führen Sie unter UNIX die Skriptdatei `scw.sh` aus.

Die Batch-Datei und die Skriptdatei befinden sich im selben Ordner wie andere Serververwaltungsskripte:

- Unter Windows: `<Installverz>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.
- Unter Unix: `<Installverz>/sap_bobj/enterprise_xi40/linux_x64/scripts`.

Die Batch-Datei und die Skriptdatei verwenden folgende Befehlszeilenparameter:

- `-help`: Zeigt die Befehlszeilenhilfe an.
- `-r`: Geben Sie den Pfad und den Namen der Antwortdatei ein.
- `-cms`: Geben Sie den Central Management Server (CMS) an, an dem Sie sich anmelden wollen. Wenn dieser Parameter nicht angegeben, verwendet der CMS standardmäßig den lokalen Rechner und den Standardport (6400). Beispiel: `Rechnername:6500`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- `-username`: Geben Sie ein Konto an, das Administratorrechte für die BI-Plattform hat. Wenn dieser Parameter nicht angegeben wird, wird das Standardadministratorkonto verwendet
- `-password`: Geben Sie das Kennwort für dieses Konto an. Wenn diese Option nicht angegeben wird, wird bei der Anmeldung ein leeres Kennwort verwendet. Um den Parameter `-password` verwenden zu können, müssen Sie auch den Parameter `-username` verwenden.

Beispiele

Unter Windows: `SCW.bat -r c:\folder\filename.ini -cms cmsname:6400 -username "Administrator" -password Beispielkennwort`

Unter Unix: `./scw.sh -r /home/folder/filename.ini -cms CMSName:6400 -username "Administrator" -password Beispielkennwort`

Beispiel für eine Antwortdatei

```
# ********************************************
# ***************** Products *****************
# ********************************************

# Keep the existing configuration for products.
# Valid values = true or false.
# "true": the existing product configuration will be preserved.
# "false": the product configuration will be modified according to the “Products.”
settings below.

Products.KeepExistingConfiguration = true

# The “Products.” settings below will be ignored if
Products.KeepExistingConfiguration = true.

# Auto-start the servers for these products.
# Valid values = true or false.
# "true": the product's servers and their dependencies are auto-started with BI
platform.
# "false": the product's servers are not auto-started with BI platform.

# Crystal Reports
Products.crystalreports = true

# Analysis edition for OLAP
Products.olap = true

# Web Intelligence
Products.webintelligence = false

# Dashboards (Xcelsius)
Products.dashboards = false

# Data Federator
Products.datafederator = true

# Lifecycle Manager
Products.LCM = true
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
# ******************************************************
# ***************** Deployment Template *****************
# ******************************************************

# Keep the existing configuration for the deployment template.
# Valid values = true or false.
# "true": the existing deployment template configuration will be preserved and the
Capacity.DeploymentTemplate setting below will be ignored.
# "false": the deployment template configuration will be modified according to the
Capacity.DeploymentTemplate setting below.

Capacity.KeepExistingConfiguration = true

# Specify the deployment template for all nodes.
# Valid values = xs, s, m, l, xl.

Capacity.DeploymentTemplate = xs


# *******************************************
# ***************** Folders *****************
# *******************************************

# Keep the existing configuration for folder locations.
# Valid values = true or false.
# "true": the existing folder configuration will be preserved.
# "false": the folder configuration will be modified according to the "Folders."
settings below.

Folders.KeepExistingConfiguration = true

# The “Folders.” settings below will be ignored if
Folders.KeepExistingConfiguration = true.

# ------ All nodes use the same folders ------
# Use this section when you have one node, or when all nodes have the same folder
locations. Otherwise, comment it out.

Folders.InputFileStore = <Path>
Folders.OutputFileStore = <Path>
Folders.Log = <Path>
Folders.Data = <Path>
Folders.Auditing = <Path>

# ------ Nodes use different folders ------
# Use this section when nodes have different folder locations. Otherwise, comment
it out.

# ------ NodeOne ------
# Folders.NodeOne.InputFileStore = <Path>
# Folders.NodeOne.OutputFileStore = <Path>
# Folders.NodeOne.Log = <Path>
# Folders.NodeOne.Data = <Path>
# Folders.NodeOne.Auditing = <Path>

# ------ NodeTwo ------
# Folders.NodeTwo.InputFileStore = <Path>
# Folders.NodeTwo.OutputFileStore = <Path>
# Folders.NodeTwo.Log = <Path>
# Folders.NodeTwo.Data = <Path>
# Folders.NodeTwo.Auditing = <Path>
```

Alle Einstellungen in der Antwortdatei müssen angegeben werden. Es dürfen keine Einstellungen leer belassen werden, ausgenommen in folgenden Fällen:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Bei einer Mehrfachknoten-Implementierung können Sie die Ordnereinstellungen für einen oder mehrere Knoten weglassen, was bedeutet, dass die Ordner in diesen Knoten unverändert bleiben. Jedoch müssen für die Knoten, die Sie in der Antwortdatei angeben, alle Ordnerspeicherorte angegeben werden.
- Wenn der Parameter `KeepExistingConfiguration` auf `true` gesetzt ist, können Sie die restlichen Einstellungen für diese Seite weglassen. Wenn z.B. `Products.KeepExistingConfiguration = true` können Sie die übrigen Einstellungen für *Produkte* von der Antwortdatei weglassen.

In manchen Fällen enthält die Antwortdatei andere Produkte als die in Ihrem Zielcluster installierten Produkte. In diesen Fällen gilt Folgendes:

- Wenn die Antwortdatei keine Definitionen für im Zielcluster installierte Produkte enthält, schlägt die Operation fehl.
- Wenn die Antwortdatei Definitionen für Produkte enthält, die nicht im Zielcluster enthalten sind, wird eine Warnmeldung zur Protokolldatei hinzugefügt, und die übrigen Produkte werden ordnungsgemäß konfiguriert.

> **Hinweis**
>
> Wenn Sie eine Antwortdatei zur Konfiguration eines Clusters verwenden, müssen Sie die im Abschnitt " Nächste Schritt" der Protokolldatei beschriebenen zusätzlichen Schritte manuell ausführen.

> **Hinweis**
>
> Für erhöhte Sicherheit ist nur Enterprise-Authentifizierung erforderlich (nicht Windows AD, LDAP oder SAP).

> **Hinweis**
>
> Wenn Sie den Neustart von Knoten auf den nächsten geplanten Neustart verschieben möchten, führen Sie das Skript direkt vor einer geplanten Systemausfallzeit aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

5 Verwalten von Lizenzen

5.1 Verwalten von Lizenzschlüsseln

In diesem Abschnitt wird beschrieben, wie Sie Lizenzschlüssel für die Implementierung der BI-Plattform verwalten.

Weitere Informationen

Anzeigen von Lizenzinformationen [Seite 98]
Hinzufügen von Lizenzschlüsseln [Seite 98]
So zeigen Sie die aktuelle Kontoaktivität an [Seite 99]

5.1.1 Anzeigen von Lizenzinformationen

Der Verwaltungsbereich *Lizenzschlüssel* der CMC zeigt die Anzahl der Zugriffslizenzen, der benannten Lizenzen und der Prozessorlizenzen, die jedem Schlüssel zugeordnet sind.

1. Wechseln Sie zum Verwaltungsbereich *Lizenzschlüssel* der CMC.
2. Wählen Sie einen Lizenzschlüssel aus.

   Die zum Schlüssel gehörenden Details werden im Bereich **Lizenzschlüsselinformationen** angezeigt. Wenn Sie weitere Lizenzschlüssel erwerben möchten, wenden Sie sich an Ihren SAP-Vertreter.

Weitere Informationen

Hinzufügen von Lizenzschlüsseln [Seite 98]
So zeigen Sie die aktuelle Kontoaktivität an [Seite 99]

5.1.2 Hinzufügen von Lizenzschlüsseln

Bei einer Aktualisierung von einer Testversion des Produkts müssen Sie den Auswertungsschlüssel löschen, bevor Sie neue Lizenzschlüssel oder Schlüsselcodes für die Produktaktivierung hinzufügen. Nachdem die neuen Lizenzschlüssel hinzugefügt wurden, müssen Sie alle Server erneut aktivieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Wenn Sie nach einer Änderung der Implementierung von BI-Plattform-Lizenzen in Ihrem Unternehmen neue Lizenzschlüssel erhalten haben, löschen Sie alle vorherigen Lizenzschlüssel aus dem System, damit die Konformität aufrechterhalten wird.

1. Wechseln Sie zum Verwaltungsbereich **Lizenzschlüssel** der CMC.
2. Geben Sie im Feld **Schlüssel hinzufügen** den Schlüssel ein.
3. Klicken Sie auf **Hinzufügen**.

Der Schlüssel wird zu der Liste hinzugefügt.

Weitere Informationen

Anzeigen von Lizenzinformationen [Seite 98]
So zeigen Sie die aktuelle Kontoaktivität an [Seite 99]

5.1.3 So zeigen Sie die aktuelle Kontoaktivität an

1. Wechseln Sie zum Verwaltungsbereich **Einstellungen** der CMC.
2. Klicken Sie auf **Globale Systemmetrik anzeigen**.

   In diesem Abschnitt werden die aktuelle Lizenznutzung sowie zusätzliche Informationen zur Auftragsmetrik angezeigt.

Weitere Informationen

Hinzufügen von Lizenzschlüsseln [Seite 98]
Anzeigen von Lizenzinformationen [Seite 98]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6 Verwalten von Benutzern und Gruppen

6.1 Übersicht über die Kontoverwaltung

Sie können sich die Kontoverwaltung als die Gesamtheit der Aufgaben vorstellen, die sich auf das Erstellen, Zuordnen, Ändern und Organisieren von Benutzer- und Gruppeninformationen beziehen. Im Verwaltungsbereich *Benutzer und Gruppen* der Central Management Console (CMC) können Sie diese Aufgaben an einem zentralen Ort ausführen.

Nachdem die Benutzerkonten und Gruppen erstellt wurden, können Sie Objekte hinzufügen und ihnen Rechte zuweisen. Wenn sich die Benutzer anmelden, können sie die Objekte mit BI-Launchpad oder ihrer benutzerdefinierten Webanwendung anzeigen.

6.1.1 Benutzerverwaltung

Im Verwaltungsbereich *Benutzer und Gruppen* können Sie alle erforderlichen Angaben machen, damit ein Benutzer auf die BI-Plattform zugreifen kann. Sie können auch die beiden standardmäßigen Benutzerkonten anzeigen lassen, die in der Tabelle "Standard-Benutzerkonten" enthalten sind.

Tabelle 2: Standard-Benutzerkonten

Kontoname	Beschreibung
Administrator	Dieser Benutzer gehört den Gruppen *Administratoren* und *Alle* an. Ein Administrator kann alle Aufgaben in sämtlichen BI-Plattform-Anwendungen ausführen (z.B. in der CMC, in CCM, im Publishing-Assistenten und in BI-Launchpad).
Guest	Dieser Benutzer gehört der Gruppe *Alle* an. Dieses Konto ist standardmäßig aktiviert und erhält kein vom System zugewiesenes Kennwort. Wenn Sie diesem Konto ein Kennwort zuweisen, wird die Einzelanmeldung bei BI-Launchpad deaktiviert.
SMAdmin	Dies ist ein schreibgeschütztes Konto, das von SAP Solution Manager für den Zugriff auf BI-Plattform-Komponenten verwendet wird.

Hinweis

Objektmigrationen werden am besten von Mitgliedern der Administratorengruppe, insbesondere dem Administratorbenutzerkonto durchgeführt. Um ein Objekt zu migrieren, müssen verschiedene zugehörige Objekte u.U. ebenfalls migriert werden. Der Erwerb der erforderlichen Sicherheitsberechtigungen für sämtliche Objekte ist für ein delegiertes Administratorkonto eventuell nicht möglich.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6.1.2 Gruppenverwaltung

Bei Gruppen handelt es sich um Zusammenstellungen von Benutzern, die über dieselben Kontoberechtigungen verfügen. Daher können Gruppen auf der Basis von Abteilungen, Rollen oder Standorten erstellt werden. Gruppen bieten Ihnen die Möglichkeit, Benutzerrechte an einem zentralen Punkt (der Gruppe) zu ändern, anstatt die Rechte für jedes Benutzerkonto einzeln zu ändern. Zudem haben Sie die Möglichkeit, einer Gruppe oder Gruppen Objektrechte zuzuweisen.

Im Bereich *Benutzer und Gruppen* können Sie Gruppen erstellen, die einer Anzahl von Personen den Zugriff auf den Bericht oder Ordner ermöglichen. Dadurch können Sie Änderungen zentral vornehmen, anstatt jedes Benutzerkonto einzeln zu ändern. Sie können auch die verschiedenen standardmäßigen Gruppenkonten anzeigen lassen, die in der Tabelle "Standard-Gruppenkonten" enthalten sind.

Um verfügbare Gruppen in der CMC anzuzeigen, klicken Sie im **Strukturbereich** auf *Gruppenliste*. Alternativ können Sie auf **Gruppenhierarchie** klicken, um eine hierarchische Liste aller verfügbaren Gruppen anzuzeigen.

Tabelle 3: Standard-Gruppenkonten

Kontoname	Beschreibung
Administratoren	Mitglieder dieser Gruppe können sämtliche Aufgaben in allen BI-Plattform-Anwendungen ausführen (CMC, CCM, Publishing-Assistent und BI-Launchpad). Die Gruppe *Administratoren* enthält standardmäßig nur den Benutzer "Administrator".
Alle	Jeder Benutzer ist Mitglied der Gruppe *Alle*.
QaaWS-Gruppendesigner	Mitglieder dieser Gruppe haben Zugriff auf Query as a Web Service.
Benutzer des Berichtskonvertierungstools	Mitglieder dieser Gruppe haben Zugriff auf das Berichtskonvertierungstool.
Übersetzer	Mitglieder dieser Gruppe haben Zugriff auf das Übersetzungsmanager-Tool.
Universe Designer-Benutzer	Benutzer, die dieser Gruppe angehören, erhalten Zugriff auf den *Universe Designer*-Ordner und den Ordner *Verbindungen*. Diese Benutzer können steuern, wer Zugriff auf Designer erhalten soll. Sie müssen dieser Gruppe bei Bedarf Benutzer hinzufügen. Standardmäßig enthält diese Gruppe keine Benutzer.

Weitere Informationen

Funktionsweise von Rechten in der BI-Plattform [Seite 124]
Gewähren von Zugriff für Benutzer und Gruppen [Seite 112]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6.1.3 Verfügbare Authentifizierungstypen

Bevor Sie in der BI-Plattform Benutzerkonten und -gruppen einrichten, legen Sie fest, welcher Authentifizierungstyp verwendet werden soll. In der Tabelle "Authentifizierungstypen" sind die Authentifizierungsoptionen zusammengefasst, die Ihnen zur Verfügung stehen können, je nachdem, welche Sicherheitstools Ihr Unternehmen verwendet.

Tabelle 4: Authentifizierungstypen

Authentifizierungstyp	Beschreibung
Enterprise	Verwenden Sie die vom System vorgegebene Enterprise-Authentifizierung, wenn Sie für die Arbeit mit der BI-Plattform eindeutige Konten und Gruppen erstellen möchten, oder wenn Sie noch keine Benutzer- und Gruppenhierarchie auf einem LDAP-Verzeichnisserver oder Windows AD-Server erstellt haben.
LDAP	Wenn Sie einen LDAP-Verzeichnisserver einrichten, können Sie bestehende LDAP-Benutzerkonten und -Gruppen in der BI-Plattform verwenden. Nach der Zuordnung von LDAP-Konten zur BI-Plattform sind Benutzer in der Lage, mit ihrem LDAP-Benutzernamen und -kennwort auf BI-Plattform-Anwendungen zuzugreifen. Dadurch ist es nicht notwendig, Benutzer- und Gruppenkonten in der BI-Plattform neu zu erstellen.
Windows AD	Sie können vorhandene Windows AD-Benutzerkonten und -gruppen in der BI-Plattform nutzen. Wenn Sie der BI-Plattform AD-Konten zuordnen, können sich Benutzer mit ihrem AD-Benutzernamen und -kennwort bei der BI-Plattform anmelden. Dadurch ist es nicht notwendig, Benutzer- und Gruppenkonten in der BI-Plattform neu zu erstellen.
SAP	Sie können vorhandene SAP-Rollen den BI-Plattform-Konten zuordnen. Nach der Zuordnung der SAP-Rollen sind Benutzer in der Lage, sich mit ihren SAP-Anmeldedaten bei BI-Plattform-Anwendungen anzumelden. Dadurch ist es nicht notwendig, Benutzer- und Gruppenkonten in der BI-Plattform neu zu erstellen.
Oracle EBS	Sie können vorhandene Oracle EBS-Rollen den BI-Plattform-Konten zuordnen. Nach der Zuordnung der Oracle EBS-Rollen sind Benutzer in der Lage, sich mit ihren Oracle EBS-Anmeldedaten bei BI-Plattform-Anwendungen anzumelden. Dadurch ist es nicht notwendig, Benutzer- und Gruppenkonten in der BI-Plattform neu zu erstellen.
Siebel	Sie können vorhandene Siebel-Rollen den BI-Plattform-Konten zuordnen. Nach der Zuordnung der Siebel-Rollen sind Benutzer in der Lage, sich mit ihren Siebel-An-

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Authentifizierungstyp	Beschreibung
	meldedaten bei BI-Plattform-Anwendungen anzumelden. Dadurch ist es nicht notwendig, Benutzer- und Gruppenkonten in der BI-Plattform neu zu erstellen.
PeopleSoft Enterprise	Sie können vorhandene PeopleSoft-Rollen den BI-Plattform-Konten zuordnen. Nach der Zuordnung der PeopleSoft-Rollen sind Benutzer in der Lage, sich mit ihren PeopleSoft-Anmeldedaten bei BI-Plattform-Anwendungen anzumelden. Dadurch ist es nicht notwendig, Benutzer- und Gruppenkonten in der BI-Plattform neu zu erstellen.
JD Edwards EnterpriseOne	Sie können vorhandene JD Edwards-Rollen den BI-Plattform-Konten zuordnen. Nach der Zuordnung der JD Edwards-Rollen sind Benutzer in der Lage, sich mit ihren JD Edwards-Anmeldedaten bei BI-Plattform-Anwendungen anzumelden. Dadurch ist es nicht notwendig, Benutzer- und Gruppenkonten in der BI-Plattform neu zu erstellen.

6.2 Verwalten von Enterprise-Konten und allgemeinen Konten

Da die Enterprise-Authentifizierung die standardmäßige Authentifizierungsmethode für die BI-Plattform ist, wird sie bei der ersten Installation des Systems automatisch aktiviert. Wenn Sie Benutzer und Gruppen hinzufügen und verwalten, speichert die BI-Plattform die Benutzer- und Gruppeninformationen in der eigenen Datenbank.

> **Hinweis**
>
> Wenn ein Benutzer seine Websitzung bei der BI-Plattform abmeldet, indem er zu einer anderen Seite navigiert oder seinen Webbrowser schließt, wird die Enterprise-Sitzung nicht abgemeldet und weiterhin eine Lizenz beansprucht. Die Enterprise-Sitzung läuft nach ungefähr 24 Stunden ab. Um die Enterprise-Sitzung des Benutzers zu beenden und die Lizenz freizugeben, damit sie von anderen Benutzern verwendet werden kann, muss sich der Benutzer von der BI-Plattform abmelden.

6.2.1 So erstellen Sie ein Benutzerkonto

Wenn Sie einen neuen Benutzer erstellen, legen Sie dessen Eigenschaften fest und wählen für ihn die Gruppe bzw. Gruppen aus.

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Klicken Sie auf **Verwalten** > **Neu** > **Neuer Benutzer**.
   Das Dialogfeld *Neuer Benutzer* wird angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. So erstellen Sie einen Enterprise-Benutzer:
   a) Wählen Sie in der Liste **Authentifizierungstyp** den Eintrag **Enterprise** aus.
   b) Geben Sie den Kontonamen, den vollständigen Namen, E-Mail sowie eine Beschreibung ein.

   > **Tipp**
   >
   > Verwenden Sie den Bereich "Beschreibung", um weitere Informationen über den Benutzer oder das Konto einzufügen.

   c) Geben Sie die Kennwortinformationen und Einstellungen an.
4. Zum Erstellen eines Benutzers, der sich mit einem anderen Authentifizierungstyp anmeldet, wählen Sie die entsprechende Option in der Liste **Authentifizierungstyp** aus, und geben Sie den Kontonamen ein.
5. Führen Sie eine der folgenden Aktionen aus, um das Benutzerkonto (basierend auf Ihrer BI-Plattform-Lizenzvereinbarung) zu bestimmen:
   - Wählen Sie die Option **Zugriffslizenzbenutzer** aus, wenn dieser Benutzer zu einer Lizenzvereinbarung gehört, die festlegt, wie viele Benutzer gleichzeitig angemeldet sein dürfen.
   - Wählen Sie die Option **Namenslizenzbenutzer** aus, wenn dieser Benutzer zu einer Lizenzvereinbarung gehört, bei der der Name eines bestimmten Benutzers mit einer Lizenz verbunden ist. Namenslizenzen sind hilfreich für Personen, die unabhängig von der Anzahl der angemeldeten Benutzer Zugriff auf die BI-Plattform benötigen.
6. Klicken Sie auf **Erstellen und schließen**.

   Der Benutzer wird dem System und automatisch der Gruppe "Alle" hinzugefügt. Für den Benutzer wird automatisch ein Posteingang sowie ein Enterprise-Alias erstellt.

Nun können Sie den Benutzer einer Gruppe hinzufügen oder Rechte für ihn festlegen.

Weitere Informationen

Funktionsweise von Rechten in der BI-Plattform [Seite 124]

6.2.2 So ändern Sie ein Benutzerkonto

Verwenden Sie dieses Verfahren, um die Eigenschaften oder Gruppenmitgliedschaft eines Benutzers zu ändern.

> **Hinweis**
>
> Wenn Sie Änderungen vornehmen, wirkt sich dies auf den Benutzer aus, sofern dieser angemeldet ist.

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Wählen Sie den Benutzer aus, dessen Eigenschaften Sie ändern möchten.
3. Klicken Sie auf **Verwalten** > **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* des Benutzers wird angezeigt.
4. Ändern Sie die Eigenschaften für den Benutzer.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Zusätzlich zu den Optionen, die beim Erstellen des Kontos verfügbar waren, haben Sie nun die Möglichkeit, das Konto zu deaktivieren, indem Sie das Kontrollkästchen **Konto ist deaktiviert** aktivieren.

> **Hinweis**
>
> Alle an dem Benutzerkonto vorgenommenen Änderungen werden erst angezeigt, wenn sich der Benutzer das nächste Mal anmeldet.

5. Klicken Sie auf **Speichern und schließen**.

Weitere Informationen

Erstellen eines neuen Alias für einen vorhandenen Benutzer [Seite 121]

6.2.3 Löschen eines Benutzerkontos

Verwenden Sie dieses Verfahren, um das Konto eines Benutzers zu löschen. Eventuell erhält der Benutzer eine Fehlermeldung, wenn Sie das Konto löschen, wenn er/sie angemeldet ist. Wenn Sie ein Benutzerkonto löschen, werden außerdem der Favoritenordner, die persönlichen Kategorien und der Posteingang des jeweiligen Benutzers gelöscht.

Wenn Sie annehmen, dass der Benutzer zu einem späteren Zeitpunkt wieder auf das Konto zugreifen möchte, aktivieren Sie das Kontrollkästchen **Konto ist deaktiviert** im Dialogfeld *Eigenschaften* des ausgewählten Benutzers, anstatt das Konto zu löschen.

> **Hinweis**
>
> Durch das Löschen eines Benutzerkontos wird nicht automatisch verhindert, dass sich der Benutzer erneut bei der BI-Plattform anmelden kann. Falls das Benutzerkonto auch auf einem Drittthersteller-System eingerichtet wurde und einer Drittthersteller-Gruppe angehört, die der BI-Plattform zugeordnet wurde, ist der Benutzer möglicherweise weiterhin in der Lage, sich anzumelden.

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Wählen Sie den Benutzer aus, den Sie löschen möchten.
3. Klicken Sie auf **Verwalten** > **Löschen**.

   Das Dialogfeld zum Bestätigen des Löschvorgangs wird angezeigt.
4. Klicken Sie auf **OK**.
   Das Benutzerkonto wird gelöscht.

Weitere Informationen

So ändern Sie ein Benutzerkonto [Seite 104]
So deaktivieren Sie einen Alias [Seite 123]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6.2.4 Erstellen von neuen Gruppen

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Klicken Sie auf **Verwalten** > **Neu** > **Neue Gruppe**.
   Das Dialogfeld *Neue Benutzergruppe erstellen* wird angezeigt.
3. Geben Sie Gruppennamen und Beschreibung ein.
4. Klicken Sie auf **OK**.

Nachdem Sie eine neue Gruppe erstellt haben, können Sie Benutzer und Untergruppen hinzufügen oder eine Gruppenmitgliedschaft festlegen, so dass die neue Gruppe eigentlich eine Untergruppe ist. Da Untergruppen Ihnen zusätzliche Strukturierungsmöglichkeiten bieten, sind sie beim Festlegen von Objektrechten hilfreich, um den Zugriff von Benutzern auf den BI-Plattform-Inhalt zu steuern.

6.2.5 So ändern Sie die Eigenschaften einer Gruppe

Sie können die Eigenschaften einer Gruppe ändern, indem Sie Änderungen an den gewünschten Einstellungen vornehmen.

> **Hinweis**
>
> Auf Benutzer, die der Gruppe angehören, wirkt sich die Änderung bei der nächsten Anmeldung aus.

1. Wählen Sie im Verwaltungsbereich *Benutzer und Gruppen* der CMC die Gruppe aus.
2. Klicken Sie auf **Verwalten** > **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
3. Ändern Sie die Eigenschaften für die Gruppe.

   Klicken Sie auf die Links in der Navigationsliste, um die verschiedenen Dialogfelder zu öffnen und unterschiedliche Eigenschaften zu bearbeiten.

   - Wenn Sie den Titel oder die Beschreibung für die Gruppe ändern möchten, klicken Sie auf **Eigenschaften**.
   - Wenn Sie die Rechte ändern möchten, die Subjekte für die Gruppe haben, klicken Sie auf **Benutzersicherheit**.
   - Wenn Sie Profilwerte für Gruppenmitglieder ändern möchten, klicken Sie auf **Profilwerte**.
   - Wenn die Gruppe einer anderen Gruppe als Untergruppe hinzugefügt werden soll, klicken Sie auf **Mitglied von**.
4. Klicken Sie auf **Speichern**.

6.2.6 So zeigen Sie Gruppenmitglieder an

Sie können dieses Verfahren verwenden, um die Benutzer anzuzeigen, die zu einer bestimmten Gruppe gehören.

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Erweitern Sie die **Gruppenhierarchie** im *Strukturbereich*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Wählen Sie die Gruppe im *Strukturbereich* aus.

> **Hinweis**
>
> Das Anzeigen Ihrer Liste kann einige Minuten dauern, wenn die Gruppe eine große Anzahl von Benutzern enthält oder einem Drittthersteller-Verzeichnis zugeordnet ist.

Es wird eine Liste der Benutzer angezeigt, die der Gruppe angehören.

6.2.7 Hinzufügen von Untergruppen

Sie können eine Gruppe einer weiteren Gruppe hinzufügen. Wenn Sie so vorgehen, wird die von Ihnen hinzugefügte Gruppe zu einer Untergruppe.

> **Hinweis**
>
> Das Hinzufügen einer Untergruppe ist mit dem Festlegen einer Gruppenmitgliedschaft vergleichbar.

1. Wählen Sie im Verwaltungsbereich *Benutzer und Gruppen* der CMC die Gruppe aus, die Sie einer anderen Gruppe als Untergruppe hinzufügen möchten.
2. Klicken Sie auf **Aktionen** > **Gruppe beitreten**.
   Das Dialogfeld *Gruppe beitreten* wird angezeigt.
3. Verschieben Sie die Gruppe, der Sie die erste Gruppe hinzufügen möchten, aus der Liste **Verfügbare Gruppen** in die Liste **Zielgruppe(n)**.
4. Klicken Sie auf **OK**.

Weitere Informationen

Festlegen von Gruppenmitgliedschaften [Seite 107]

6.2.8 Festlegen von Gruppenmitgliedschaften

Sie können festlegen, dass eine Gruppe Mitglied einer anderen Gruppe ist. Die Gruppe, die zum Mitglied wird, wird als Untergruppe bezeichnet. Die Gruppe, der Sie die Untergruppe hinzufügen, ist die übergeordnete Gruppe. Eine Untergruppe übernimmt die Rechte der übergeordneten Gruppe.

1. Klicken Sie im Verwaltungsbereich *Benutzer und Gruppen* der CMC auf die Gruppe, die Sie einer anderen Gruppe hinzufügen möchten.
2. Klicken Sie auf **Aktionen** > **Mitglied von**.
   Das Dialogfeld *Mitglied von* wird angezeigt.
3. Klicken Sie auf **Gruppe beitreten**.
   Das Dialogfeld *Gruppe beitreten* wird angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Verschieben Sie die Gruppe, der Sie die erste Gruppe hinzufügen möchten, aus der Liste **Verfügbare Gruppen** in die Liste **Zielgruppe(n)**.

   Alle Rechte, die zu der übergeordneten Gruppe gehören, werden von der neuen, von Ihnen erstellten Gruppe übernommen.
5. Klicken Sie auf **OK**.
   Sie kehren zum Dialogfeld *Mitglied von* zurück, und die übergeordnete Gruppe wird in der Liste der übergeordneten Gruppen angezeigt.

6.2.9 So löschen Sie eine Gruppe

Sie können eine Gruppe löschen, wenn Sie sie nicht mehr benötigen. Die Standardgruppen "Administratoren" und "Alle" können nicht gelöscht werden.

> **Hinweis**
>
> Auf Benutzer, die der gelöschten Gruppe angehören, wirkt sich die Änderung bei der nächsten Anmeldung aus.

> **Hinweis**
>
> Benutzer, die der gelöschten Gruppe angehören, verlieren alle von der Gruppe übernommenen Rechte.

Um Dritthersteller-Authentifizierungsgruppen, beispielsweise die Gruppe Windows AD-Benutzer, zu löschen, verwenden Sie den Verwaltungsbereich *Authentifizierung* in der CMC.

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Wählen Sie die Gruppe aus, die Sie löschen möchten.
3. Klicken Sie auf **Verwalten** > **Löschen**.
   Das Dialogfeld zum Bestätigen des Löschvorgangs wird angezeigt.
4. Klicken Sie auf **OK**.
   Die Gruppe wird gelöscht.

6.2.10 Hinzufügen von Benutzern oder Benutzergruppen in Massenvorgängen

Sie können eine CSV-Datei (kommagetrennte Werte) verwenden, um Benutzer oder Benutzergruppen in Massenvorgängen zur CMC hinzuzufügen. In einer korrekt formatierten CSV-Datei trennen die Kommas die Daten in einer Zeile, wie im folgenden Beispiel dargestellt:

```
Add,MyGroup,MyUser1,MyFullName,Password1,My1@example.com,ProfileName,ProfileValue
```

Folgende Bedingungen gelten für den Prozess der Massenhinzufügung:

- Jede Zeile in der CSV-Datei, die einen Fehler enthält, wird vom Importprozess ausgeschlossen.
- Benutzerkonten sind nach dem Import anfänglich deaktiviert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Sie können beim Erstellen neuer Benutzer leere Kennwörter verwenden. Sie müssen jedoch ein gültiges Enterprise-Authentifizierungskennwort für nachfolgende Aktualisierungen der vorhandenen Benutzer verwenden.
- Wenn DB-Zugangsdaten zu einem Konto hinzugefügt werden, werden die Datenbankanmeldedaten im Profil des Benutzers aktiviert.

1. Wählen Sie im Verwaltungsbereich **Benutzer und Gruppen** der CMC ▶ **Verwalten** > **Importieren** > **Benutzer-/Gruppen-/DB-Zugangsdaten** ◀.

   Das Dialogfeld *Benutzer-/Gruppen-/DB-Zugangsdaten importieren* wird angezeigt.
2. Klicken Sie auf **Durchsuchen**, wählen Sie eine CSV-Datei und klicken auf **Verifizieren**.

   Die Datei wird verarbeitet. Wenn die Daten in der Datei korrekt formatiert sind, wird die Schaltfläche **Importieren** aktiviert. Wenn die Daten nicht korrekt formatiert sind, werden Informationen zu dem Fehler angezeigt, der behoben werden muss, bevor die CMC die Datei für den Import verifizieren kann.
3. Klicken Sie auf **Importieren**.

Die Benutzer und Gruppen werden in die CMC importiert.

Um die von Ihnen hinzugefügten Benutzer und Benutzergruppen zu überprüfen, wählen Sie ▶ **Verwalten** > **Importieren** > **Verlauf** ◀ im Verwaltungsbereich **Benutzer und Gruppen**.

6.2.11 So aktivieren Sie das Guest-Konto

Das Guest-Konto ist standardmäßig deaktiviert, um sicherzustellen, dass sich niemand unter diesem Konto bei der BI-Plattform anmelden kann. Durch diese Standardeinstellung wird auch die anonyme Einzelanmeldung der BI-Plattform deaktiviert, sodass Benutzer nur mit einem gültigen Benutzernamen und Kennwort Zugriff auf BI-Launchpad erhalten.

Führen Sie diese Aufgabe aus, wenn Sie das Guest-Konto aktivieren möchten, damit Benutzer für den Zugriff auf BI-Launchpad kein eigenes Konto verwenden müssen.

1. Wechseln Sie zum Verwaltungsbereich **Benutzer und Gruppen** der CMC.
2. Klicken Sie im Navigationsbereich auf **Benutzerliste**.
3. Wählen Sie **Guest** aus.
4. Klicken Sie auf ▶ **Verwalten** > **Eigenschaften** ◀.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
5. Deaktivieren Sie das Kontrollkästchen **Konto ist deaktiviert**.
6. Klicken Sie auf **Speichern und schließen**.

6.2.12 Hinzufügen von Benutzern zu Gruppen

Anhand von Benutzergruppen können Administratoren BI-Launchpad-Aufgaben für ganze Gruppen von Benutzern auf einmal durchführen (sie können z. B. für bestimmte Benutzergruppen Einstellungen anpassen oder Veröffentlichungen zeitgesteuert verarbeiten).

Benutzer können Gruppen auf folgende Weisen hinzugefügt werden:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Wählen Sie die Gruppe aus, und klicken Sie auf **Aktionen** > **Elemente zur Gruppe hinzufügen**.
- Wählen Sie den Benutzer aus, und klicken Sie auf **Aktionen** > **Mitglied von**.
- Wählen Sie den Benutzer aus, und klicken Sie auf **Aktionen** > **Gruppe beitreten**.

Sie können Benutzer mehr als einer Gruppe hinzufügen. Wenn ein Benutzer jedoch zwei oder mehr Benutzergruppen angehört, zeigt das BI-Launchpad nur die Einstellungen für eine Gruppe an.

Weitere Informationen

Festlegen von Gruppenmitgliedschaften [Seite 107]

6.2.12.1 Hinzufügen von Benutzern zu einer oder mehreren Benutzergruppen

Sie können Benutzer mehr als einer Gruppe hinzufügen. Im BI-Launchpad werden jedoch nur die Einstellungen für eine der Benutzergruppen angezeigt.

1. Wählen Sie im Verwaltungsbereich *Benutzer und Gruppen* der CMC den Benutzer aus, der einer Gruppe hinzugefügt werden soll.
2. Wählen Sie **Aktionen** > **Gruppe beitreten** aus.

   Hinweis

   Standardmäßig sind alle BI-Plattform-Benutzer des Systems Mitglied der Gruppe "Alle".

3. Verschieben Sie im Dialogfeld *Gruppe beitreten* die Gruppe, der Sie den Benutzer hinzufügen möchten, aus der Liste **Verfügbare Gruppen** in die Liste **Zielgruppe(n)**.

   Tipp

   Mit *UMSCHALTTASTE+Klicken* oder *STRG-Taste+Klicken* können Sie mehrere Gruppen auswählen.

4. Klicken Sie auf **OK**.

6.2.12.2 Hinzufügen von einem oder mehreren Benutzern zu einer Gruppe

Sie können einer Benutzergruppe mehrere Benutzer hinzufügen.

Für eine Benutzergruppe festgelegte Einstellungen gelten für alle Benutzer in der Gruppe. Im BI-Launchpad werden immer nur die Einstellungen für eine Benutzergruppe angezeigt.

1. Wählen Sie im Verwaltungsbereich *Benutzer und Gruppen* der CMC die Benutzergruppe aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Wählen Sie **Aktionen** > **Elemente zur Gruppe hinzufügen** aus.
3. Klicken Sie im Dialogfeld *Hinzufügen* auf **Benutzerliste**.
   Die Liste **Verfügbare Benutzer/Gruppen** wird regeneriert und enthält alle Benutzerkonten im System.
4. Verschieben Sie einen oder mehrere Benutzer aus der Liste **Verfügbare Benutzer/Gruppen** in die Liste **Ausgewählte Benutzer/Gruppen**, um sie der Gruppe hinzuzufügen.

   > **Tipp**
   >
   > Mit *UMSCHALTTASTE+Klicken* oder *STRG-Taste+Klicken* können Sie mehrere Benutzer auswählen. Um nach einem bestimmten Benutzer zu suchen, geben Sie den Namen des Benutzers in das Feld **Suche** ein.

   > **Tipp**
   >
   > Wenn Ihr System sehr viele Benutzer aufweist, können Sie anhand der Schaltflächen **Vorherige** und **Nächste** in der Benutzerliste navigieren.

5. Klicken Sie auf **OK**.

6.2.13 Ändern der Kennworteinstellungen

In der CMC können Sie die Kennworteinstellungen für einen bestimmten Benutzer oder für alle Benutzer im System ändern. Die verschiedenen nachfolgend aufgeführten Beschränkungen gelten nur für Enterprise-Konten, d.h. sie gelten nicht für Konten, die Sie einer externen Benutzerdatenbank (LDAP oder Windows AD) zugeordnet haben. Normalerweise können Sie jedoch im externen System den externen Konten ähnliche Beschränkungen auferlegen.

6.2.13.1 Ändern der Benutzerkennworteinstellungen

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Wählen Sie den Benutzer aus, dessen Kennworteinstellungen Sie ändern möchten.
3. Klicken Sie auf **Verwalten** > **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
4. Aktivieren oder deaktivieren Sie das Kontrollkästchen, das zu der Kennworteinstellung gehört, die Sie ändern möchten.

   Folgende Optionen stehen zur Verfügung:

   - **Kennwort ist zeitlich unbegrenzt gültig**
   - **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**
   - **Benutzer kann Kennwort nicht ändern**
5. Klicken Sie auf **Speichern und schließen**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6.2.13.2 Ändern der allgemeinen Kennworteinstellungen

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
2. Doppelklicken Sie auf **Enterprise**.
   Das Dialogfeld *Enterprise* wird angezeigt.
3. Aktivieren Sie das Kontrollkästchen der gewünschten Kennworteinstellungen und geben Sie ggf. einen Wert ein.

   Die untenstehende Tabelle gibt den Mindest- und den Höchstwert für jede Einstellung an.

   Tabelle 5: Kennworteinstellungen

Kennworteinstellung	Minimum	Empfohlener Höchstwert
Kennwörter mit Groß- und Kleinschreibung obligatorisch machen	N/A	N/A
Mindestens N Zeichen	0 Zeichen	64 Zeichen
Kennwort muss alle n Tage geändert werden	1 Tag	100 Tage
Die letzten N Kennwörter dürfen nicht wiederverwendet werden	1 Kennwort	100 Kennwörter
Mindestens N Minuten bis zur Änderung des Kennworts warten	0 Minuten	100 Minuten
Konto nach N fehlgeschlagenen Anmeldeversuchen deaktivieren	1 Fehlschläge	100 Fehlschläge
Zähler für fehlgeschlagene Anmeldungen nach N Minuten zurücksetzen	1 Minute	100 Minuten
Konto nach N Minuten wieder aktivieren	0 Minuten	100 Minuten

4. Klicken Sie auf **Aktualisieren**.

Inaktive Benutzerkonten werden nicht automatisch deaktiviert.

6.2.14 Gewähren von Zugriff für Benutzer und Gruppen

Sie können Benutzern und Gruppen Administratorzugriff auf andere Benutzer und Gruppen gewähren. Zu den Administratorrechten zählen das Anzeigen, Bearbeiten und Löschen von Objekten, das Anzeigen und Löschen von Objektinstanzen sowie das Anhalten von Objektinstanzen. Beispielsweise können Sie der IT-Abteilung zu Fehlerbehebungs- und Systemwartungszwecken das Bearbeiten und Löschen von Objekten gestatten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

So weisen Sie einer Zugriffskontrollliste für ein Objekt Prinzipale hinzu [Seite 134]

6.2.15 Steuern des Zugriffs auf Posteingänge von Benutzern

Wenn Sie einen Benutzer hinzufügen, wird vom System automatisch ein Posteingang für diesen Benutzer erstellt. Der Posteingang hat denselben Namen wie der Benutzer. Das Zugriffsrecht für den Posteingang eines Benutzers ist standardmäßig dem Benutzer und dem Administrator vorbehalten.

Weitere Informationen

Festlegen der zeitgesteuerten Verarbeitung für ein Programmobjekt [Seite 77]
Verwalten von Sicherheitseinstellungen für Objekte in der CMC [Seite 133]
Typspezifische Rechte [Seite 131]

6.2.16 Konfigurieren von BI-Launchpad-Optionen

In der CMC können Administratoren BI-Launchpad-Einstellungen für Benutzergruppen konfigurieren. Indem Sie die Eigenschaften in der Datei `BOE.war` konfigurieren, können Sie angeben, welche Informationen auf dem BI-Launchpad-Anmeldebildschirm des Benutzers angezeigt werden.

> **Hinweis**
>
> Wenn ein Benutzer zwei oder mehr Benutzergruppen angehört, zeigt das BI-Launchpad nur die konfigurierten Einstellungen für eine Gruppe an.

6.2.16.1 Konfigurieren des BI-Launchpad-Anmeldebildschirms

Am BI-Launchpad-Anmeldebildschirm werden Benutzer standardmäßig aufgefordert, Benutzernamen und Kennwort einzugeben. Sie können Benutzer auch zur Angabe des CMS-Namens und Authentifizierungstyps auffordern. Um diese Einstellung zu ändern, müssen Sie die BI-Launchpad-Eigenschaften für die Datei BOE.war bearbeiten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6.2.16.1.1 Konfigurieren des Anmeldebildschirms von BI-Launchpad

Damit Sie die Standardeinstellungen von BI-Launchpad ändern können, müssen Sie benutzerdefinierte BI-Launchpad-Eigenschaften für die BOE.war-Datei festlegen. Diese Datei ist auf dem Rechner implementiert, der den Webanwendungsserver hostet.

1. Wechseln Sie zu folgendem Verzeichnis in der BI-Plattform-Installation:

   <INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\

2. Erstellen Sie eine neue Datei mit einem Texteditor.
3. Speichern Sie die Datei unter folgendem Namen:

   BIlaunchpad.properties

4. Fügen Sie folgende Zeile hinzu, um die Authentifizierungsoptionen auf dem Anmeldebildschirm von BI-Launchpad einzubeziehen:

   ```
   authentication.visible=true
   ```

5. Fügen Sie folgende Zeile hinzu, um die Standardauthentifizierung zu ändern:

   ```
   authentication.default=<authentication>
   ```

   Ersetzen Sie `<authentication>` durch eine der folgenden Optionen:

Authentifizierungstyp	Wert von <authentication>
Enterprise	secEnterprise
LDAP	secLDAP
Windows AD	secWinAD
SAP	secSAPR3

6. Geben Sie folgende Zeile ein, um Benutzer zur Eingabe des CMS-Namens auf dem Anmeldebildschirm von BI-Launchpad aufzufordern:

   ```
   cms.visible=true
   ```

7. Speichern und schließen Sie die Datei.
8. Starten Sie Ihren Webanwendungsserver neu.

Implementieren Sie die `BOE.war`-Datei mit WDeploy erneut auf dem Webanwendungsserver. Weitere Informationen zur Verwendung von WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen für SAP BusinessObjects Business Intelligence* .

6.2.16.2 Festlegen der BI-Launchpad-Einstellungen für Benutzergruppen in der CMC

Administratoren können die BI-Launchpad-Standardeinstellungen für Benutzergruppen in der CMC konfigurieren.

Administratoren können in der CMC Standardwerte für folgende BI-Launchpad-Einstellungen eingeben:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Registerkarte **Startseite**
- Speicherort für Dokumente
- Ordner
- Kategorien
- Maximale Anzahl von Objekten pro Seite
- Auf der Registerkarte **Dokumente** angezeigte Spalten
- Ob Dokumente im BI-Launchpad auf Registerkarten oder in einem neuen Fenster angezeigt werden sollen

Vom Administrator für eine Benutzergruppe konfigurierte Einstellungen gelten für alle Benutzer in der Gruppe. Wenn ein Benutzer zwei oder mehr Benutzergruppen angehört, zeigt das BI-Launchpad nur die konfigurierten Einstellungen für eine Gruppe an.

Benutzer können ihre eigenen BI-Launchpad-Einstellungen definieren, und diese Einstellungen übersteuern die Standardwerte. (Benutzer können jederzeit zu den Standardeinstellungen zurückkehren.) Wenn der Administrator jedoch die BI-Launchpad-Standardeinstellungen in der CMC ändert, haben die Standardwerte Vorrang vor den benutzerdefinierten Werten.

6.2.16.2.1 Festlegen der BI-Launchpad-Einstellungen für eine Benutzergruppe

Die in der CMC konfigurierten BI-Launchpad-Einstellungen sind die Standardeinstellungen für alle Benutzer in einer Benutzergruppe.

> **Hinweis**
>
> Wenn ein Benutzer zwei oder mehr Benutzergruppen angehört, zeigt das BI-Launchpad nur die Standardeinstellungen einer Gruppe an.

Benutzer können ihre eigenen BI-Launchpad-Einstellungen definieren, wenn sie über die entsprechenden Zugriffsrechte verfügen. Wenn Sie nicht möchten, dass die Benutzer Einstellungen ändern, sollten Sie ihnen nicht die Berechtigung erteilen, Einstellungen festzulegen.

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Wählen Sie unter **Gruppenliste** die Benutzergruppe aus, für die Sie die BI-Launchpad-Einstellungen ändern möchten.
3. Wählen Sie **Aktionen** > **BI-Launchpad-Einstellungen** aus.
   Das Dialogfeld *BI-Launchpad-Einstellungen* wird angezeigt.
4. Deaktivieren Sie das Kontrollkästchen **Keine Einstellungen definiert**.
5. Wählen Sie entweder die Registerkarte **Startseite** oder **Dokumente** aus, um die Standardstartseite im BI-Launchpad zu wählen.
6. Wenn Sie die Registerkarte **Startseite** ausgewählt haben, führen Sie eine der folgenden Aktionen aus, um auf der Registerkarte die Startseite zu wählen:
   - Zum Anzeigen der Standard-**Startseite** des BI-Launchpads wählen Sie **Standard-Startseite** aus.
   - Zum Anzeigen einer bestimmten Website als **Startseite** wählen Sie **Startseite auswählen** aus, klicken auf **Startseite durchsuchen**, wählen ein Objekt im BI-Repository aus und klicken auf **Öffnen**.
7. Wenn Sie die Registerkarte **Dokumente** ausgewählt haben, führen Sie eine der folgenden Aktionen durch:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Wählen Sie **Eigene Dokumente** aus, um Ihr Dokumentenfach anzuzeigen, und wählen Sie den Standardknoten aus, um Folgendes anzuzeigen:
  - **Meine Favoriten**
  - **Persönliche Kategorien**
  - **Mein Posteingang**
- Wählen Sie **Ordner** aus, um Ihr Ordnerfach anzuzeigen, und wählen Sie den Standardordner aus, um Folgendes anzuzeigen:
  - Um alle öffentlichen Ordner auszuwählen, wählen Sie **Öffentliche Ordner** aus.
  - Um einen bestimmten Ordner auszuwählen, wählen Sie **Öffentlichen Ordner auswählen**, klicken auf **Ordner durchsuchen**, wählen den Ordner aus und klicken auf **Öffnen**.
- Wählen Sie **Kategorien** aus, um Ihr Kategorienfach anzuzeigen, und wählen Sie die Standardkategorie aus, um Folgendes anzuzeigen:
  - Um alle öffentlichen Kategorien auszuwählen, wählen Sie **Öffentliche Kategorien** aus.
  - Um eine bestimmte Kategorie auszuwählen, wählen Sie **Öffentliche Kategorie auswählen**, klicken auf **Kategorie durchsuchen**, wählen die Kategorie aus und klicken auf **Öffnen**.

8. Aktivieren Sie unter **Wählen Sie die auf der Registerkarte "Dokumente" anzuzeigenden Spalten aus** im Bereich **Liste** das Kontrollkästchen für jedes Objekt.
   - **Typ**
   - **Letzte Ausführung**
   - **Instanzen**
   - **Beschreibung**
   - **Erstellt von**
   - **Erstellt am**
   - **Speicherort (Kategorien)**
   - **Empfangen am (Posteingang)**
   - **Von (Posteingang)**
9. Führen Sie unter **Ort für Dokumentanzeige festlegen** eine der folgenden Aktionen aus, um festzulegen, wie die Benutzer Dokumente anzeigen:
   - Wählen Sie **Im Portal von BI-Launchpad als Registerkarten** aus, um Dokumente im BI-Launchpad auf einzelnen Registerkarten anzuzeigen.
   - Wählen Sie **In mehreren Vollbild-Browserfenstern ein Fenster für jedes Dokument** aus, um Dokumente in einzelnen Browserfenstern anzuzeigen.
10. Geben Sie in das Feld **Maximale Anzahl an Elementen pro Seite festlegen** die maximale Anzahl von Objekten pro BI-Launchpad-Seite an, die beim Anzeigen von Objektlisten angezeigt werden sollen.
11. Klicken Sie auf **Speichern und schließen**.

6.2.17 Verwalten von Attributen für Systembenutzer

BI-Plattform-Administratoren definieren und fügen Benutzerattribute Systembenutzern im Bereich *Benutzerattributverwaltung* in der Central Management Console (CMC) hinzu. Sie können Attribute für folgende Benutzerverzeichnisse verwalten und erweitern:

- Enterprise

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- SAP
- LDAP
- Windows AD

Beim Import von Benutzern von externen Verzeichnissen wie SAP, LDAP und Windows AD stehen im Allgemeinen folgende Attribute für die Benutzerkonten zur Verfügung:

- Vollständiger Name
- E-Mail-Adresse

Attributnamen

Alle zum System hinzugefügten Attribute müssen folgende Eigenschaften besitzen:

- *Name*
- *Interner Name*

Die Eigenschaft “Name” ist die benutzerfreundliche Kennung des Attributs. Mit ihr werden bei der Arbeit mit der semantischen Universumsschicht Filter abgefragt. Weitere Informationen finden Sie in der Dokumentation zum Universe-Design-Tool. Der “interne Name” wird von Entwicklern bei der Arbeit mit dem BI-Plattform-SDK verwendet. Diese Eigenschaft ist ein automatisch generierter Name.

Attributnamen dürfen nicht länger als 256 Zeichen sein und nur alphanumerische Zeichen und Unterstriche enthalten.

> **Tipp**
>
> Wenn Sie ungültige Zeichen für das Attribut "Name" angeben, wird von der BI-Plattform kein interner Name generiert. Da interne Namen nicht geändert werden können, nachdem sie zum System hinzugefügt wurden, wird empfohlen, die geeigneten Attributnamen, bestehend aus alphanumerischen Zeichen und Unterstrichen, sorgfältig auszuwählen.

Voraussetzungen für die Erweiterung von zugeordneten Benutzerattributen

Konfigurieren Sie vor dem Hinzufügen von Benutzerattributen zum System alle relevanten Authentifizierungs-Plugins für externe Benutzerverzeichnisse für die Zuordnung und den Import von Benutzern. Machen Sie sich außerdem mit dem Schema der externen Verzeichnisse vertraut, insbesondere mit den für Zielattribute verwendeten Namen.

> **Hinweis**
>
> Für das SAP-Authentifizierungs-Plugin können nur die in der BAPIADDR3-Struktur enthaltenen Attribute angegeben werden.

Nachdem die BI-Plattform für die Zuordnung neuer Benutzerattribute konfiguriert wurde, werden die Werte bei der nächsten geplanten Aktualisierung aufgefüllt. Alle Benutzerattribute werden im Verwaltungsbereich *Benutzer und Gruppen* der CMC angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6.2.18 Priorisierung von Benutzerattributen über mehrere Authentifizierungsoptionen hinweg

Bei der Konfiguration der Authentifizierungs-Plugins für SAP, LDAP und AD können Sie die Prioritätsstufen für jedes Plugin in Bezug auf die anderen beiden angeben. Verwenden Sie beispielsweise im LDAP-Authentifizierungsbereich die Option **Priorität der LDAP-Attributbindung im Verhältnis zu anderen Attributbindungen festlegen**, um die LDAP-Priorität in Bezug auf SAP und AD anzugeben. Der Enterprise-Attributwert hat standardmäßig Priorität vor einem Wert eines externen Verzeichnisses. Prioritäten für die Attributbindung werden nicht für ein bestimmtes Attribut, sondern auf Ebene des Authentifizierungs-Plugins festgelegt.

Weitere Informationen

Konfigurieren des LDAP-Hosts [Seite 241]
Importieren von SAP-Rollen [Seite 308]
Zuordnen von Windows-AD-Benutzern und -Benutzergruppen [Seite 265]

6.2.19 Hinzufügen von neuen Benutzerattributen

Bevor Sie der BI-Plattform ein neues Benutzerattribut hinzufügen, müssen Sie das Authentifizierungs-Plugin für das externe Verzeichnis, von dem aus Sie Benutzerkonten zuordnen, konfigurieren. Dies gilt für SAP, LDAP und Windows AD. Insbesondere müssen Sie die Option **Vollständigen Namen, E-Mail-Adresse und andere Attribute importieren** für alle erforderlichen Plugins aktivieren.

> **Hinweis**
>
> Es müssen keine vorbereitenden Aufgaben vor der Erweiterung der Attribute für Enterprise-Benutzerkonten ausgeführt werden.

> **Tipp**
>
> Wenn Sie planen, dasselbe Attribut über mehrere Plugins hinweg zu erweitern, sollten Sie die entsprechende Attributbindungs-Prioritätsstufe basierend auf den Anforderungen Ihres Unternehmens festlegen.

1. Wechseln Sie zum Verwaltungsbereich *Benutzerattributverwaltung* der CMC.
2. Klicken Sie auf das Symbol **Neues benutzerdefiniert zugeordnetes Attribut hinzufügen**.
   Das Dialogfeld *Attribut hinzufügen* wird angezeigt.
3. Geben Sie den Namen für das neue Attribut in das Feld *Name* ein.

   Die BI-Plattform verwendet den als benutzerfreundlichen Namen angegebenen Namen für das neue Attribut.

   Bei der Eingabe des benutzerfreundlichen Namens wird das Feld *Interner Name* automatisch im folgenden Format befüllt: `SI_[benutzerfreundlicher_Name]`. Der Systemadministrator gibt einen "benutzerfreundlichen" Attributnamen ein und die BI-Plattform generiert automatisch den "internen" Namen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Ändern Sie das Feld *Interner Name* nach Bedarf unter Verwendung von Buchstaben, Ziffern oder Unterstrichen.

   > **Tipp**
   >
   > Der Wert des Felds *Interner Name* kann nur zu diesem Zeitpunkt geändert werden. Der Wert kann nicht mehr geändert werden, nachdem das neue Attribut gespeichert wurde.

   Falls das neue Attribut für Enterprise-Konten ist, überspringen Sie Schritt 8.
5. Wählen Sie die entsprechende Option für **Neue Quelle hinzufügen für** aus der Liste aus, und klicken Sie auf das Symbol **Hinzufügen**. Folgende Optionen stehen zur Verfügung:
   - *SAP*
   - *LDAP*
   - *AD*

   Es wird eine Tabellenzeile für das in der angegebenen Attributquelle angegebene Attribut erstellt.
6. Geben Sie in die Spalte **Attributquellenname** den Namen des Attributs im Quellverzeichnis ein.

   Die BI-Plattform verfügt über keinen Mechanismus zur automatischen Verifizierung, ob der eingegebene Attributname im externen Verzeichnis vorhanden ist. Stellen Sie sicher, dass der angegebene Name richtig und gültig ist.
7. Wiederholen Sie die Schritte 5 bis 6, falls zusätzliche Quellen für das neue Attribut erforderlich sind.
8. Klicken Sie auf **OK**, um das neue Attribut zu speichern und an die BI-Plattform zu senden.
   Der Name, der interne Name und die Quelle des neuen Attributs sowie der Attributquellenname werden im Verwaltungsbereich *Benutzerattributverwaltung* in der CMC aufgeführt.

Das neue Attribut und sein zugehöriger Wert für jedes betreffende Benutzerkonto wird nach der nächsten geplanten Regenerierung im Verwaltungsbereich *Benutzer und Gruppen* angezeigt.

Wenn Sie mehrere Quellen für das neue Attribut verwenden, stellen Sie sicher, dass für jedes Authentifizierungs-Plugin die richtigen Prioritäten für die Attributbindung angegeben werden.

6.2.20 Bearbeiten benutzerdefinierter Benutzerattribute

Gehen Sie wie folgt vor, um in der BI-Plattform erstellte Benutzerattribute zu bearbeiten. Sie können Folgendes bearbeiten:

- den Namen des Attributs in der BI-Plattform

  > **Hinweis**
  >
  > Dabei handelt es sich nicht um den internen Namen des Attributs. Nachdem ein Attribut erstellt und der BI-Plattform hinzugefügt wurde, kann der interne Name nicht mehr geändert werden. Zum Entfernen eines internen Namens müssen Administratoren das zugehörige Attribut löschen.
- den Attributquellennamen
- Zusätzliche Quellen für das Attribut

1. Wechseln Sie zum Verwaltungsbereich *Benutzerattributverwaltung* der CMC.
2. Wählen Sie das zu bearbeitende Attribut aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Klicken Sie auf das Symbol **Ausgewähltes Attribut bearbeiten**.
   Das Dialogfeld *Bearbeiten* wird angezeigt.
4. Ändern Sie den Attributnamen oder die Quellinformationen.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern und an die BI-Plattform zu senden.
   Die geänderten Werte werden im Verwaltungsbereich *Benutzerattributverwaltung* der CMC angezeigt.

Der geänderte Name und die geänderten Werte werden nach der nächsten zeitgesteuerten Regenerierung im Verwaltungsbereich *Benutzer und Gruppen* angezeigt.

6.3 Verwalten von Aliasen

Wenn ein Benutzer in der BI-Plattform über mehrere Konten verfügt, können Sie diese über die Funktion "Alias zuweisen" verknüpfen. Dies ist hilfreich, wenn ein Benutzer über ein Drittthersteller-Konto verfügt, das Enterprise und einem Enterprise-Konto zugeordnet ist.

Indem Sie dem Benutzer einen Alias zuweisen, kann er sich entweder unter Verwendung eines Drittthersteller-Benutzernamens und -Kennworts oder eines Enterprise-Benutzernamens und -Kennworts anmelden. Mit einem Alias kann sich ein Benutzer daher über mehrere Authentifizierungstypen anmelden.

In der CMC werden die Aliasinformationen im unteren Bereich des Dialogfelds *Eigenschaften* eines Benutzers angezeigt. Benutzer können über beliebige Kombinationen von Enterprise-, LDAP- oder Windows AD-Aliase verfügen.

6.3.1 Erstellen von Benutzern und Hinzufügen eines Drittthersteller-Alias

Wenn Sie einen Benutzer erstellen und einen anderen Authentifizierungstyp als "Enterprise" auswählen, erstellt das System den neuen Benutzer in der BI-Plattform und einen Drittthersteller-Alias für den Benutzer.

> **Hinweis**
>
> Damit vom System der Drittthersteller-Alias erstellt wird, müssen die folgenden Kriterien erfüllt werden:
>
> - Das Authentifizierungstool muss in der CMC aktiviert sein.
> - Das Format des Kontonamens muss mit dem für den Authentifizierungstyp erforderlichen Format übereinstimmen.
> - Das Benutzerkonto muss im Authentifizierungstool des Drittherstellers vorhanden sein und einer Gruppe angehören, die der BI-Plattform bereits zugeordnet wurde.

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Klicken Sie auf **Verwalten** > **Neu** > **Neuer Benutzer**.
   Das Dialogfeld *Neuer Benutzer* wird angezeigt.
3. Wählen Sie den Authentifizierungstyp für den Benutzer, beispielsweise "Windows AD".
4. Geben Sie den Namen des Drittherstellerkontos für den Benutzer ein, beispielsweise `bsmith`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

5. Wählen Sie den Verbindungstyp für den Benutzer aus.
6. Klicken Sie auf **Erstellen und schließen**.

   Der Benutzer wird der BI-Plattform hinzugefügt und ihm wird ein Alias für den ausgewählten Authentifizierungstyp zugewiesen, beispielsweise secWindowsAD:ENTERPRISE:bsmith. Falls erforderlich, können Sie Benutzern Aliase hinzufügen, zuweisen und neu zuweisen.

6.3.2 Erstellen eines neuen Alias für einen vorhandenen Benutzer

Sie können Aliase für bestehende BI-Plattform-Benutzer erstellen. Dabei kann es sich um einen Enterprise-Alias oder einen Alias für ein Authentifizierungstool eines anderen Herstellers handeln.

> **Hinweis**
>
> Damit vom System der Dritthersteller-Alias erstellt wird, müssen die folgenden Kriterien erfüllt werden:
>
> - Das Authentifizierungstool muss in der CMC aktiviert sein.
> - Das Format des Kontonamens muss mit dem für den Authentifizierungstyp erforderlichen Format übereinstimmen.
> - Das Benutzerkonto muss im Authentifizierungstool des anderen Herstellers vorhanden sein und einer Gruppe angehören, die der Plattform zugeordnet wurde.

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Wählen Sie den Benutzer aus, dem Sie einen Alias hinzufügen möchten.
3. Klicken Sie auf **Verwalten** > **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
4. Klicken Sie auf **Neuer Alias**.
5. Wählen Sie den Authentifizierungstyp aus.
6. Geben Sie den Kontonamen für den Benutzer ein.
7. Klicken Sie auf **Aktualisieren**.

   Für den Benutzer wird ein Alias erstellt. Wenn Sie den Benutzer in der CMC anzeigen lassen, sind mindestens zwei Aliase aufgeführt, und zwar der dem Benutzer bereits zugewiesene und der von Ihnen gerade erstellte Alias.
8. Klicken Sie auf **Speichern und schließen**, um das Dialogfeld *Eigenschaften* zu schließen.

6.3.3 So weisen Sie einen Alias eines anderen Benutzers zu

Wenn Sie einem Benutzer einen Alias zuweisen, übertragen Sie einen Dritthersteller-Alias von einem anderen Benutzer auf den aktuell angezeigten Benutzer. Sie können keine Enterprise-Aliase zuweisen oder neu zuweisen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Wenn ein Benutzer nur über einen Alias verfügt und Sie diesen letzten Alias einem anderen Benutzer zuweisen, werden Benutzerkonto, Favoritenordner, persönliche Kategorien und Posteingang des jeweiligen Kontos vom System gelöscht.

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Wählen Sie den Benutzer aus, dem Sie einen Alias zuweisen möchten.
3. Klicken Sie auf **Verwalten** > **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
4. Klicken Sie auf **Alias zuweisen**.
5. Geben Sie das Benutzerkonto mit dem Alias ein, den Sie zuweisen möchten, und klicken Sie auf **Jetzt suchen**.
6. Verschieben Sie den Alias, den Sie zuweisen möchten, aus der Liste **Verfügbare Aliase** in die Liste **Aliase, die `<Benutzername>` hinzugefügt werden sollen**.

   Hier steht der Begriff `<Benutzername>` für den Namen des Benutzers, dem Sie einen Alias zuweisen.

   > **Tipp**
   >
   > Um mehrere Aliase auszuwählen, verwenden Sie die Kombination *UMSCHALTTASTEKlicken* oder *STRGKlicken*.

7. Klicken Sie auf **OK**.

6.3.4 So löschen Sie einen Alias

Wenn Sie einen Alias löschen, wird er aus dem System entfernt. Wenn ein Benutzer nur über einen Alias verfügt und Sie diesen Alias löschen, werden Benutzerkonto, Favoritenordner, persönliche Kategorien und Posteingang des jeweiligen Kontos automatisch vom System gelöscht.

> **Hinweis**
>
> Durch das Löschen eines Benutzeralias wird nicht automatisch verhindert, dass sich der Benutzer erneut bei der BI-Plattform anmelden kann. Wenn das Benutzerkonto weiterhin im Drittherstellersystem vorhanden ist und einer Gruppe angehört, die der BI-Plattform zugeordnet ist, kann sich der Benutzer noch beim System anmelden. Ob vom System ein neuer Benutzer erstellt oder der Alias einem vorhandenen Benutzer zugewiesen wird, richtet sich danach, welche Aktualisierungsoptionen Sie im Verwaltungsbereich *Authentifizierung* der CMC für das Authentifizierungstool ausgewählt haben.

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Wählen Sie den Benutzer aus, dessen Alias Sie löschen möchten.
3. Klicken Sie auf **Verwalten** > **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
4. Klicken Sie neben dem Alias, den Sie löschen möchten, auf die Schaltfläche **Alias löschen**.
5. Wenn Sie zum Bestätigen aufgefordert werden, klicken Sie auf **OK**.
   Der Alias wird gelöscht.
6. Klicken Sie auf **Speichern und schließen**, um das Dialogfeld *Eigenschaften* zu schließen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6.3.5 So deaktivieren Sie einen Alias

Sie können verhindern, dass sich ein Benutzer unter Verwendung einer bestimmten Authentifizierungsmethode bei der BI-Plattform anmeldet, indem Sie den Benutzeralias deaktivieren, der dieser Methode zugeordnet ist. Um einen Benutzer vollständig am Zugriff auf die Plattform zu hindern, deaktivieren Sie alle Aliase dieses Benutzers.

> **Hinweis**
>
> Durch das Löschen eines Benutzers aus dem System wird nicht automatisch verhindert, dass sich der Benutzer erneut bei der BI-Plattform anmelden kann. Wenn das Benutzerkonto weiterhin im Drittherstellersystem vorhanden ist und einer Gruppe angehört, die der Plattform zugeordnet ist, kann sich der Benutzer noch beim System anmelden. Um sicherzustellen, dass ein Benutzer keinen seiner Aliase mehr zur Anmeldung bei der Plattform verwenden kann, empfiehlt es sich, die Aliase zu deaktivieren.

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Wählen Sie den Benutzer aus, dessen Alias Sie deaktivieren möchten.
3. Klicken Sie auf **Verwalten** > **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
4. Deaktivieren Sie das Kontrollkästchen **Aktiviert** für den Alias, den Sie deaktivieren möchten.

   Wiederholen Sie diesen Schritt für jeden Alias, den Sie deaktivieren möchten.
5. Klicken Sie auf **Speichern und schließen**.
   Der Benutzer ist nicht mehr in der Lage, sich mit dem gerade deaktivierten Authentifizierungstyp anzumelden.

Weitere Informationen

So löschen Sie einen Alias [Seite 122]

Wenn Sie einen Alias löschen, wird er aus dem System entfernt. Wenn ein Benutzer nur über einen Alias verfügt und Sie diesen Alias löschen, werden Benutzerkonto, Favoritenordner, persönliche Kategorien und Posteingang des jeweiligen Kontos automatisch vom System gelöscht.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7 Festlegen von Rechten

7.1 Funktionsweise von Rechten in der BI-Plattform

Rechte bilden die Grundlage für die Steuerung des Benutzerzugriffs auf Objekte, Benutzer, Anwendungen, Server und andere Funktionen in der BI-Plattform. Sie spielen eine wichtige Rolle bei der Systemsicherheit, da mit Rechten einzelne Aktionen festgelegt werden, die Benutzer für Objekte ausführen können. Außerdem können Sie mit Rechten den Zugriff auf Inhalte in der BI-Plattform steuern, die Benutzer- und Gruppenverwaltung an verschiedene Abteilungen delegieren und den Mitarbeitern der IT-Abteilung die Administratorberechtigung für Server und Servergruppen gewähren.

Beachten Sie, dass Rechte für Objekte wie Berichte und Ordner und nicht für die *Prinzipale* (die Benutzer und Gruppen) festgelegt werden, die darauf zugreifen. Um einem Abteilungsleiter beispielsweise Zugriff auf einen bestimmten Ordner im Bereich *Ordner* zu gewähren, nehmen Sie den Abteilungsleiter in die *Zugriffskontrollliste* (die Liste der Prinzipale, die Zugriff auf ein Objekt haben) für den Ordner auf. Sie können einem Abteilungsleiter keinen Zugriff gewähren, indem Sie dessen Rechteeinstellungen im Bereich *Benutzer und Gruppen* konfigurieren. Die Rechteeinstellungen des Abteilungsleiters im Bereich *Benutzer und Gruppen* werden verwendet, um anderen Prinzipalen (z.B. delegierten Administratoren) Zugriff auf den Abteilungsleiter als Objekt im System zu gewähren. Auf diese Weise stellen Prinzipale für andere Benutzer eine Art Objekt dar, das jedoch mit umfangreicheren Verwaltungsrechten ausgestattet ist.

Jedes Recht an einem Objekt kann gewährt, verweigert bzw. nicht angegeben werden. Das BI-Plattform-Sicherheitsmodell ist so konzipiert, dass ein nicht angegebenes Recht standardmäßig verweigert wird. Wenn Einstellungen dazu führen, dass ein Recht einem Benutzer oder einer Gruppe sowohl gewährt als auch verweigert wird, wird das Recht im Ergebnis verweigert. Mit diesem “verweigerungsorientierten” Prinzip wird gewährleistet, dass Benutzer und Gruppen nicht automatisch Rechte erhalten, die ihnen nicht explizit gewährt wurden.

Es gibt eine wichtige Ausnahme von dieser Regel. Wenn ein Recht für ein untergeordnetes Objekt explizit festgelegt wird und den vom übergeordneten Objekt übernommenen Rechten widerspricht, werden die übernommenen Rechte von dem für das untergeordnete Objekt festgelegten Recht überschrieben. Diese Ausnahme gilt für Benutzer, die auch Mitglieder von Gruppen sind. Wenn ein Recht, das der Gruppe eines Benutzers verweigert wurde, einem Benutzer explizit gewährt wird, werden die übernommenen Rechte durch das für den Benutzer festgelegte Recht überschrieben.

Weitere Informationen

Rechte überschreiben [Seite 128]

7.1.1 Zugriffsberechtigungen

Bei *Zugriffsberechtigungen* werden Rechte, die von Benutzern häufig verwendet werden, in Gruppen zusammengefasst. Sie bieten Administratoren die Möglichkeit, schnell einheitliche Sicherheitsebenen festzulegen, anstatt die einzelnen Rechte nacheinander zu definieren.

Die BI-Plattform wird mit mehreren vordefinierten Zugriffsberechtigungen ausgeliefert. Diese vordefinierten Zugriffsberechtigungen basieren auf einem Modell sukzessiv ansteigender Rechte, das mit *Ansicht* beginnt und

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

mit *Voller Zugriff* endet. Alle dazwischen liegenden Zugriffsberechtigungen bauen mehr oder weniger auf der vorherigen Zugriffsberechtigung auf.

Sie können jedoch eigene Zugriffsberechtigungen erstellen und anpassen. Dadurch lassen sich administrative Kosten und Verwaltungskosten in Zusammenhang mit der Sicherheit deutlich reduzieren. Stellen Sie sich eine Situation vor, in der ein Administrator zwei Gruppen verwalten muss: Vertriebsmanager und Vertriebsmitarbeiter. Beide Gruppen müssen auf fünf Berichte im BI-Plattform-System zugreifen, Vertriebsmanager benötigen jedoch mehr Rechte als Vertriebsmitarbeiter. Die vordefinierten Zugriffsberechtigungen erfüllen nicht die Anforderungen dieser beiden Gruppen. Anstatt den einzelnen Berichten Gruppen als Subjekte hinzuzufügen und die zugehörigen Rechte an fünf verschiedenen Orten zu ändern, kann der Administrator zwei neue Zugriffsberechtigungen erstellen: Vertriebsmanager und Vertriebsmitarbeiter. Der Administrator fügt den Berichten dann beide Gruppen als Subjekte hinzu und weist den Gruppen die entsprechenden Zugriffsberechtigungen zu. Wenn Rechte geändert werden müssen, kann der Administrator die Zugriffsberechtigungen bearbeiten. Da die Zugriffsberechtigungen für beide Gruppen in allen fünf Berichten gelten, werden die Rechte, über die diese Gruppen für die Berichte verfügen, schnell aktualisiert.

Weitere Informationen

Arbeiten mit Zugriffsberechtigungen [Seite 139]

7.1.2 Einstellungen für erweiterte Rechte

Um vollständige Kontrolle über die Objektsicherheit zu erhalten, bietet Ihnen die CMC die Möglichkeit, *erweiterte Rechte* festzulegen. Diese erweiterten Rechte bieten mehr Flexibilität, da die Sicherheit für Objekte detaillierter festgelegt werden kann.

Sie können Einstellungen für erweiterte Rechte z.B. verwenden, wenn Sie die Rechte eines Prinzipals für ein bestimmtes Objekt oder eine Gruppe von Objekten anpassen möchten. Setzen Sie insbesondere dann erweiterte Rechte ein, wenn Sie einem Benutzer oder einer Gruppe ein bestimmtes Recht verweigern möchten, das sich nicht ändern soll, wenn Sie zu einem späteren Zeitpunkt Änderungen an Gruppenzugehörigkeiten oder Sicherheitsebenen von Ordnern vornehmen.

In der folgenden Tabelle sind die Optionen zusammengefasst, die Ihnen beim Festlegen erweiterter Rechte zur Verfügung stehen.

Tabelle 6: Rechteoptionen

Symbol	Rechteoption	Beschreibung
	Gewährt	Das Recht wird einem Subjekt gewährt.
	Verweigert	Das Recht wird einem Subjekt verweigert.
	Nicht angegeben	Das Recht wird für ein Subjekt nicht angegeben. Auf **Nicht angegeben** festgelegte Rechte sind standardmäßig verweigert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Symbol	Rechteoption	Beschreibung
	Auf Objekt anwenden	Das Recht wird auf das Objekt angewendet. Diese Option ist verfügbar, wenn Sie auf **Gewährt** oder **Verweigert** klicken.
	Auf Unterobjekt anwenden	Das Recht wird auf Unterobjekte angewendet. Diese Option ist verfügbar, wenn Sie auf **Gewährt** oder **Verweigert** klicken.

Weitere Informationen

Typspezifische Rechte [Seite 131]

7.1.3 Übernahme

Objektrechte werden für einen Prinzipal festgelegt, um den Zugriff auf das jeweilige Objekt zu steuern. Dabei erweist es sich jedoch als undurchführbar, den expliziten Wert jedes möglichen Rechts für jeden Prinzipal an jedem Objekt zu definieren. Stellen Sie sich beispielsweise ein System mit 100 Rechten, 1000 Benutzern und 10.000 Objekten vor: Um die Rechte explizit für jedes Objekt festzulegen, müssten im CMS-Speicher zigtausende von Rechten gespeichert werden, die darüber hinaus von einem Administrator auch noch einzeln festgelegt werden müssten.

Mit Übernahmemustern lässt sich dies umgehen. Bei Verwendung der Übernahme stammen die Rechte, die Benutzern an den im System enthaltenen Objekten gewährt werden, aus einer Kombination ihrer Mitgliedschaften in unterschiedlichen Gruppen und Untergruppen mit Objekten, die Rechte von übergeordneten Ordnern und Unterordnern übernommen haben. Diese Benutzer können Rechte infolge einer Gruppenmitgliedschaft übernehmen, Untergruppen können Rechte von übergeordneten Gruppen übernehmen, und sowohl Benutzer als auch Gruppen können Rechte von übergeordneten Ordnern übernehmen.

Standardmäßig übernehmen Benutzer oder Gruppen, die Rechte für einen Ordner besitzen, dieselben Rechte für jedes Objekt, das nachfolgend in diesem Ordner veröffentlicht wird. Daher ist es strategisch ratsam, zuerst die entsprechenden Rechte für Benutzer und Gruppen auf Ordnerebene festzulegen und dann die Objekte in diesem Ordner zu veröffentlichen.

Die BI-Plattform erkennt zwei Arten der Übernahme: Gruppenübernahme und Ordnerübernahme.

7.1.3.1 Gruppenübernahme

Bei der Gruppenübernahme können Prinzipale Rechte infolge einer Gruppenzugehörigkeit übernehmen. Die Gruppenübernahme ist besonders nützlich, wenn Sie alle Benutzer in Gruppen organisieren, die den aktuellen Sicherheitskonventionen Ihres Unternehmens entsprechen.

Aus “Gruppenübernahme: Beispiel 1” ist ersichtlich, wie die Gruppenübernahme funktioniert. Da die rote Gruppe eine Untergruppe der blauen Gruppe ist, übernimmt sie die Rechte der blauen Gruppe. In diesem Fall übernimmt

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

die Gruppe Recht 1 als "Gewährt" und die übrigen Rechte als "Nicht angegeben". Jedes Mitglied der roten Gruppe übernimmt diese Rechte. Darüber hinaus werden alle weiteren, für die Untergruppe festgelegten Rechte von deren Mitgliedern übernommen. Da der grüne Benutzer in diesem Beispiel ein Mitglied der roten Gruppe ist, übernimmt er Recht 1 als "Gewährt", die Rechte 2, 3, 4 und 6 als "Nicht angegeben" und Recht 5 als "Verweigert".

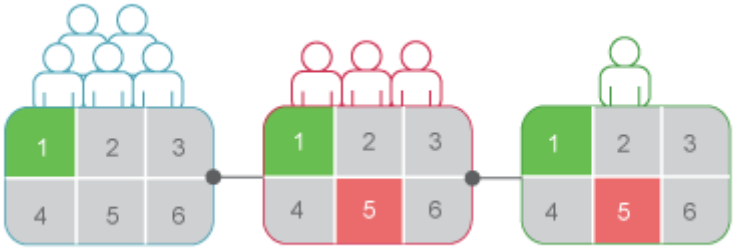


Abbildung 1: Gruppenübernahme: Beispiel 1

Wenn die Gruppenübernahme für einen Benutzer aktiviert ist, der mehreren Gruppen angehört, werden die Rechte aller übergeordneten Gruppen berücksichtigt, wenn das System die Anmeldedaten prüft. Dem Benutzer werden alle Rechte verweigert, die in einer der übergeordneten Gruppen explizit verweigert wurden, sowie jegliche Rechte, deren Status vollständig "Nicht angegeben" lautet. Folglich werden dem Benutzer nur die Rechte gewährt, die (explizit oder durch Zugriffsberechtigungen) in einer oder mehreren Gruppen gewährt und nie explizit verweigert wurden.

In “Gruppenübernahme: Beispiel 2” ist der grüne Benutzer Mitglied in zwei Gruppen, die voneinander unabhängig sind. Der grüne Benutzer übernimmt von der blauen Gruppe die Rechte 1 und 5 als "Gewährt" und die übrigen Rechte als "Nicht angegeben". Da der grüne Benutzer jedoch auch der roten Gruppe angehört und der roten Gruppe Recht 5 explizit verweigert wurde, wird die Übernahme von Recht 5 aus der blauen Gruppe außer Kraft gesetzt.

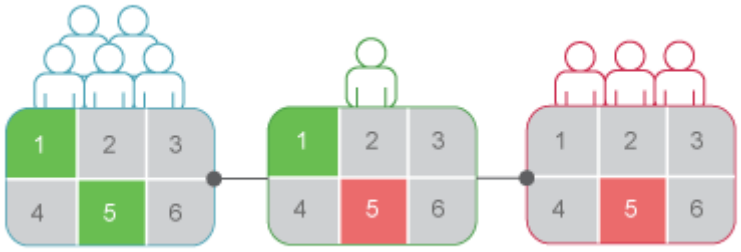


Abbildung 2: Gruppenübernahme: Beispiel 2

Weitere Informationen

Rechte überschreiben [Seite 128]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7.1.3.2 Ordnerübernahme

Die Ordnerübernahme ermöglicht Prinzipalen die Übernahme aller Rechte, die für den übergeordneten Ordner eines Objekts gewährt wurden. Die Ordnerübernahme erweist sich als besonders leistungsfähig, wenn Sie BI-Plattform-Inhalte in einer Ordnerhierarchie organisieren, die die aktuellen Sicherheitskonventionen Ihres Unternehmens widerspiegelt. Angenommen, Sie erstellen einen Ordner namens "Vertriebsberichte" und gewähren der Gruppe "Vertrieb" für diesen Ordner das Recht *Ansicht auf Abruf*. Standardmäßig übernimmt jeder Benutzer, der Rechte für den Ordner "Vertriebsberichte" besitzt, dieselben Rechte für alle Berichte, die Sie nachfolgend in diesem Ordner veröffentlichen. Folglich verfügt die Gruppe "Vertrieb" für alle Berichte über den Zugriff *Ansicht auf Abruf*, und die Objektrechte müssen nur einmal auf der Ordnerebene festgelegt werden.

In “Beispiel für die Ordnerübernahme” wurden für die rote Gruppe Ordnerrechte festgelegt. Rechte 1 und 5 wurden gewährt, während die übrigen Rechte nicht angegeben wurden. Bei aktivierter Ordnerübernahme verfügen Mitglieder der roten Gruppe über Rechte auf der Objektebene, die mit den Rechten der Gruppe auf der Ordnerebene identisch sind. Die Rechte 1 und 5 wurden als "Gewährt" übernommen, während die übrigen Rechte nicht angegeben wurden.

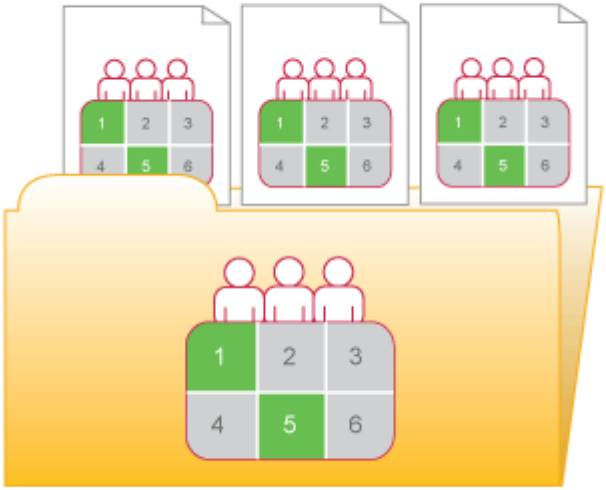


Abbildung 3: Beispiel für die Ordnerübernahme

Weitere Informationen

Rechte überschreiben [Seite 128]

7.1.3.3 Rechte überschreiben

Das *Überschreiben von Rechten* ist ein Verhalten, bei dem Rechte, die für untergeordnete Objekte festgelegt wurden, die für übergeordnete Objekte festgelegten Rechte überschreiben. Das Überschreiben von Rechten findet unter folgenden Bedingungen statt:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Im Allgemeinen überschreiben die Rechte, die für untergeordnete Objekte festgelegt werden, die Rechte, die für übergeordnete Objekte festgelegt werden.
- Im Allgemeinen überschreiben die Rechte, die für Untergruppen oder Gruppenelemente festgelegt werden, die Rechte, die für Gruppen festgelegt werden.

Die Übernahme muss nicht deaktiviert werden, um benutzerdefinierte Rechte für ein Objekt festzulegen. Das untergeordnete Objekt übernimmt die Rechteeinstellungen des übergeordneten Objekts, mit Ausnahme der Rechte, die explizit für das untergeordnete Objekt festgelegt werden. Alle Änderungen an den Rechteeinstellungen für das übergeordnete Objekt gelten auch für das untergeordnete Objekt.

"Rechte überschreiben: Beispiel 1" verdeutlicht, wie das Überschreiben von Rechten für übergeordnete und untergeordnete Objekte funktioniert. Dem blauen Benutzer wird das Recht zur Bearbeitung eines Ordnerinhalts verweigert. Die Rechteeinstellung wird vom Unterordner übernommen. Ein Administrator gewährt dem blauen Benutzer jedoch *Bearbeitungs*rechte für ein Dokument im Unterordner. Das *Bearbeitungs*recht, das der blaue Benutzer für das Dokument erhält, überschreibt die übernommenen Rechte des Ordners und Unterordners.

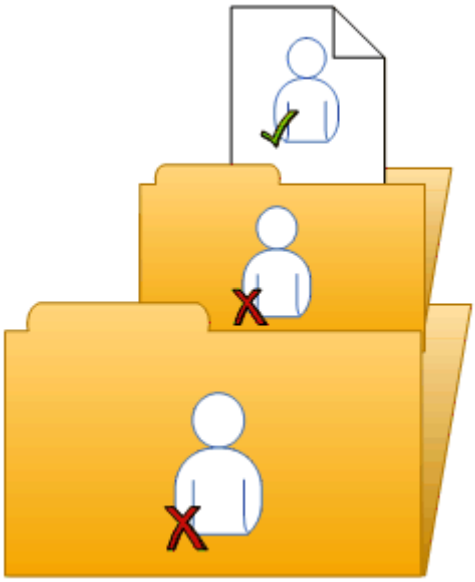


Abbildung 4: Rechte überschreiben: Beispiel 1

"Rechte überschreiben: Beispiel 2" verdeutlicht, wie das Überschreiben von Rechten für Mitglieder und Gruppen funktioniert. Der blauen Gruppe wird das Recht zur Bearbeitung eines Ordners verweigert. Die blaue Untergruppe übernimmt diese Rechteeinstellung. Ein Administrator gewährt dem blauen Benutzer, der Mitglied der blauen Gruppe und der blauen Untergruppe ist, jedoch *Bearbeitungs*rechte für den Ordner. Die *Bearbeitungs*rechte, die der blaue Benutzer für den Ordner erhält, überschreiben die übernommenen Rechte der blauen Gruppe und der blauen Untergruppe.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

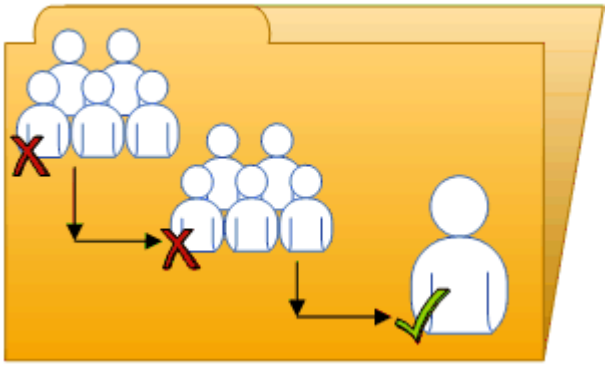


Abbildung 5: Rechte überschreiben: Beispiel 2

“Komplexes Überschreiben von Rechten” veranschaulicht eine Situation, in der die Auswirkungen des Überschreibens von Rechten weniger transparent sind. Der violette Benutzer ist ein Mitglied der Untergruppen 1A und 2A, die der Gruppe 1 bzw. 2 angehören. Die Gruppen 1 und 2 verfügen über *Bearbeitungs*rechte für den Ordner. 1A übernimmt die *Bearbeitungs*rechte von Gruppe 1, die *Bearbeitungs*rechte für 2A werden jedoch von einem Administrator verweigert. Die Rechteeinstellungen für 2A überschreiben aufgrund von "Rechte überschreiben" die Rechteeinstellungen für Gruppe 2. Der violette Benutzer übernimmt deshalb widersprüchliche Rechteeinstellungen von 1A und 2A. Zwischen 1A und 2A besteht keine Parent-/Child-Beziehung, sodass keine Überschreibung von Rechten stattfindet. Die Rechteeinstellungen einer Untergruppe überschreiben also keine Rechteinstellungen einer anderen Gruppe, da sie einen gleichwertigen Status haben. Dem violetten Benutzer werden also aufgrund des auf *Verweigerungen* basierenden Rechtemodells in der BI-Plattform “ Bearbeitungsrechte” verweigert.

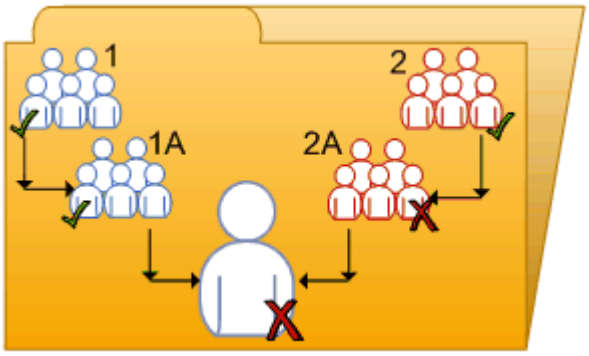


Abbildung 6: Komplexes Überschreiben von Rechten

Mit "Rechte überschreiben" können Sie geringfügige Änderungen an den Rechteeinstellungen für ein untergeordnetes Objekt vornehmen, ohne sämtliche übernommenen Rechteeinstellungen zu ignorieren. Stellen Sie sich eine Situation vor, in der ein Vertriebsmanager Einsicht in vertrauliche Berichte im Ordner "Vertraulich" nehmen muss. Der Vertriebsmanager gehört der Gruppe "Vertrieb" an, der der Zugriff auf den Ordner und dessen Inhalt verweigert wurde. Der Administrator gewährt dem Manager *Ansichts*rechte für den Ordner "Vertraulich" und verweigert der Gruppe "Vertrieb" weiterhin den Zugriff. In diesem Fall wird der verweigerte Zugriff, den der Manager durch die Mitgliedschaft in der Gruppe "Vertrieb" übernommen hat, durch die dem Vertriebsmanager gewährten *Ansichts*rechte überschrieben.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7.1.3.4 Gültigkeitsbereich von Rechten

Der *Gültigkeitsbereich von Rechten* bezieht sich auf die Fähigkeit, das Ausmaß der Übernahme von Rechten einzuschränken. Um den Gültigkeitsbereich eines Rechts festzulegen, entscheiden Sie, ob das Recht auf das Objekt, seine Unterobjekte oder beides angewendet wird. Der Gültigkeitsbereich eines Rechts erstreckt sich standardmäßig sowohl auf Objekte als auch auf Unterobjekte.

Der Gültigkeitsbereich von Rechten kann verwendet werden, um persönlichen Inhalt an freigegebenen Speicherorten zu schützen. Stellen Sie sich eine Situation vor, in der die Finanzabteilung einen gemeinsamen Ordner "Kostenabrechnungen" führt, der jeweils einen Unterordner "Persönliche Kostenabrechnungen" für die einzelnen Mitarbeiter enthält. Die Mitarbeiter möchten in der Lage sein, den Ordner "Kostenabrechnungen" einzusehen und ihm Objekte hinzuzufügen. Gleichzeitig möchten Sie den Inhalt ihrer Unterordner "Persönliche Kostenabrechnungen" schützen. Der Administrator gewährt allen Mitarbeitern *Ansichts*- und *Hinzufüge*rechte für den Ordner "Kostenabrechnungen" und beschränkt den Gültigkeitsbereich dieser Rechte auf den Ordner "Kostenabrechnungen". Dies bedeutet, dass die *Ansichts*- und *Hinzufüge*berechtigungen nicht für Unterobjekte im Ordner "Kostenabrechnungen" gelten. Der Administrator gewährt den Mitarbeitern dann *Ansichts*- und *Hinzufüge*rechte für ihre eigenen Unterordner "Persönliche Kostenabrechnungen".

Durch den Gültigkeitsbereich von Rechten können auch die effektiven Rechte beschränkt werden, über die ein delegierter Administrator verfügt. Ein delegierter Administrator kann über die Rechte *Sicher Rechte ändern* und *Bearbeiten* für einen Ordner verfügen, der Gültigkeitsbereich dieser Rechte ist jedoch nur auf den Ordner beschränkt und umfasst nicht dessen Unterobjekte. Der delegierte Administrator kann diese Rechte für eines der Unterobjekte des Ordners keinem anderen Benutzer gewähren.

7.1.4 Typspezifische Rechte

Typspezifische Rechte sind Rechte, die sich nur auf bestimmte Objekttypen wie Crystal-Reports-Berichte, Ordner oder Zugriffsberechtigungen auswirken. Typspezifische Rechte umfassen:

- Allgemeine Rechte für den Objekttyp

  Diese Rechte sind identisch mit allgemeinen globalen Rechten (z.B. dem Recht zum Hinzufügen, Löschen oder Bearbeiten eines Objekts), Sie legen sie jedoch auf spezifische Objekttypen fest, um die allgemeinen globalen Rechteeinstellungen zu überschreiben.
- Spezifische Rechte für den Objekttyp

  Diese Rechte sind nur für spezifische Objekttypen verfügbar. Das Recht zum Exportieren von Berichtsdaten wird beispielsweise für Crystal-Reports-Berichte, nicht aber für Word-Dokumente angezeigt.

Durch das Diagramm “Beispiel für typspezifische Rechte” wird veranschaulicht, wie typspezifische Rechte funktionieren. Recht 3 entspricht dem Recht zur Bearbeitung eines Objekts. Der blauen Gruppe werden *Bearbeitung*srechte für Ordner der obersten Ebene verweigert und *Bearbeitung*srechte für Crystal-Reports-Berichte im Ordner und Unterordner gewährt. Diese *Bearbeitung*srechte sind spezifisch für Crystal-Reports-Berichte und überschreiben die Rechteeinstellungen auf einer allgemeinen globalen Ebene. Folglich verfügen Mitglieder der blauen Gruppe über *Bearbeitungsrechte* für Crystal-Reports-Berichte, aber nicht für die XLF-Datei im Unterordner.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

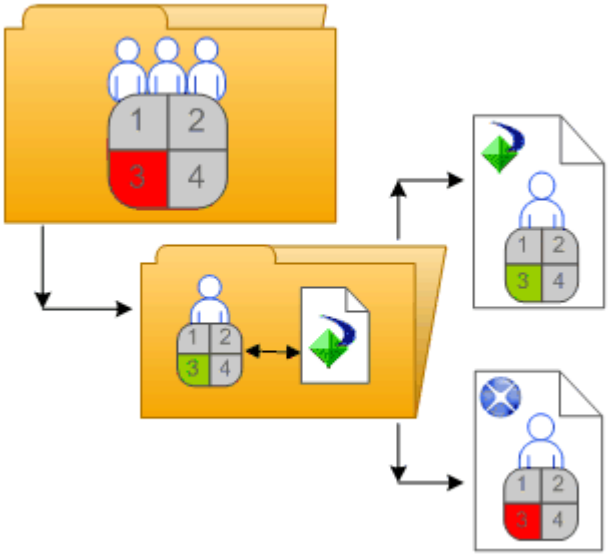


Abbildung 7: Beispiel für typspezifische Rechte

Typspezifische Rechte sind hilfreich, da Sie mit ihnen die Rechte von Subjekten auf der Grundlage des Objekttyps beschränken können. Stellen Sie sich eine Situation vor, in der ein Administrator seine Mitarbeiter dazu befähigen möchte, einem Ordner Objekte hinzuzufügen, aber keine Unterordner zu erstellen. Der Administrator gewährt *Hinzufüge*rechte auf allgemeiner globaler Ebene für den Ordner und verweigert dann *Hinzufüge*rechte für den Ordnerobjekttyp.

Rechte werden auf der Grundlage der jeweiligen Objekttypen in die folgenden Sammlungen unterteilt.

- *Allgemein*

  Diese Rechte wirken sich auf alle Objekte aus.
- *Inhalt*

  Diese Rechte werden entsprechend den verschiedenen Inhaltsobjekttypen unterteilt. Beispiele für Inhaltsobjekttypen sind Crystal-Reports-Berichte und Adobe Acrobat PDFs.
- *Anwendung*

  Diese Rechte werden danach unterteilt, auf welche BI-Plattform-Anwendung sie sich auswirken. Beispiele für Anwendungen sind CMC und BI-Launchpad.
- *System*

  Diese Rechte werden danach unterteilt, auf welche zentralen Systemkomponenten sie sich auswirken. Beispiele für zentrale Systemkomponenten sind Kalender, Ereignisse sowie Benutzer und Gruppen.

Typspezifische Rechte befinden sich in der *Inhalts*-, *Anwendungs*- und *System*sammlung. In den einzelnen Sammlungen werden sie auf der Grundlage des Objekttyps weiter in Kategorien unterteilt.

7.1.5 Ermitteln effektiver Rechte

Berücksichtigen Sie diese Überlegungen beim Festlegen von Rechten für ein Objekt:

- Stattdessen gewährt jede Zugriffsberechtigung bestimmte Rechte, verweigert bestimmte Rechte und behält für die übrigen Rechte die Einstellung "Nicht angegeben" bei. Wenn einem Benutzer mehrere

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Zugriffsberechtigungen zugewiesen werden, aggregiert das System die effektiven Rechte und verweigert standardmäßig alle nicht angegebenen Rechte.

- Wenn Sie einem Subjekt, das einem Objekt zugeordnet ist, mehrere Zugriffsberechtigungen zuweisen, verfügt das Subjekt über die Kombination der Rechte für die einzelnen Zugriffsberechtigungen. Dem Benutzer in " Mehrere Zugriffsberechtigungen" werden zwei Zugriffsberechtigungen zugewiesen. Durch eine Zugriffsberechtigung werden die Benutzerrechte 3 und 4 und durch die andere Zugriffsberechtigung nur Recht 3 gewährt. Die effektiven Rechten für den Benutzer sind die Rechte 3 und 4.

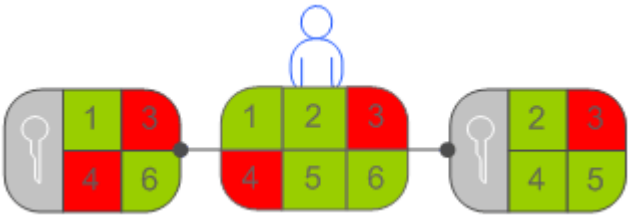


Abbildung 8: Mehrere Zugriffsberechtigungen

- Erweiterte Rechte können mit Zugriffsberechtigungen kombiniert werden, um die Rechteeinstellungen für ein einem Objekt zugewiesenes Subjekt anzupassen. Wenn ein erweitertes Recht und eine Zugriffsberechtigung beide explizit einem Prinzipal zugewiesen sind, der einem Objekt zugeordnet ist, und das erweiterte Recht einem Recht in der Zugriffsberechtigung widerspricht, wird das Recht in der Zugriffsberechtigung vom erweiterten Recht überschrieben.

  Identische Rechte in Zugriffsberechtigungen können durch erweiterte Rechte nur überschrieben werden, wenn sie für dasselbe Objekt desselben Prinzipals festgelegt wurden. Beispiel: Ein erweitertes Hinzufügerecht, das auf der allgemeinen globalen Ebene festgelegt wurde, kann die allgemeine Einstellung für das Hinzufügerecht in einer Zugriffsberechtigung überschreiben, es kann jedoch keine typspezifische Einstellung für das Hinzufügerecht in einer Zugriffsberechtigung überschreiben. Zugriffsberechtigungen werden jedoch nicht immer durch erweiterte Rechte überschrieben. Einem Prinzipal wird beispielsweise das *Bearbeitungsrecht* für ein übergeordnetes Objekt verweigert. Für das untergeordnete Objekt wird dem Prinzipal eine Zugriffsberechtigung zugewiesen, durch die ihm das *Bearbeitungsrecht* gewährt wird. Der Prinzipal verfügt schließlich über *Bearbeitungsrechte* für das untergeordnete Objekt, da die für das untergeordnete Objekt festgelegten Rechte die Rechte überschreiben, die für das übergeordnete Objekt festgelegt sind.
- Auf diese Weise können Rechte, die für ein untergeordnetes Objekt festgelegt wurden, Rechte überschreiben, die vom übergeordneten Objekt übernommen werden.

7.2 Verwalten von Sicherheitseinstellungen für Objekte in der CMC

Sie können Sicherheitseinstellungen für die meisten Objekte in der CMC unter Verwendung der Sicherheitsoptionen im Menü **Verwalten** verwalten. Mit diesen Optionen können Sie der Zugriffskontrollliste für ein Objekt Prinzipale zuweisen, die Rechte eines Prinzipals anzeigen lassen und die Rechte des Prinzipals für ein Objekt ändern.

Die jeweiligen Einstellungen der Sicherheitsverwaltung hängen von den Sicherheitsanforderungen und dem Objekttyp ab, für den Sie Rechte festlegen. Die Arbeitsabläufe für die folgenden Aufgaben sind jedoch im Allgemeinen sehr ähnlich:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Anzeigen von Rechten für ein einem Objekt zugewiesenes Subjekt
- Zuweisen von Prinzipalen zu einer Zugriffskontrollliste für ein Objekt und Festlegen der Rechte und Zugriffsberechtigungen für diese Prinzipale
- Festlegen von Rechten für einen Ordner der obersten Ebene in der BI-Plattform

7.2.1 So lassen Sie Rechte für einen Prinzipal auf einem Objekt anzeigen

Im Allgemeinen führen Sie diesen Arbeitsablauf aus, um Rechte für ein einem Objekt zugewiesenen Prinzipal anzuzeigen.

1. Wählen Sie das Objekt aus, für das Sie Sicherheitseinstellungen anzeigen möchten.
2. Klicken Sie auf **Verwalten** > **Benutzersicherheit**.
   Das Dialogfeld *Benutzersicherheit* wird angezeigt und enthält die Zugriffskontrollliste für das Objekt.
3. Wählen Sie einen Prinzipal aus der Zugriffskontrollliste aus, und klicken Sie auf **Sicherheit anzeigen**

   Der *Berechtigungs-Explorer* wird gestartet und zeigt eine Liste der effektiven Rechte für den dem Objekt zugewiesenen Prinzipal an. Zusätzlich können Sie im *Berechtigungs-Explorer* folgende Schritte ausführen:

   - Suchen nach einem anderen Prinzipal, dessen Rechte angezeigt werden sollen
   - Filtern Sie die angezeigten Rechte entsprechend den folgenden Kriterien:

     zugewiesene Rechte
     gewährte Rechte
     nicht zugewiesene Rechte
     Zugriffsberechtigung
     Objekttyp
     den Namen des Rechts
   - Sortieren Sie die Liste der angezeigten Rechte aufsteigend oder absteigend nach den folgenden Kriterien:

     Sammlung
     Typ
     Rechtename
     Rechtestatus ("Gewährt", "Verweigert" oder "Nicht angegeben")

   Zusätzlich können Sie auf einen der Links in der Spalte *Quelle* klicken, um die Quelle der übernommenen Rechte anzuzeigen.

7.2.2 So weisen Sie einer Zugriffskontrollliste für ein Objekt Prinzipale hinzu

In einer Zugriffskontrollliste werden die Benutzer angegeben, denen Rechte für ein Objekt gewährt oder verweigert werden. Im Allgemeinen führen Sie diesen Arbeitsablauf aus, um einer Zugriffkontrollliste einen Prinzipal zuzuweisen und die Rechte anzugeben, über die der Prinzipal für das betreffende Objekt verfügt.

1. Wählen Sie das Objekt aus, für das Sie ein Subjekt hinzufügen möchten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Klicken Sie auf **Verwalten** > **Benutzersicherheit**.
   Das Dialogfeld *Benutzersicherheit* wird angezeigt und enthält die Zugriffskontrollliste.
3. Klicken Sie auf **Prinzipale hinzufügen**.
   Das Dialogfeld *Prinzipale hinzufügen* wird angezeigt.
4. Verschieben Sie die Benutzer und Gruppen, die Sie als Prinzipale hinzufügen möchten, aus der Liste **Verfügbare Benutzer/Gruppen** in die Liste **Ausgewählte Benutzer/Gruppen**.
5. Klicken Sie auf **Sicherheit hinzufügen und zuweisen**.
6. Wählen Sie die Zugriffsberechtigungen aus, die Sie dem Prinzipal gewähren möchten.
7. Wählen Sie aus, ob die Übernahme von Ordnern oder Gruppen aktiviert oder deaktiviert werden soll.

Falls erforderlich, können Sie auch Rechte auf Detailebene ändern, um bestimmte Rechte in einer Zugriffsberechtigung zu überschreiben.

Weitere Informationen

Ändern der Sicherheit für einen Prinzipal auf einem Objekt [Seite 135]

7.2.3 Ändern der Sicherheit für einen Prinzipal auf einem Objekt

Allgemein wird empfohlen, dass Sie Zugriffsberechtigungen verwenden, um einem Prinzipal Rechte zuzuweisen. Zeitweise kann es jedoch erforderlich sein, bestimmte genau abgestimmte Rechte in einer Zugriffsberechtigung zu überschreiben. Über erweiterte Rechte können Sie die Rechte für ein Subjekt anpassen, und zwar zusätzlich zu den Zugriffsberechtigungen, über die das Subjekt bereits verfügt. Im Allgemeinen führen Sie diesen Arbeitsablauf aus, um einem Prinzipal erweiterte Rechte für ein Objekt zuzuweisen.

1. Weisen Sie den Prinzipal der Zugriffskontrollliste für das Objekt zu.
2. Nachdem der Prinzipal hinzugefügt wurde, wechseln Sie zu **Verwalten** > **Benutzersicherheit**, um die Zugriffskontrollliste für das Objekt anzuzeigen.
3. Wählen Sie einen Prinzipal aus der Zugriffskontrollliste aus, und klicken Sie auf **Sicherheit zuweisen**.
   Das Dialogfeld *Sicherheit zuweisen* wird angezeigt.
4. Klicken Sie auf die Registerkarte **Erweitert**.
5. Klicken Sie auf **Rechte hinzufügen/entfernen**.
6. Ändern Sie die Rechte für den Prinzipal.
   Alle verfügbaren Rechte sind im *Anhang "Rechte"* zusammengefasst.

Weitere Informationen

So weisen Sie einer Zugriffskontrollliste für ein Objekt Prinzipale hinzu [Seite 134]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7.2.4 Festlegen von Rechten für einen Ordner der obersten Ebene in der BI-Plattform

Im Allgemeinen führen Sie diesen Workflow aus, um Rechte für einen Ordner der obersten Ebene in der BI-Plattform festzulegen.

> **Hinweis**
>
> Für diese Version erfordern Prinzipale *Ansichts*rechte für einen Containerordner, damit sie in diesem Ordner navigieren und dessen Unterobjekte anzeigen lassen können. Dies bedeutet, dass Prinzipale *Ansichts*rechte für die Ordner der obersten Ebene benötigen, um die in Ordnern enthaltenen Objekte anzuzeigen. Wenn Sie die *Ansichts*rechte für einen Prinzipal beschränken möchten, können Sie einem Prinzipal *Ansichts*rechte für einen bestimmten Ordner gewähren und den Gültigkeitsbereich der Rechte so festlegen, dass sie nur für diesen Ordner gelten.

1. Wechseln Sie zum CMC-Bereich, in dem der Ordner der obersten Ebene festgelegt wird, für den Sie Rechte festlegen möchten.
2. Klicken Sie auf **Verwalten** > **Sicherheit auf oberster Ebene** > **Alle** `<Objekte>`.

   Hier steht der Begriff `<Objekte>` für den Inhalt des Ordners der obersten Ebene. Wenn Sie zum Bestätigen aufgefordert werden, klicken Sie auf **OK**.

   Das Dialogfeld *Benutzersicherheit* wird angezeigt und enthält die Zugriffskontrollliste für den Ordner der obersten Ebene.
3. Weisen Sie der Zugriffskontrollliste das Subjekt für den Ordner der obersten Ebene zu.
4. Weisen Sie dem Subjekt ggf. erweiterte Rechte zu.

Weitere Informationen

So weisen Sie einer Zugriffskontrollliste für ein Objekt Prinzipale hinzu [Seite 134]
Ändern der Sicherheit für einen Prinzipal auf einem Objekt [Seite 135]

7.2.5 Überprüfen von Sicherheitseinstellungen für ein Subjekt

In einigen Fällen möchten Sie vielleicht wissen, für welche Objekte einem Prinzipal Zugriff gewährt oder verweigert wurde. Zu diesem Zweck können Sie eine Sicherheitsabfrage verwenden. Anhand von Sicherheitsabfragen können Sie die Objekte ermitteln, für die ein Subjekt über bestimmte Rechte verfügt sowie die Benutzerrechte verwalten. Für jede Sicherheitsabfrage geben Sie folgende Informationen an:

- Abfrageprinzipal

  Sie geben den Benutzer oder die Gruppe an, für die die Sicherheitsabfrage ausgeführt werden soll. Sie können ein Subjekt pro Sicherheitsabfrage angeben.
- Abfrageberechtigung

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Sie geben das Recht bzw. die Rechte an, für die die Sicherheitsabfrage ausgeführt werden soll, sowie den Status dieser Rechte und den Objekttyp, für den diese Rechte festgelegt wurden. Beispiel: Sie können eine Sicherheitsabfrage für alle Berichte ausführen, die von einem Subjekt regeneriert werden können, sowie für alle Berichte, die ein Subjekt nicht exportieren kann.

- Abfragekontext

  Sie können die CMC-Bereiche angeben, die von der Sicherheitsabfrage durchsucht werden sollen. Für jeden Bereich können Sie auswählen, ob Unterobjekte in die Sicherheitsabfrage aufgenommen werden sollen. Eine Sicherheitsabfrage kann maximal vier Bereiche umfassen.

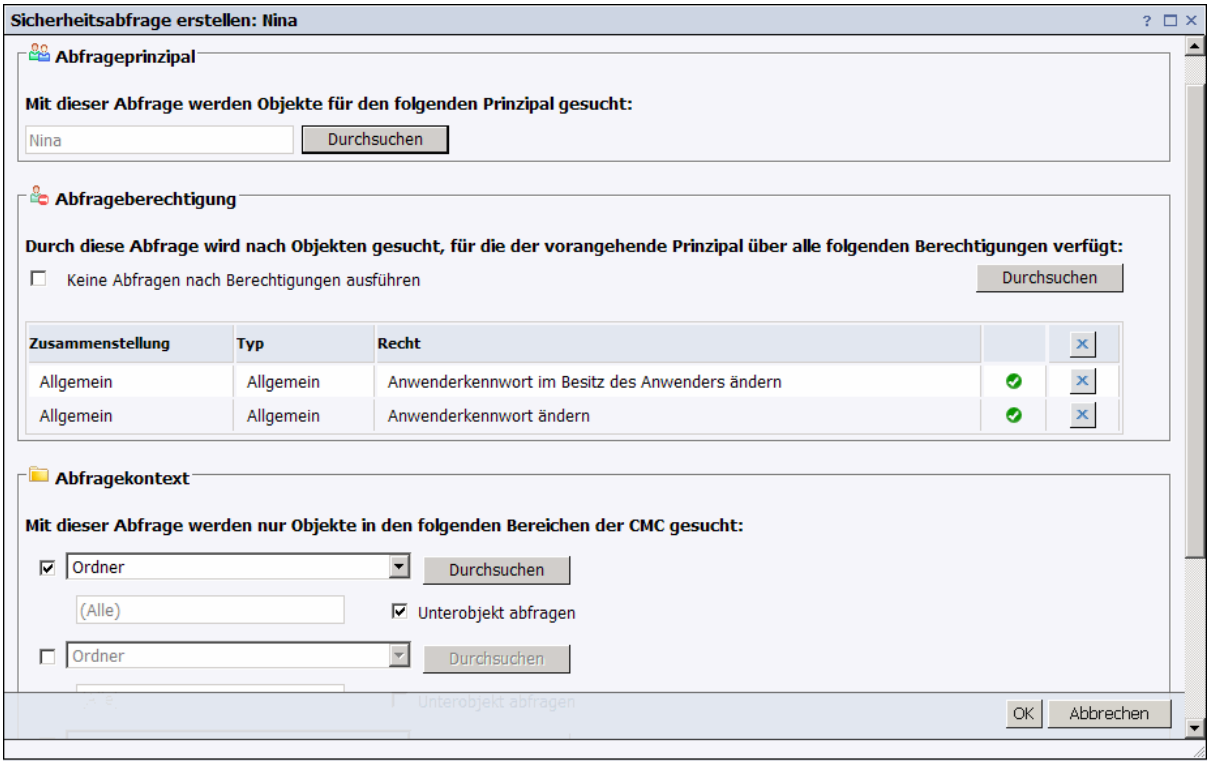
Wenn Sie eine Sicherheitsabfrage ausführen, werden die Ergebnisse im Bereich *Abfrageergebnisse* angezeigt, der sich im *Strukturbereich* unterhalb von **Sicherheitsabfragen** befindet. Wenn Sie eine Sicherheitsabfrage optimieren möchten, können Sie eine zweite Abfrage in den Ergebnissen der ersten Abfrage ausführen.

Sicherheitsabfragen sind hilfreich, da über sie Objekte angezeigt werden können, für die ein Subjekt bestimmte Rechte hat. Außerdem verweisen sie auf den Speicherort dieser Objekte, für den Fall, dass Sie diese Rechte ändern möchten. Stellen Sie sich eine Situation vor, in der ein Vertriebsmitarbeiter zum Vertriebsmanager befördert wird. Der Vertriebsmanager benötigt *Zeitsteuerungs*rechte für Crystal-Reports-Berichte, für die er zuvor nur über *Ansichts*rechte verfügte, und diese Berichte befinden sich in unterschiedlichen Ordnern. In diesem Fall führt der Administrator eine Sicherheitsabfrage aus, um das Ansichtsrecht des Vertriebsmanagers für Crystal-Reports-Berichte in allen Ordnern zu überprüfen, und nimmt Unterobjekte in die Abfrage auf. Nachdem die Sicherheitsabfrage ausgeführt wurde, kann der Administrator alle Crystal-Reports-Berichte, für die der Vertriebsmanager über *Ansichts*rechte verfügt, im Bereich *Abfrageergebnisse* anzeigen lassen. Da im *Detailbereich* der Pfad zu den einzelnen Crystal-Reports-Berichten angezeigt wird, kann der Administrator jeden Bericht suchen und die diesbezüglichen Rechte des Vertriebsmanagers ändern.

7.2.5.1 So führen Sie eine Sicherheitsabfrage aus

1. Wählen Sie im Bereich *Benutzer und Gruppen* im *Detailbereich* den Benutzer oder die Gruppe aus, für den bzw. die eine Sicherheitsabfrage ausgeführt werden soll.
2. Klicken Sie auf **Verwalten** > **Extras** > **Sicherheitsabfrage erstellen**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.



Das Dialogfeld *Sicherheitsabfrage erstellen* wird angezeigt.

3. Stellen Sie sicher, dass das Subjekt im Bereich **Abfragesubjekt** richtig ist.

   Wenn Sie sich entscheiden, eine Sicherheitsabfrage für ein anderes Subjekt auszuführen, können Sie auf **Durchsuchen** klicken, um ein anderes Subjekt auszuwählen. Erweitern Sie im Dialogfeld *Nach Abfrageprinzipal suchen* die Option **Benutzerliste** oder **Gruppenliste**, um den Prinzipal zu suchen oder die Namen der Prinzipale zu durchsuchen. Klicken Sie abschließend auf **OK**, um zum Dialogfeld *Sicherheitsabfrage erstellen* zurückzukehren.

4. Geben Sie im Bereich *Abfrageberechtigung* die Rechte und den Status der einzelnen Rechte an, für die Sie die Abfrage ausführen möchten.

   - Wenn Sie eine Abfrage für bestimmte Rechte ausführen möchten, über die der Prinzipal für Objekte verfügt, klicken Sie auf **Durchsuchen**, legen den Status der einzelnen Rechte fest, für die Sie die Sicherheitsabfrage ausführen möchten, und klicken auf **OK**.

     > **Tipp**
     >
     > Sie können spezifische Rechte aus der Abfrage löschen, indem Sie neben dem jeweiligen Recht auf die Schaltfläche zum Löschen klicken, oder Sie können alle Rechte aus der Abfrage löschen, indem Sie in der Kopfzeile auf die Schaltfläche zum Löschen klicken.

   - Zum Ausführen einer allgemeinen Sicherheitsabfrage aktivieren Sie das Kontrollkästchen **Keine Abfragen nach Berechtigungen ausführen**.

     In diesem Fall führt die BI-Plattform eine allgemeine Sicherheitsabfrage für alle Objekte aus, in deren Zugriffskontrolllisten der Prinzipal enthalten ist, und zwar unabhängig von den Berechtigungen, die der Prinzipal für die Objekte besitzt.

5. Geben Sie im Bereich *Abfragekontext* die CMC-Bereiche an, die Sie abfragen möchten.

   a) Aktivieren Sie ein Kontrollkästchen neben einer Liste.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

b) Wählen Sie in der Liste einen CMC-Bereich aus, den Sie abfragen möchten.

Wenn Sie einen spezifischeren Speicherort innerhalb eines Bereichs abfragen möchten (z.B. einen bestimmten Ordner unter "Ordner"), klicken Sie auf **Durchsuchen**, um das Dialogfeld *Nach Abfragekontext suchen* zu öffnen. Wählen Sie im *Detailbereich* den Ordner aus, den Sie abfragen möchten, und klicken Sie auf **OK**. Wenn Sie zum Dialogfeld **Sicherheitsabfrage** zurückkehren, wird der von Ihnen angegebene Ordner im Feld unterhalb der Liste angezeigt.

c) Wählen Sie **Unterobjekt abfragen**.

d) Wiederholen Sie die oben genannten Schritte für jeden CMC-Bereich, den Sie abfragen möchten.

> **Hinweis**
>
> Eine Abfrage kann maximal vier Bereiche umfassen.

6. Klicken Sie auf **OK**.
   Die Sicherheitsabfrage wird ausgeführt, und Sie wechseln zum Bereich *Abfrageergebnisse*.
7. Um die Abfrageergebnisse in der *Strukturansicht* anzuzeigen, erweitern Sie **Sicherheitsabfrage** und klicken auf ein Abfrageergebnis.

> **Tipp**
>
> Abfrageergebnisse werden nach den Namen der Subjekte aufgeführt.

Die Abfrageergebnisse werden im *Detailbereich* angezeigt.

Im Bereich *Abfrageergebnisse* werden sämtliche Ergebnisse von Sicherheitsabfragen einer einzelnen Benutzersitzung so lange beibehalten, bis sich der Benutzer abmeldet. Wenn Sie die Abfrage erneut mit neuen Spezifikationen ausführen möchten, klicken Sie auf **Aktionen** > **Abfrage bearbeiten**. Sie können auch dieselbe Abfrage erneut ausführen, indem Sie sie auswählen und auf **Aktionen** > **Abfrage erneut ausführen** klicken. Wenn Sie die Ergebnisse der Sicherheitsabfrage beibehalten möchten, klicken Sie auf **Aktionen** > **Exportieren**, um die Ergebnisse der Sicherheitsabfrage als CSV-Datei zu exportieren.

7.3 Arbeiten mit Zugriffsberechtigungen

Mit Zugriffsberechtigungen stehen Ihnen folgende Möglichkeiten zur Verfügung:

- Kopieren einer vorhandenen Zugriffsberechtigung, Vornehmen von Änderungen an der Kopie, Umbenennen und Speichern der Kopie als neue Zugriffsberechtigung
- Erstellen, Umbenennen und Löschen von Zugriffsberechtigungen.
- Ändern der Rechte in einer Zugriffsberechtigung.
- Verfolgen der Beziehung zwischen Zugriffsberechtigungen und anderen Objekten im System.
- Replizieren und Verwalten von Zugriffsberechtigungen über verschiedene Websites.
- Verwenden einer der vordefinierten Zugriffsberechtigungen in BI-Plattform, um Rechte für viele Subjekte schnell und einheitlich festzulegen.

In der folgenden Tabelle werden die Rechte zusammengefasst, die in den einzelnen vordefinierten Zugriffsberechtigungen enthalten sind.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Tabelle 7: Vordefinierte Zugriffsberechtigungen

Zugriffsberechtigung	Beschreibung	Zugehörige Rechte
Ansicht	Wenn diese Berechtigung auf Ordnerebene festgelegt wird, kann ein Prinzipal den Ordner, Objekte innerhalb des Ordners und die von den einzelnen Objekten generierten Instanzen anzeigen lassen. Wenn die Berechtigung auf Objektebene festgelegt wird, hat der Prinzipal Einblick in das Objekt, dessen Verlauf und die generierten Instanzen.	• Objekte anzeigen • Dokumentinstanzen anzeigen
Zeitgesteuert verarbeiten	Ein Prinzipal kann Instanzen generieren, indem er die zeitgesteuerte einmalige oder wiederkehrende Ausführung eines Objekts gegen eine festgelegte Datenquelle plant. Der Prinzipal kann die zeitgesteuerte Verarbeitung eigener Instanzen einsehen, löschen und anhalten. Außerdem können sie unterschiedliche Formate und Ziele zeitgesteuert planen, Parameter und Anmeldedaten für die Datenbank festlegen, Server zur Verarbeitung von Aufträgen auswählen, dem Ordner Inhalte hinzufügen und den Ordner oder das Objekt kopieren.	*Ansicht*srecht für die Zugriffsberechtigung UND: • Ausführung des Berichts zeitsteuern • Servergruppen für die Verarbeitung von Aufträgen definieren • Objekte in andere Ordner kopieren • Auf Ziele zeitgesteuert verarbeiten • Berichtsdaten drucken • Berichtsdaten exportieren • Objekte des Benutzers bearbeiten • Instanzen des Benutzers löschen • Instanzen des Benutzers anhalten und fortsetzen
Ansicht auf Abruf	Ein Prinzipal kann Daten "auf Abruf" gegen eine Datenquelle regenerieren.	*Zeitgesteuert verarbeiten*-Recht für Zugriffsberechtigungen UND: • Berichtsdaten regenerieren
Voller Zugriff	Ein Prinzipal hat vollständigen Verwaltungszugriff auf das Objekt.	Alle verfügbaren Rechte einschließlich: • Objekte zum Ordner hinzufügen • Objekte bearbeiten • Rechte ändern, die Benutzer für Objekte haben • Objekte löschen • Instanzen löschen

In der folgenden Tabelle werden die Rechte zusammengefasst, die zur Ausführung bestimmter Aufgaben für Zugriffsberechtigungen erforderlich sind.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Aufgabe für Zugriffsberechtigung	Erforderliche Rechte
Erstellen einer Zugriffsberechtigung	*Hinzufüge*recht für den Ordner *Zugriffsberechtigungen* der obersten Ebene
Anzeigen genau abgestimmter Rechte in einer Zugriffsberechtigung	*Ansicht*srecht für die Zugriffsberechtigung
Zuweisen einer Zugriffsberechtigung zu einem Subjekt, das einem Objekt zugewiesen ist	*Ansicht*srecht für die Zugriffsberechtigung *Zugriffsberechtigung für Sicherheitszuweisung verwenden*-Rechte für die Zugriffsberechtigung *Rechte ändern*-Recht für das Objekt oder *Sicher Rechte ändern*-Recht für das Objekt und den Prinzipal **Hinweis** Benutzern, die über das Recht *Sicher Rechte ändern* verfügen und einem Prinzipal eine Zugriffsberechtigung zuweisen möchten, muss dieselbe Zugriffsberechtigung zugewiesen sein.
Ändern einer Zugriffsberechtigung	*Ansichts*- und *Bearbeitung*srecht für die Zugriffsberechtigung
Löschen einer Zugriffsberechtigung	*Ansichts*- und *Lösch*recht für die Zugriffsberechtigung
Klonen einer Zugriffsberechtigung	*Ansicht*srecht für die Zugriffsberechtigung *Kopier*recht für die Zugriffsberechtigung *Hinzufüge*recht für den Ordner *Zugriffsberechtigungen* der obersten Ebene

7.3.1 Auswählen zwischen den Zugriffsberechtigungen *Ansicht* und *Ansicht auf Abruf*

Bei der Berichterstellung über das Web ist die Wahl zwischen Live- oder gespeicherten Daten eine der wichtigsten Entscheidungen, die Sie treffen werden. Unabhängig von Ihrer Wahl zeigt die BI-Plattform jedoch die erste Seite immer so schnell wie möglich an, damit Sie den Bericht bereits sehen können, während die restlichen Daten noch verarbeitet werden. In diesem Abschnitt wird der Unterschied zwischen zwei vordefinierten Zugriffsberechtigungen erläutert, unter denen Sie auswählen können.

Ansicht auf Abruf (Zugriffsberechtigung)

Mit der Berichterstellung auf Abruf können Benutzer in Echtzeit auf Live-Daten zugreifen, die direkt vom Datenbankserver abgerufen werden. Verwenden Sie Live-Daten, um Benutzer über sich konstant ändernde Informationen auf dem Laufenden zu halten, damit sie Zugang zu Informationen erhalten, die bis auf die Sekunde genau sind. Wenn beispielsweise die Manager eines großen Vertriebszentrums regelmäßig ausgelieferte Bestände nachverfolgen müssen, dann erhalten sie die benötigten Informationen am besten durch live erstellte Berichte.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Bevor Sie Live-Daten für alle Berichte bereitstellen, sollten Sie jedoch zuerst überlegen, ob der ständige Zugriff auf den Datenbankserver durch die Benutzer wirklich in Ihrem Sinne ist. Wenn sich Daten nicht schnell oder nicht ständig ändern, dann führen all diese Anfragen an die Datenbank nur zu erhöhtem Netzwerkverkehr und stärkerer Auslastung von Serverressourcen. In solchen Fällen sollten Sie Berichte wiederholt zeitgesteuert verarbeiten, damit Benutzer immer aktuelle Daten (Berichtsinstanzen) einsehen können, ohne auf den Datenbankserver zuzugreifen.

Benutzer benötigen das Zugriffsrecht *Ansicht auf Abruf*, um Berichte anhand der Datenbank zu regenerieren.

Ansicht **(Zugriffsberechtigung)**

Um den Netzwerkdatenverkehr und die bei den Datenbankservern eingehenden Abfragen zu reduzieren, können Sie Berichte zeitgesteuert verarbeiten lassen. Nachdem der Bericht ausgeführt wurde, können Benutzer die Berichtsinstanzen bei Bedarf anzeigen, ohne dass zusätzliche Datenbankabfragen ausgeführt werden müssen.

Berichtsinstanzen eignen sich für den Umgang mit Informationen, die nicht ständig aktualisiert werden. Wenn die Benutzer Berichtsinstanzen durchlesen und sich Einzelheiten in Spalten oder Diagrammen genauer anzeigen lassen, brauchen sie dazu nicht auf den Datenbankserver direkt zugreifen. Es reicht, wenn sie dazu auf die gespeicherten Daten zugreifen. Berichte mit gespeicherten Daten reduzieren dementsprechend nicht nur die Menge der im Netzwerk übertragenen Daten, sondern verringern auch die Belastung des Datenbankservers.

Wenn Ihre Vertriebsdatenbank beispielsweise einmal täglich aktualisiert wird, können Sie den Bericht nach einem ähnlichen Zeitplan ausführen. Die Verkäufer haben somit stets Zugang zu den aktuellen Verkaufszahlen, ohne die Datenbank bei jedem Öffnen eines Berichts abzufragen.

Benutzer benötigen nur das Zugriffsrecht *Ansicht*, um Berichtsinstanzen anzuzeigen.

7.3.2 Kopieren von vorhandenen Zugriffsberechtigungen

Dies ist die beste Möglichkeit zum Erstellen einer Zugriffsberechtigung, wenn Sie eine Zugriffsberechtigung benötigen, die sich geringfügig von einer der vorhandenen Zugriffsberechtigungen unterscheidet.

1. Wechseln Sie zum Bereich *Zugriffsberechtigungen*.
2. Wählen Sie im *Detailbereich* eine Zugriffsberechtigung aus.

   Tipp

   Wählen Sie eine Zugriffsberechtigung aus, die ähnliche Rechte wie diejenigen enthält, die Sie für Ihre Zugriffsberechtigung festlegen möchten.

3. Klicken Sie auf **Organisieren** > **Kopieren**.
   Eine Kopie der ausgewählten Zugriffsberechtigung wird im *Detailbereich* angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7.3.3 Erstellen von Zugriffsberechtigungen

Dies ist die beste Möglichkeit zum Erstellen einer Zugriffsberechtigung, wenn Sie eine Zugriffsberechtigung benötigen, die sich deutlich von einer der vorhandenen Zugriffsberechtigungen unterscheidet.

1. Wechseln Sie zum Bereich *Zugriffsberechtigungen*.
2. Klicken Sie auf **Verwalten** > **Neu** > **Zugriffsberechtigung erstellen**.
   Das Dialogfeld *Neue Zugriffsberechtigung erstellen* wird angezeigt.
3. Geben Sie Titel und Beschreibung für die neue Zugriffsberechtigung ein, und klicken Sie dann auf **OK**.
   Sie kehren zum Bereich *Zugriffsberechtigungen* zurück, und die neue Zugriffsberechtigung wird im *Detailbereich* angezeigt.

7.3.4 Umbenennen von Zugriffsberechtigungen

1. Wählen Sie im Bereich *Zugriffsberechtigungen* im *Detailbereich* die Zugriffsberechtigung aus, die Sie umbenennen möchten.
2. Klicken Sie auf **Verwalten** > **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
3. Geben Sie im Feld **Titel** einen neuen Namen für die Zugriffsberechtigung ein, und klicken Sie dann auf **Speichern und schließen**.
   Sie kehren zum Bereich *Zugriffsberechtigungen* zurück.

7.3.5 So löschen Sie eine Zugriffsberechtigung

1. Wählen Sie im Bereich *Zugriffsberechtigungen* im *Detailbereich* die Zugriffsberechtigung aus, die Sie löschen möchten.
2. Klicken Sie auf **Verwalten** > **Zugriffsberechtigung löschen**.

   > **Hinweis**
   >
   > Vordefinierte Zugriffsberechtigungen können nicht gelöscht werden.

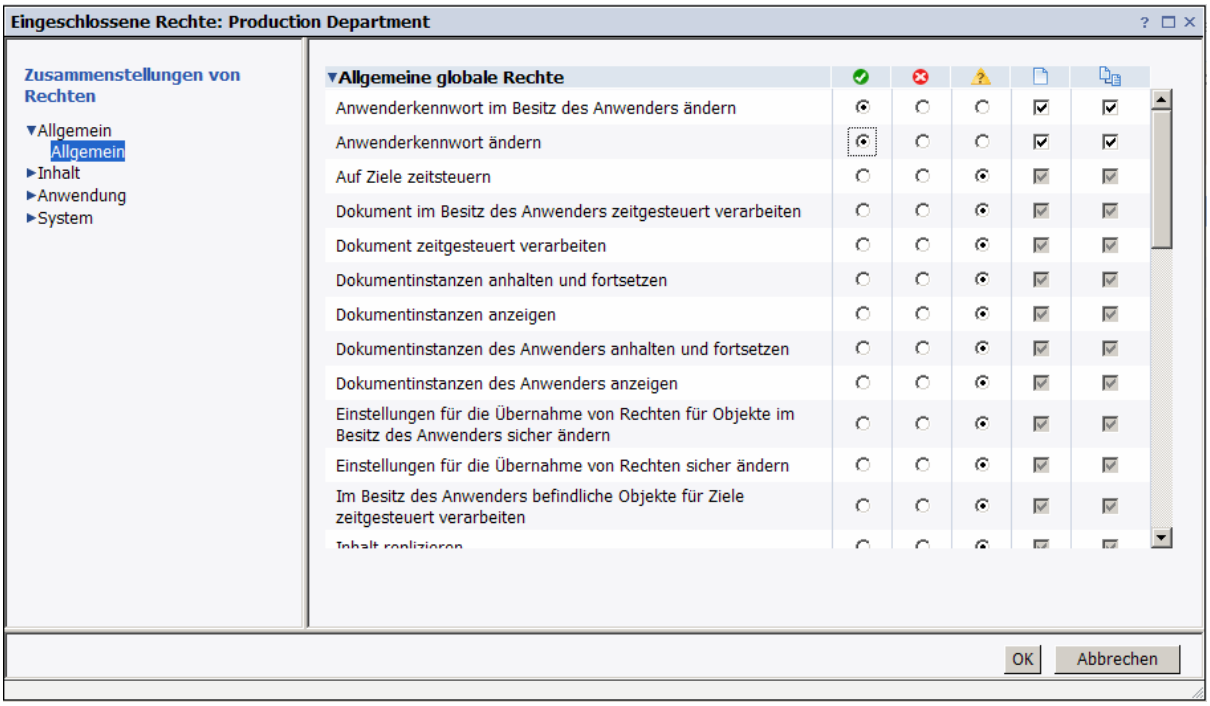
   Es wird ein Dialogfeld mit Informationen über die Objekte angezeigt, auf die sich diese Zugriffsberechtigung auswirkt. Wenn Sie die Zugriffsberechtigung nicht löschen möchten, klicken Sie auf **Abbrechen**, um das Dialogfeld zu schließen.
3. Klicken Sie auf **Löschen**.
   Die Zugriffsberechtigung wird gelöscht, und Sie kehren zum Bereich *Zugriffsberechtigungen* zurück.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7.3.6 So ändern Sie Rechte in einer Zugriffsberechtigung

Um Rechte für eine Zugriffsberechtigung festzulegen, legen Sie zunächst allgemeine globale Rechte fest, die sich unabhängig vom Typ auf alle Objekte auswirken. Anschließend geben Sie an, wann die allgemeinen Einstellungen basierend auf dem jeweiligen Objekttyp überschrieben werden sollen.

1. Wählen Sie im Bereich **Zugriffsberechtigungen** im *Detailbereich* die Zugriffsberechtigung aus, für die Rechte geändert werden sollen.
2. Klicken Sie auf **Aktionen** > **Enthaltene Rechte**.
   Das Dialogfeld **Enthaltene Rechte** wird angezeigt und enthält eine Liste der effektiven Rechte.
3. Klicken Sie auf **Rechte hinzufügen/entfernen**.



   Das Dialogfeld **Enthaltene Rechte** zeigt die Zusammenstellung von Rechten für die Zugriffsberechtigung in der Navigationsliste an. Der Bereich **Allgemeine globale Rechte** ist standardmäßig erweitert.
4. Legen Sie die allgemeinen globalen Rechte fest.
   Die einzelnen Rechte können den Status **Gewährt**, **Verweigert** oder **Nicht angegeben** haben. Sie können außerdem auswählen, ob das Recht nur auf das Objekt, nur auf Unterobjekte oder beides angewendet werden soll.
5. Um typspezifische Rechte für die Zugriffsberechtigung festzulegen, klicken Sie in der Navigationsliste auf die Zusammenstellung von Rechten und dann auf die untergeordnete Zusammenstellung, die sich auf den Objekttyp bezieht, für den Sie Rechte festlegen möchten.
6. Wenn Sie fertig sind, klicken Sie auf **OK**.
   Sie kehren zur Liste der effektiven Rechte zurück.

Weitere Informationen

Verwalten von Sicherheitseinstellungen für Objekte in der CMC [Seite 133]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Typspezifische Rechte [Seite 131]

7.3.7 Verfolgen der Beziehung zwischen Zugriffsberechtigungen und Objekten

Bevor Sie eine Zugriffsberechtigung ändern oder löschen, sollten Sie sicherstellen, dass keine der an der Zugriffsberechtigung vorgenommenen Änderungen sich negativ auf Objekte in der CMC auswirkt. Zu diesem Zweck können Sie eine Beziehungsabfrage für die Zugriffsberechtigung ausführen.

Beziehungsabfragen sind hilfreich zur Verwaltung von Rechten, da über sie Objekte, auf die sich eine Zugriffsberechtigung auswirkt, an einem zentralen Ort anzeigt werden können. Stellen Sie sich eine Situation vor, in der ein Unternehmen seine Organisation umstrukturiert und aus den Abteilungen A und B die Abteilung C wird. Der Administrator entschließt sich, die Zugriffsberechtigungen für Abteilung A und B zu löschen, da diese Abteilungen nicht mehr existieren. Der Administrator führt vor dem Löschen Beziehungsabfragen für beide Zugriffsberechtigungen aus. Im Bereich *Abfrageergebnisse* kann der Administrator die Objekte anzeigen lassen, die betroffen sind, wenn der Administrator die Zugriffsberechtigungen löscht. Im *Detailbereich* wird dem Administrator außerdem der Speicherort der Objekte in der CMC angezeigt, wenn die Objektrechte vor dem Löschen der Zugriffsberechtigungen geändert werden müssen.

> **Hinweis**
>
> Um die Liste der betroffenen Objekte anzuzeigen, benötigen Sie *Ansicht*srechte für diese Objekte.

> **Hinweis**
>
> Ergebnisse von Beziehungsabfragen für eine Zugriffsberechtigung geben nur Objekte zurück, für die die Zugriffsberechtigung explizit zugewiesen wurde. Wenn ein Objekt eine Zugriffsberechtigung aufgrund von Übernahmeeinstellungen verwendet, wird das Objekt nicht in den Abfrageergebnissen angezeigt.

7.3.8 Standortübergreifende Verwaltung von Zugriffsberechtigungen

Zugriffsberechtigungen gehören zu den Objekten, die Sie von einer ursprünglichen Website zu Zielwebsites replizieren können. Sie haben die Möglichkeit, Zugriffsberechtigungen zu replizieren, wenn sie in der Zugriffskontrollliste eines Replikationsobjekts angezeigt werden. Wenn einem Prinzipal beispielsweise Zugriffsberechtigung A für einen Crystal-Reports-Bericht gewährt wird und der Crystal-Reports-Bericht standortübergreifend repliziert wird, wird auch Zugriffsberechtigung A repliziert.

> **Hinweis**
>
> Wenn eine Zugriffsberechtigung mit demselben Namen in der Zielwebsite vorhanden ist, schlägt die Replikation der Zugriffsberechtigung fehl. Eine der Zugriffsberechtigungen muss vor der Replikation von Ihnen oder dem Administrator der Zielwebsite umbenannt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Nachdem Sie eine Zugriffsberechtigung standortübergreifend repliziert haben, sollten Sie die Überlegungen zur Verwaltung berücksichtigen.

Ändern replizierter Zugriffsberechtigungen in der ursprünglichen Website

Wenn eine replizierte Zugriffsberechtigung in der ursprünglichen Website geändert wird, wird die Zugriffsberechtigung in der Zielwebsite aktualisiert, wenn die Replikation das nächste Mal zeitgesteuert ausgeführt wird. Wenn Sie bei Szenarios mit beidseitiger Replikation eine replizierte Zugriffsberechtigung in der Zielwebsite ändern, ändert sich die Zugriffsberechtigung in der ursprünglichen Website.

> **Hinweis**
>
> Stellen Sie sicher, dass sich Änderungen an einer Zugriffsberechtigung auf einer Website nicht negativ auf Objekte anderer Websites auswirken. Bevor Sie Änderungen vornehmen, sollten Sie sich mit den Administratoren der Sites beratschlagen und ihnen empfehlen, Beziehungsabfragen für die replizierte Zugriffsberechtigung auszuführen.

Ändern replizierter Zugriffsberechtigungen in der Zielwebsite

> **Hinweis**
>
> Dies gilt nur für die einseitige Replikation.

Änderungen an replizierten Zugriffsberechtigungen, die in einer Zielwebsite vorgenommen wurden, werden nicht in der ursprünglichen Website reflektiert. Der Administrator einer Zielwebsite kann beispielsweise das Recht zur zeitgesteuerten Verarbeitung von Crystal-Reports-Berichten in der replizierten Zugriffsberechtigung gewähren, auch wenn dieses Recht in der ursprünglichen Website verweigert wurde. Obwohl die Namen von Zugriffsberechtigung und repliziertem Objekt unverändert bleiben, können die effektiven Rechte, die Prinzipale für Objekte haben, folglich von Zielwebsite zu Zielwebsite variieren.

Wenn sich die replizierte Zugriffsberechtigung zwischen der ursprünglichen Website und der Zielwebsite unterscheidet, wird der Unterschied in Bezug auf effektive Rechte ermittelt, wenn ein Replikationsauftrag das nächste Mal zeitgesteuert verarbeitet wird. Sie können erzwingen, dass die Zugriffsberechtigung der Zielwebsite von der Zugriffsberechtigung der ursprünglichen Website überschrieben wird oder die Zugriffsberechtigung der Zielwebsite intakt lassen. Wenn Sie jedoch nicht erzwingen, dass die Zugriffsberechtigung der Zielwebsite von der Zielberechtigung der ursprünglichen Website überschrieben wird, werden sämtliche für die Replikation ausstehenden Objekte, die diese Zugriffsberechtigung verwenden, nicht repliziert.

Um Benutzer davon abzuhalten, replizierte Zugriffsberechtigungen in der Zielwebsite zu ändern, können Sie der Zugriffsberechtigung Benutzer der Zielwebsite als Prinzipale hinzufügen und diesen Benutzern nur *Ansichts*rechte gewähren. Dies bedeutet, dass Benutzer der Zielwebsite die Zugriffsberechtigung zwar anzeigen, aber deren Rechteeinstellungen weder ändern noch anderen Benutzern zuweisen können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

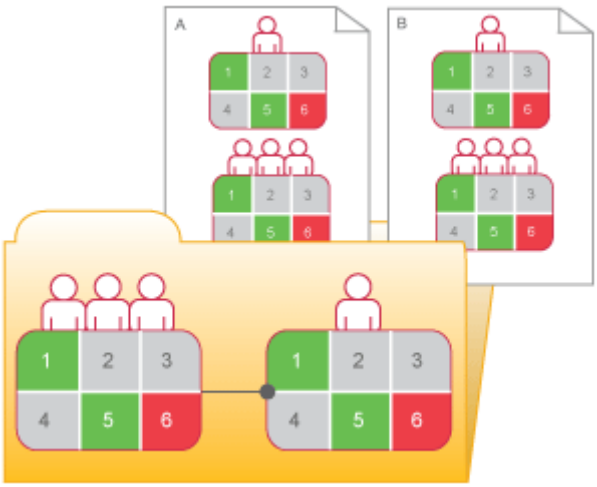
Föderation [Seite 756]
Verfolgen der Beziehung zwischen Zugriffsberechtigungen und Objekten [Seite 145]

7.4 Auflösen der Übernahme

Anhand der Übernahme können Sie Ihre Sicherheitseinstellungen verwalten, ohne Rechte für die einzelnen Objekte festzulegen. In einigen Fällen möchten Sie jedoch vielleicht verhindern, dass Rechte übernommen werden. Sie können beispielsweise Rechte für jedes Objekt anpassen. Sie können die Übernahme für einen Prinzipal in der objekteigenen Zugriffskontrollliste deaktivieren. In diesem Fall können Sie auswählen, ob die Gruppenübernahme, Ordnerübernahme oder beides deaktiviert werden soll.

> **Hinweis**
>
> Wenn die Übernahme aufgelöst wird, wirkt sich dies auf alle Rechte aus. Die Übernahme kann also nicht für einige Rechte aufgelöst werden, während andere Rechte in Kraft bleiben.

Im Diagramm “Auflösen der Übernahme” ist die Gruppen- und Ordnerübernahme anfänglich aktiviert. Der rote Benutzer übernimmt die Rechte 1 und 5 als "gewährt", die Rechte 2, 3 und 4 als "nicht angegeben" und das Recht 6 als "explizit verweigert". Diese auf Ordnerebene für die Gruppe festgelegten Rechte haben zur Folge, dass der rote Benutzer und alle weiteren Gruppenmitglieder diese Rechte an den Ordnerobjekten A und B besitzen. Wenn die Übernahme auf Ordnerebene aufgelöst wird, werden die Objektrechte des roten Benutzers in diesem Ordner aufgehoben, bis dem Benutzer von einem Administrator neue Rechte zugewiesen werden.



© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

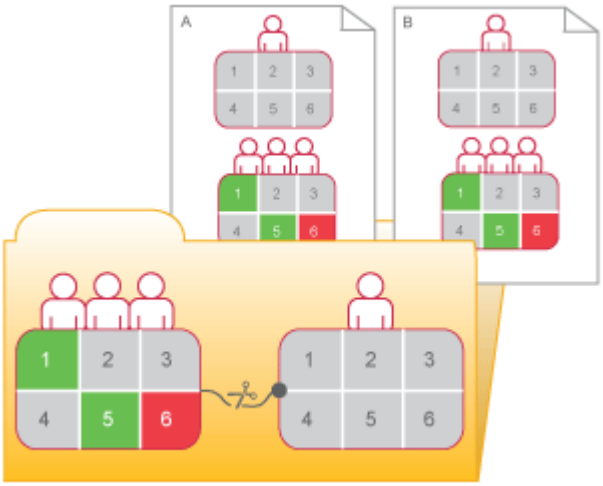


Abbildung 9: Auflösen der Übernahme

7.4.1 So deaktivieren Sie die Übernahme

Über dieses Verfahren können Sie die Gruppen- oder Ordnerübernahme bzw. beides für einen Prinzipal in der Zugriffskontrolliste eines Objekts deaktivieren.

1. Wählen Sie das Objekt aus, für das Sie die Übernahme deaktivieren möchten.
2. Klicken Sie auf **Verwalten** > **Benutzersicherheit**.
   Das Dialogfeld *Benutzersicherheit* wird angezeigt.
3. Wählen Sie den Prinzipal, für den Sie die Übernahme deaktivieren möchten, und klicken Sie auf **Sicherheit zuweisen**.
   Das Dialogfeld *Sicherheit zuweisen* wird angezeigt.
4. Konfigurieren Sie die Übernahmeeinstellungen.
   - Wenn Sie die Gruppenübernahme (die Rechte, die der Prinzipal von der Gruppenmitgliedschaft übernimmt) deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Von übergeordneter Gruppe übernehmen**.
   - Wenn Sie die Gruppenübernahme (die Rechteeinstellungen, die das der Prinzipal vom Ordner übernimmt) deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Vom übergeordneten Ordner übernehmen**.
5. Klicken Sie auf **OK**.

7.5 Delegieren der Administration mithilfe von Rechten

Rechte bieten nicht nur die Möglichkeit, den Zugriff auf Objekte und Einstellungen zu steuern, sondern können auch verwendet werden, um administrative Aufgaben auf Funktionsgruppen innerhalb Ihres Unternehmens zu verteilen. Beispielsweise können Sie veranlassen, dass die verschiedenen Abteilungen ihre Benutzer und Gruppen selbst verwalten. Sie könnten aber auch einem Administrator die globale Verwaltung der BI-Plattform übertragen, die Verwaltung aller Server aber an die Mitarbeiter der IT-Abteilung delegieren.

Angenommen, Ihre Gruppen- und Ordnerstruktur wurden unter Berücksichtigung der Sicherheitsstruktur aufgestellt, die für die delegierte Administration festgelegt wurde: In diesem Fall sollten Sie Ihrem delegierten

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Administrator zwar Rechte für vollständige Benutzergruppen gewähren, diese aber gleichzeitig soweit einschränken, dass er niemals sämtliche Rechte für die von ihm betreuten Benutzer erhält. Beispielsweise können Sie verhindern, dass der delegierte Administrator Benutzerattribute bearbeiten oder anderen Gruppen zuweisen kann.

> **Hinweis**
>
> Objektmigrationen werden am besten von Mitgliedern der Administratorgruppe, insbesondere dem Administratorbenutzerkonto durchgeführt. Um ein Objekt zu migrieren, müssen verschiedene zugehörige Objekte u.U. ebenfalls migriert werden. Der Erwerb der erforderlichen Sicherheitsberechtigungen für sämtliche Objekte ist für ein delegiertes Administratorkonto eventuell nicht möglich.

In der Tabelle "Rechte für delegierte Administratoren" sind die Rechte zusammengefasst, die delegierte Administratoren zum Ausführen allgemeiner Aktionen benötigen.

Tabelle 8: Rechte für delegierte Administratoren

Aktion des delegierten Administrators	Vom delegierten Administrator benötigte Rechte
Erstellen neuer Benutzer	*Hinzufüge*recht für den Ordner *Benutzer* der obersten Ebene
Erstellen neuer Gruppen	*Hinzufüge*recht für den Ordner *Benutzergruppen* der obersten Ebene
Löschen betreuter Gruppen sowie einzelner Benutzer in diesen Gruppen	*Lösch*recht für die betreffenden Gruppen
Löschen nur der vom delegierten Administrator erstellten Benutzer	*Objekte des Benutzers löschen*-Recht für den Ordner *Benutzer* der obersten Ebene
Löschen nur der vom delegierten Administrator erstellten Benutzer und Gruppen	*Objekte des Benutzers löschen*-Recht für den Ordner *Benutzergruppen* der obersten Ebene
Bearbeiten nur der vom delegierten Administrator erstellten Benutzer (einschließlich Hinzufügen dieser Benutzer zu Gruppen)	*Objekte des Benutzers bearbeiten*- und *Sicher Rechte ändern, die Benutzer für eigene Objekte haben*-Recht für den Ordner *Benutzer* der obersten Ebene
Bearbeiten nur der vom delegierten Administrator erstellten Gruppen (einschließlich Hinzufügen von Benutzern zu diesen Gruppen)	*Objekte des Benutzers bearbeiten*- und *Sicher Rechte ändern, die Benutzer für eigene Objekte haben*-Recht für den Ordner *Benutzergruppen* der obersten Ebene
Ändern der Kennwörter für Benutzer in den vom Administrator betreuten Gruppen	*Kennwort bearbeiten*-Recht für die betreffenden Gruppen
Ändern der Kennwörter nur der vom delegierten Administrator erstellten Subjekte	*Benutzerkennwort im Besitz des Benutzers ändern*-Recht für den Ordner *Benutzer* der obersten Ebene oder betreffende Gruppen

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Aktion des delegierten Administrators	Vom delegierten Administrator benötigte Rechte
	Hinweis Das Recht *Benutzerkennwort im Besitz des Benutzers ändern* für eine Gruppe hat nur Auswirkungen auf einen einzelnen Benutzer, wenn Sie den Benutzer der jeweiligen Gruppe hinzufügen.
Ändern von Benutzernamen, Beschreibungen und sonstigen Attributen sowie Neuzuweisen von Benutzern zu anderen Gruppen	*Bearbeitungs*recht für die betreffenden Gruppen
Ändern von Benutzernamen, Beschreibungen und sonstigen Attributen sowie Neuzuweisen von Benutzern zu anderen Gruppen, jedoch nur für die vom delegierten Administrator erstellten Benutzer	*Objekte des Benutzers bearbeiten*-Recht für den Ordner *Benutzer* der obersten Ebene oder betreffende Gruppen **Hinweis** Das Recht *Objekte des Benutzers bearbeiten* für die betreffenden Gruppen hat nur Auswirkungen auf einen einzelnen Benutzer, wenn Sie den Benutzer der jeweiligen Gruppe hinzufügen.

7.5.1 Welche der beiden Optionen "*Rechte von Benutzern für Objekte ändern*" sollte verwendet werden?

Wenn Sie die delegierte Administration einrichten, sollten Sie Ihrem delegierten Administrator Rechte für die von ihm betreuten Subjekte gewähren. Obwohl Sie ihm sämtliche Rechte (*Voller Zugriff*) gewähren können, empfiehlt es sich, das Recht *Rechte ändern* auf der Seite "Erweiterte Einstellungen" zu verweigern und dem delegierten Administrator stattdessen das Recht *Sicher Rechte ändern* einzuräumen. Sie können Ihrem Administrator anstelle des Rechts *Einstellungen für die Übernahme von Rechten ändern* auch das Recht *Einstellungen für die Übernahme von Rechten sicher ändern* gewähren. Die Unterschiede zwischen diesen Rechten sind nachfolgend zusammengefasst.

Rechte von Benutzern für Objekte ändern

Mit diesem Recht kann ein Benutzer alle Rechte jedes Benutzers für das jeweilige Objekt ändern. Wenn Benutzer A beispielsweise die Rechte *Objekte anzeigen* und *Rechte von Benutzern für Objekte ändern* für ein Objekt besitzt, kann Benutzer A die Rechte für das Objekt so ändern, dass er oder beliebige andere Benutzer vollen Zugriff auf dieses Objekt erhalten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Sicher Rechte ändern, die Benutzer für Objekte haben

Mit diesem Recht kann ein Benutzer nur Berechtigungen gewähren, verweigern oder zurücksetzen, die ihm selbst bereits eingeräumt wurden. Wenn Benutzer A beispielsweise die Rechte *Anzeigen* und *Sicher Rechte ändern, die Benutzer für Objekte haben* besitzt, kann Benutzer A sich selbst keine weiteren Rechte gewähren und anderen Benutzern ausschließlich diese beiden Rechte (zum *Anzeigen* und *sicheren Ändern von Rechten*) gewähren oder verweigern. Außerdem kann Benutzer A bei anderen Benutzern nur die Rechte für Objekte ändern, für die ihm das Recht *Sicher Rechte ändern, die Benutzer für Objekte haben* gewährt wurde.

Alle folgenden Bedingungen müssen erfüllt sein, damit Benutzer A die Rechte für Benutzer B an Objekt O ändern kann:

- Benutzer A verfügt über das Recht *Sicher Rechte ändern, die Benutzer für Objekte haben* für Objekt O.
- Jedes Recht oder jede Zugriffsberechtigung, das bzw. die Benutzer A für Benutzer B ändert, wurde A gewährt.
- Benutzer A verfügt über das Recht *Sicher Rechte ändern, die Benutzer für Objekte haben* für Benutzer B.
- Falls eine Zugriffsberechtigung zugewiesen wurde, verfügt Benutzer A über das Recht *Zugriffsberechtigung zuweisen* für die Zugriffsberechtigung, die für Benutzer B geändert wird.

Durch den Gültigkeitsbereich von Rechten können die effektiven Rechte, die ein delegierter Administrator zuweisen kann, weiter beschränkt werden. Ein delegierter Administrator kann über die Rechte *Sicher Rechte ändern* und *Bearbeiten* für einen Ordner verfügen, der Gültigkeitsbereich dieser Rechte ist jedoch nur auf den Ordner beschränkt und umfasst nicht dessen Unterobjekte. Der delegierte Administrator kann das Recht *Bearbeiten* tatsächlich nur für den Ordner (nicht aber für dessen Unterobjekte) und ausschließlich mit dem Gültigkeitsbereich "Auf Objekt anwenden" gewähren. Wenn dem delegierten Administrator das Recht *Bearbeiten* für einen Ordner ausschließlich mit dem Gültigkeitsbereich "Auf Unterobjekt anwenden" gewährt wird, kann er anderen Prinzipalen andererseits das Recht *Bearbeiten* mit beiden Gültigkeitsbereichen für die Unterobjekte des Ordners gewähren, für den Ordner selbst kann er jedoch nur das Recht *Bearbeiten* mit dem Gültigkeitsbereich " Auf Unterobjekt anwenden" gewähren.

Darüber hinaus wird verhindert, dass der delegierte Administrator Rechte dieser Gruppen für andere Prinzipale ändert, für die ihm nicht das Recht *Sicher Rechte ändern* gewährt wurde. Dies ist beispielsweise hilfreich, wenn zwei delegierte Administratoren dafür verantwortlich sind, unterschiedlichen Benutzergruppen Rechte für denselben Ordner zu gewähren, ein delegierter Administrator jedoch nicht in der Lage sein soll, Zugriff auf die Gruppen zu verweigern, die vom anderen delegierten Administrator überwacht werden. Dieses Risiko lässt sich mit dem Recht *Sicher Rechte ändern, die Benutzer für Objekte haben* ausschließen, da delegierte Administratoren sich das Recht zum *sicheren Ändern von Rechten* in der Regel nicht gegenseitig gewähren.

Einstellungen für die Übernahme von Rechten sicher ändern

Dieses Recht ermöglicht es einem delegierten Administrator, Übernahmeeinstellungen für andere Prinzipale zu ändern, die den Objekten zugewiesen sind, auf die der delegierte Administrator Zugriff hat. Um die Übernahmeeinstellungen anderer Prinzipale erfolgreich zu ändern, muss ein delegierter Administrator über dieses Recht für das Objekt und für die Benutzerkonten der Prinzipale verfügen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7.5.2 Eigentümerrechte

Hierbei handelt es sich um Rechte, die nur für den Eigentümer des Objekts gelten, für das Rechte aktiviert werden. In der BI-Plattform entspricht der Eigentümer eines Objekts dem Prinzipal, der ein Objekt erstellt hat. Falls dieser Prinzipal aus dem System gelöscht werden sollte, geht das Eigentum wieder auf den Administrator über.

Eigentümerrechte sind hilfreich bei der Verwaltung von eigentümerbasierten Sicherheitseinstellungen. Beispielsweise können Sie einen Ordner oder eine Ordnerhierarchie erstellen, in denen verschiedene Benutzer Dokumente erstellen und anzeigen lassen können, jedoch darauf beschränkt sind, nur eigene Dokumente zu ändern oder zu löschen. Darüber hinaus sind Eigentümerrechte nützlich, wenn Benutzer nur berechtigt sein sollen, Instanzen der von Ihnen erstellten Berichte, jedoch keine anderen Instanzen zu ändern. Bei der Zugriffsberechtigung "Zeitgesteuerte Verarbeitung" können Benutzer auf diese Weise lediglich eigene Instanzen bearbeiten, löschen, anhalten und erneut zeitgesteuert verarbeiten.

Eigentümerrechte funktionieren ähnlich wie die entsprechenden regulären Rechte. Eigentümerrechte treten jedoch nur dann in Kraft, wenn dem Prinzipal Eigentümerrechte gewährt, reguläre Rechte aber verweigert bzw. nicht angegeben wurden.

7.6 Zusammenfassung der Empfehlungen zur Verwaltung von Rechten

Berücksichtigen Sie diese Überlegungen bei der Verwaltung von Rechten:

- Verwenden Sie möglichst immer Zugriffsberechtigungen. Mit diesen vordefinierten, kombinierten Rechten lässt sich die Verwaltung vereinfachen, da die mit allgemeinen Benutzeranforderungen verknüpften Rechte praktisch gruppiert sind.
- Legen Sie Rechte und Zugriffsberechtigungen für Ordner der obersten Ebene fest. Indem Sie die Übernahme aktivieren, können diese Rechte mit einem minimalen Verwaltungsaufwand innerhalb des Systems an untergeordnete Objekte weitergegeben werden.
- Vermeiden Sie nach Möglichkeit das Auflösen der Übernahme. Dadurch können Sie die in der BI-Plattform hinzugefügten Inhalte mit weniger Zeitaufwand sicherer gestalten.
- Legen Sie geeignete Rechte für Benutzer und Gruppen auf Ordnerebene fest, und veröffentlichen Sie anschließend Objekte in diesem Ordner. Standardmäßig übernehmen Benutzer oder Gruppen, die Rechte für einen Ordner besitzen, dieselben Rechte für jedes Objekt, das nachfolgend in diesem Ordner veröffentlicht wird.
- Organisieren Sie Benutzer in Benutzergruppen, weisen Sie der gesamten Gruppe und ggf. bestimmten Mitgliedern Zugriffsberechtigungen und Rechte zu.
- Erstellen Sie einzelne Administratorkonten für jeden Administrator im System, und fügen Sie sie der Gruppe "Administratoren" hinzu, um die Verantwortlichkeit in Bezug auf Systemänderungen zu verbessern.
- Der Gruppe "Alle" werden standardmäßig sehr eingeschränkte Rechte für Ordner der obersten Ebene in der BI-Plattform gewährt. Nach der Installation wird empfohlen, dass Sie die Rechte von Mitgliedern der Gruppe "Alle" überprüfen und entsprechende Sicherheitsmerkmale zuweisen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8 Sichern der BI-Plattform

8.1 Überblick zum Thema Sicherheit

In diesem Abschnitt werden die Verfahren erläutert, mit denen die BI-Plattform Probleme der Unternehmenssicherheit angeht, wobei Administratoren und Systemarchitekten Antworten auf typische Fragen in Bezug auf die Sicherheit erhalten.

Die Architektur der BI-Plattform geht auf viele der heutigen Sicherheitsbedenken in Unternehmen und Organisationen ein. Die aktuelle Version unterstützt u. a. die folgenden Funktionen: Verteilte Sicherheit, Einzelanmeldung, Ressourcenzugriffssicherheit, granulare Objektrechte sowie Authentifizierung von Drittherstellern, um Schutz vor unbefugtem Zugriff zu bieten.

Da die BI-Plattform das Framework für immer mehr Komponenten der Enterprise-Familie von SAP-BusinessObjects-Produkten bereitstellt, enthält dieser Abschnitt ausführliche Informationen zu Sicherheitsfunktionen und der damit verbundenen Funktionalität, die verdeutlichen, wie das Framework selbst die Sicherheit durchsetzt und aufrechterhält. In diesem Abschnitt werden keine ausführlichen Verfahrensabläufe dargestellt. Der Schwerpunkt liegt vielmehr auf konzeptionellen Informationen. Außerdem finden Sie hier Links zu wichtigen Verfahren.

Nach einer kurzen Einführung in die Sicherheitskonzepte für das System werden Einzelheiten zu den folgenden Themen erläutert:

- Verwenden von Sicherheitsmodi für Verschlüsselung und Datenverarbeitung zum Schutz von Daten.
- Einrichten der Secure Sockets Layer (SSL) für BI-Plattform-Implementierungen.
- Richtlinien zum Konfigurieren und Warten von Firewalls für die BI-Plattform.
- Konfigurieren von Reverse Proxy-Servern.

8.2 Notfallwiederherstellungsplanung

Zum Schutz der Investitionen Ihrer Organisation in die BI-Plattform müssen bestimmte Schritte ausgeführt werden, um die maximale Aufrechterhaltung des Geschäftsbetriebs im Notfall zu gewährleisten. Dieser Abschnitt enthält Richtlinien zur Erstellung eines Notfallwiederherstellungsplans für Ihre Organisation.

Allgemeine Richtlinien

- Durchführen regelmäßiger Sicherungen und ggf. Senden von Kopien einer Reihe von Sicherungsmedien an externe Stellen.
- Sichere Speicherung sämtlicher Softwaremedien.
- Sichere Speicherung sämtlicher Lizenzdokumentation.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Spezifische Richtlinien

Drei Systemressourcen bedürfen besonderer Aufmerksamkeit hinsichtlich der Notfallwiederherstellungsplanung:

- Inhalte der File Repository Server: Dazu gehören proprietäre Inhalte, z.B. Berichte. Diese Inhalte sollten regelmäßig gesichert werden. Im Falle eines Notfalls besteht keine Möglichkeit zum Regenerieren solcher Inhalte ohne einen regelmäßigen Sicherungsprozess.
- Die von der CMS-Datei verwendete Systemdatenbank. Diese Ressource enthält sämtliche wichtigen Metadaten für Ihre Implementierung, z.B. Benutzerdaten, Berichte und andere sensible Daten, die spezifisch für Ihre Organisation sind.
- Schlüsseldatei mit den Datenbankinformationen (.dbinfo file): Diese Ressource enthält den Masterschlüssel für die Systemdatenbank. Falls dieser Schlüssel aus irgendeinem Grund nicht verfügbar ist, können Sie nicht auf die Systemdatenbank zugreifen. Nach der Implementierung der BI-Plattform sollten Sie Ihr Kennwort für diese Ressource an einem sicheren oder bekannten Ort aufbewahren. Ohne dieses Kennwort können Sie die Datei nicht regenerieren und verlieren damit den Zugriff auf die Systemdatenbank.

8.3 Allgemeine Empfehlungen zur Sicherung der Implementierung

Im Folgenden sind Empfehlungen zur Sicherung der BI-Plattform-Implementierungen aufgeführt.

- Schützen Sie die Kommunikation zwischen dem CMS und anderen Systemkomponenten mit Firewalls. Verbergen Sie nach Möglichkeit den CMS immer hinter der Firewall. Sorgen Sie zumindest dafür, dass sich die Systemdatenbank sicher hinter der Firewall befindet.
- Sichern Sie die File Repository Server mit zusätzlicher Verschlüsselung. Sobald das System in Betrieb ist, werden proprietäre Inhalte auf diesen Servern gespeichert. Fügen Sie zusätzliche Verschlüsselung über das Betriebssystem oder ein Drittherstellertool hinzu.

  > **Hinweis**
  >
  > SFTP wird von der BI-Plattform nicht unterstützt. Wenn Sie SFTP-Funktionalität benötigen, lesen Sie SAP-Hinweis 1556571, oder ziehen Sie eine SAP-Partnerlösung in Betracht.

- Implementieren Sie einen Reverse Proxy-Server vor den Webanwendungsservern, um sie hinter einer einzigen IP-Adresse zu verbergen. In dieser Konfiguration wird der gesamte an private Webanwendungsserver gerichtete Internet-Datenverkehr über den Reverse Proxy-Server geroutet, während die privaten IP-Adressen unerkannt bleiben.
- Sorgen Sie für die strikte Einhaltung von unternehmensinternen Kennwortrichtlinien. Stellen Sie sicher, dass Benutzerkennwörter regelmäßig geändert werden.
- Wenn Sie die mit der BI-Plattform gelieferte Systemdatenbank und den Webanwendungsserver installiert haben, sollten Sie mithilfe der entsprechenden Dokumentation sicherstellen, dass diese Komponenten mit angemessenen Sicherheitskonfigurationen implementiert wurden.
- Verwenden Sie das SSL-Protokoll (Secure Sockets Layer) für die gesamte Netzwerkkommunikation zwischen Clients und Servern in der Implementierung.
- Stellen Sie sicher, dass das Installationsverzeichnis und die Unterverzeichnisse der Plattform gesichert sind. In diesen Verzeichnissen können während des Systembetriebs sensible temporäre Daten abgelegt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Der Zugriff auf die Central Management Console (CMC) sollte nur lokal erfolgen dürfen. Informationen zu Implementierungsoptionen für die CMC finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.
- Standardmäßig beinhalten Web-Intelligence-spezifische Fehlermeldungen Datenbankschemainformationen. Führen Sie zum Anzeigen der Fehlermeldungen ohne die Datenbankschemainformationen die folgenden Schritte aus:
  1. Öffnen Sie die Konfigurationsdatei `WebIContainer_ServerDescriptor.xml` zur Bearbeitung. Standardmäßig befindet sie sich im Verzeichnis unter `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86\config`.
  2. Ändern Sie den Wert dieses Parameters in False: `WebiParamDetailedDbErrorsEnabled = False`.

Weitere Informationen

Konfigurieren des SSL-Protokolls [Seite 179]
Kennworteinschränkungen [Seite 161]
Konfigurieren der Sicherheit für Drittthersteller-Serverpakete [Seite 155]

8.4 Konfigurieren der Sicherheit für Drittthersteller-Serverpakete

Falls Sie sich für die Installation von Fremdhersteller-Servern entschieden haben, die mit der BI-Plattform gebündelt werden, sollten Sie Zugriff auf die Dokumentation für folgende Komponentenpakete haben und diese durchsehen:

- Sybase SQL Anywhere: Einzelheiten zur Sicherung dieser Systemdatenbank finden Sie unter *http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.help.sqlanywhere.12.0.0/dbadmin/da-part-securing.html*.
- Apache Tomcat: Einzelheiten zur Sicherheit dieses Webanwendungsservers finden Sie unter *http://tomcat.apache.org/*.

8.5 Aktive Vertrauensstellung

In einem Netzwerk ist eine Vertrauensstellung zwischen zwei Domänen normalerweise eine Verbindung, mit der eine Domäne Benutzer erkennen kann, die von der anderen Domäne authentifiziert wurden. Die Vertrauensstellung erhält die Sicherheit und ermöglicht gleichzeitig den Benutzern, auf Ressourcen in mehreren Domänen zuzugreifen, ohne wiederholt die Anmeldedaten eingeben zu müssen.

In der BI-Plattform-Umgebung funktioniert die aktive Vertrauensstellung ähnlich und gibt jedem Benutzer nahtlosen Zugriff auf alle im System vorhandenen Ressourcen. Wenn der Benutzer authentifiziert und ihm eine

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

aktive Sitzung gewährt wurde, können alle anderen BI-Plattform-Komponenten die Anforderungen und Vorgänge des Benutzers ohne weitere Eingabe der Benutzerinformationen verarbeiten. In diesem Sinne stellt die aktive Vertrauensstellung die Grundlage für die verteilte Sicherheit in der BI-Plattform dar.

8.5.1 Anmeldetoken

Ein Anmeldetoken ist eine verschlüsselte Zeichenfolge, die die eigenen Nutzungsattribute definiert und die Sitzungsinformationen des Benutzers enthält. Die Nutzungsattribute des Anmeldetokens werden beim Erstellen des Anmeldetokens angegeben. Mit diesen Attributen können dem Anmeldetoken Beschränkungen zugewiesen werden, um die Chance zu verringern, dass das Anmeldetoken von unberechtigten Benutzern verwendet wird. Die aktuellen Nutzungsattribute des Anmeldetokens lauten:

- **Anzahl der Minuten**

  Dieses Attribut schränkt die Nutzungsdauer des Anmeldetokens ein.
- **Anzahl der Anmeldungen**

  Dieses Attribut schränkt ein, wie oft das Anmeldetoken für eine Anmeldung bei der BI-Plattform verwendet werden kann.

Beide Attribute verhindern, dass Benutzer in böswilliger Absicht mit Anmeldetoken legitimer Benutzer unbefugten Zugriff auf die BI-Plattform erlangen.

> **Hinweis**
>
> Ein Anmeldetoken in einem Cookie zu speichern stellt ein potenzielles Sicherheitsrisiko dar, wenn das Netzwerk zwischen Browser und Anwendungs- oder Webserver nicht sicher ist, beispielsweise, wenn die Verbindung über ein öffentliches Netzwerk hergestellt und weder SSL noch die vertrauenswürdige Authentifizierung verwendet wird. Es empfiehlt sich, Secure Sockets Layer (SSL) zu verwenden, um Sicherheitsrisiken zwischen dem Browser und Anwendungs- bzw. Webserver zu vermeiden.

Wenn das Anmeldecookie deaktiviert wurde und der Webserver oder Webbrowser eine Zeitüberschreitung verursacht, wird dem Benutzer der Anmeldebildschirm angezeigt. Wenn das Cookie aktiviert ist und der Server oder Browser eine Zeitüberschreitung verursacht, wird der Benutzer unverzüglich wieder beim System angemeldet. Da Zustandsinformationen jedoch an die Websitzung gebunden sind, geht der Zustand des Benutzers verloren. Beispiel: Wenn der Benutzer eine Navigationsstruktur erweitert und ein bestimmtes Element ausgewählt hatte, wird die Struktur zurückgesetzt.

Im Webclient der BI-Plattform sind Anmeldetoken standardmäßig aktiviert, für BI-Launchpad können Anmeldetoken jedoch deaktiviert werden. Wenn Sie die Anmeldetoken im Client deaktivieren, ist die Benutzersitzung auf die Zeitüberschreitung des Webservers oder Webbrowsers beschränkt. Wenn diese Sitzung abläuft, muss sich der Benutzer erneut bei der BI-Plattform anmelden.

8.5.2 Ticketverfahren für verteilte Sicherheit

Enterprise-Systeme für viele Benutzer erfordern normalerweise eine gewisse verteilte Sicherheit. Ein Enterprise-System erfordert z.B. verteilte Sicherheit, um bestimmte Funktionen zu unterstützen, wie den Vertrauenstransfer (eine andere Komponente kann für den Benutzer handeln).

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Die BI-Plattform implementiert für das Bereitstellen verteilter Sicherheit ein Ticketverfahren (das dem Kerberos-Ticketverfahren ähnelt). Der CMS gewährt Tickets, die es Komponenten erlauben, Vorgänge für einen bestimmten Benutzer auszuführen. In der BI-Plattform wird das Ticket als Anmeldetoken bezeichnet.

Das Anmeldetoken wird meistens über das Web verwendet. Wenn Benutzer zum ersten Mal von der BI-Plattform authentifiziert werden, erhalten sie Anmeldetoken vom CMS. Der Webbrowser des Benutzers speichert dieses Anmeldetoken im Cache. Wenn der Benutzer eine neue Anforderung erstellt, können andere BI-Plattform-Komponenten das Anmeldetoken vom Webbrowser des Benutzers lesen.

8.6 Sitzungen und Sitzungsnachverfolgung

Im Allgemeinen ist eine Sitzung eine Verbindung zwischen Client und Server, über die Informationen zwischen den beiden Rechnern ausgetauscht werden. Der Zustand einer Sitzung entspricht einer Reihe von Daten, die die Attribute, die Konfiguration oder den Inhalt der Sitzung beschreiben. Wenn Sie eine Verbindung zwischen Client und Server über das Web herstellen, schränkt HTTP die Dauer jeder Sitzung auf eine Seite von Informationen ein. Aus diesem Grund speichert der Webbrowser den Zustand jeder Sitzung nur so lange, wie eine Webseite angezeigt wird. Sobald Sie von einer Webseite auf eine andere wechseln, wird der Zustand der ersten Sitzung verworfen und durch den Zustand der nächsten Sitzung ersetzt. Aus diesem Grund müssen Websites und Webanwendungen auf irgendeine Weise den Zustand der Sitzung speichern, wenn sie diese Informationen in einer anderen wiederverwenden müssen.

Die BI-Plattform speichert den Sitzungszustand mit zwei gängigen Verfahren:

- Cookies: Ein Cookie ist eine kleine Textdatei, in der der Sitzungszustand auf der Clientseite gespeichert wird. Der Webbrowser des Benutzers speichert das Cookie für die spätere Verwendung. Das BI-Plattform-Anmeldetoken ist ein Beispiel für dieses Verfahren.
- Sitzungsvariablen: Eine Sitzungsvariable ist ein Teil des Arbeitsspeichers, in dem der Sitzungszustand auf der Serverseite gespeichert wird. Wenn die BI-Plattform einem Benutzer eine aktive Identität im System gewährt, werden Informationen wie der Authentifizierungstyp des Benutzers in einer Sitzungsvariablen gespeichert. Solange die Sitzung erhalten wird, muss der Benutzer weder ein zweites Mal die Benutzerinformationen eingeben noch Tasks wiederholen, die für den Abschluss der nächsten Anforderung erforderlich sind.

  Bei Java-Implementierungen wird die Sitzung zur Verarbeitung von JSP-Anforderungen verwendet. Bei .NET-Implementierungen wird die Sitzung zur Verarbeitung von ASPX-Anforderungen verwendet.

Hinweis

Im Idealfall sollte das System die Sitzungsvariable so lange speichern, wie der Benutzer im System aktiv ist. Das System sollte auch für das Erhalten der Sicherheit und das Verringern der verwendeten Ressourcen die Sitzungsvariable sofort zerstören, wenn der Benutzer nicht mehr mit dem System arbeitet. Da jedoch die Interaktion zwischen einem Webbrowser und einen Webserver zustandslos sein kann, ist es mitunter schwer zu ermitteln, wann Benutzer das System verlassen, wenn sie sich nicht explizit abmelden. Für dieses Problem ist in der BI-Plattform die Sitzungsnachverfolgung implementiert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.6.1 CMS-Sitzungsnachverfolgung

Der CMS implementiert einen einfachen Nachverfolgungsalgorithmus. Wenn sich ein Benutzer anmeldet, wird ihm eine CMS-Sitzung gewährt, die der CMS speichert, bis sich der Benutzer abmeldet oder bis die Webanwendungsserver-Sitzungsvariable freigegeben wird.

Die Webanwendungsserver-Sitzung informiert den CMS in regelmäßigen Abständen darüber, ob die Sitzung noch aktiv ist. Die CMS-Sitzung wird aus diesem Grund so lange beibehalten, wie die Webanwendungsserver-Sitzung besteht. Wenn die Webanwendungsserver-Sitzung zehn Minuten lang nicht mit dem CMS kommuniziert, wird die CMS-Sitzung vom CMS zerstört. Dies handhabt Situationen, in denen Client-seitige Komponenten nicht ordnungsgemäß heruntergefahren werden.

8.6.2 Verwalten von Sitzungen

Sie können Sitzungen in der CMC anzeigen und beenden.

Sie können Benutzersitzungen in der Central Management Console (CMC) anzeigen und beenden. Vielleicht möchten Sie beispielsweise sehen, welche Benutzer mit mehreren Sitzungen arbeiten. Oder Sie möchten Sitzungen, die zu viele Systemressourcen verbrauchen, oder sehr alte Sitzungen beenden. Möglicherweise müssen Sie auch Sitzungen beenden, wenn Sie Ausfallzeiten oder Upgrades für das System vorbereiten.

8.6.2.1 Anzeigen der Sitzungsliste

Sitzungen in der CMC anzeigen.

Sie können eine Liste der Sitzungen in der Central Management Console anzeigen.

1. Melden Sie sich als Administrator bei der CMC an.
2. Klicken Sie im Bereich **Verwalten** auf **Sitzungen**.

Die Liste der Benutzersitzungen für das Cluster wird angezeigt. Sie können auf die Spaltenköpfe klicken, um die Liste nach Benutzername, nach der Anzahl der offenen Sitzungen oder nach den Anmeldezeiten zu sortieren. Sie können auch auf den Benutzernamen, die Anzahl von Sitzungen oder die Anmeldezeit klicken, um Details zur Sitzung des jeweiligen Benutzers im unteren Bereich anzuzeigen.

8.6.2.2 Beenden von Sitzungen

Sitzungen in der CMC beenden.

Sie können eine oder mehrere Sitzungen beenden.

1. Melden Sie sich als Administrator bei der CMC an.
2. Klicken Sie im Bereich **Verwalten** auf **Sitzungen**.

   Die Liste der Benutzersitzungen für das Cluster wird angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Klicken Sie auf einen Benutzernamen, eine Anzahl von Sitzungen oder eine Anmeldezeit, um die Sitzung eines Benutzers im unteren Bereich anzuzeigen.
4. Klicken Sie auf eine einzige Sitzung, oder halten Sie beim Klicken die *STRG-Taste* gedrückt, um mehrere Sitzungen auszuwählen.
5. Klicken Sie auf **Sitzung beenden**.

> **Hinweis**
>
> Um Sitzungen beenden zu können, müssen Sie über die Berechtigung “Objekte bearbeiten” für das CMS-Objekt verfügen.

> **Hinweis**
>
> Ihre aktuelle Administratorsitzung können Sie nicht beenden.

8.7 Umgebungsschutz

Umgebungsschutz bezieht sich auf die Sicherheit des allgemeinen Umfelds, in dem Client- und Serverkomponenten kommunizieren. Obwohl das Internet und webbasierte Systeme aufgrund der Flexibilität und des Funktionsreichtums immer beliebter werden, werden sie in einer Umgebung ausgeführt, die evtl. schwer zu schützen ist. Bei der Implementierung der BI-Plattform ist der Umgebungsschutz auf zwei Bereiche der Kommunikation aufgeteilt: Webbrowser mit Webserver und Webserver mit der BI-Plattform.

8.7.1 Webbrowser zu Webserver

Wenn Daten zwischen dem Webbrowser und dem Webserver übertragen werden, ist normalerweise ein gewisses Sicherheitsniveau erforderlich. Relevante Sicherheitsmaßnahmen bestehen in der Regel aus zwei Schritten:

- Gewährleisten, dass die Übertragung der Daten sicher ist
- Gewährleisten, dass nur autorisierte Benutzer die Informationen vom Webserver abrufen.

> **Hinweis**
>
> Webserver führen diese Aufgaben normalerweise anhand von verschiedenen Sicherheitsverfahren aus, einschließlich des SSL-Protokolls (Secure Sockets Layer) und anderen ähnlichen Verfahren. Es empfiehlt sich, SSL zu verwenden, um Sicherheitsrisiken zwischen dem Browser und Anwendungs- bzw. Webserver zu vermeiden.

Sie müssen die Kommunikation zwischen dem Webbrowser und dem Webserver unabhängig von der BI-Plattform sichern. Weitere Informationen zum Sichern der Clientverbindungen finden Sie in der Dokumentation des Webservers.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.7.2 Webserver und die BI-Plattform

Firewalls werden in der Regel zum Sichern der Kommunikation zwischen dem Webserver und dem restlichen Unternehmensintranet (einschließlich der BI-Plattform) verwendet. Die BI-Plattform unterstützt Firewalls, die IP-Filterung bzw. statische Netzwerkadressenübersetzung (NAT) verwenden. Zu den unterstützten Umgebungen gehören u.a. mehrere Firewalls, Webserver oder Anwendungsserver.

8.8 Auditieren von Änderungen an der Sicherheitskonfiguration

Änderungen an Standardsicherheitskonfigurationen für folgende Elemente und Vorgänge werden von der BI-Plattform nicht auditiert:

- Eigenschaftendateien für Webanwendungen (BOE, Webdienste)
- TrustedPrincipal.conf
- In BI-Launchpad und Open Document vorgenommene Anpassungen

Änderungen an der Sicherheitskonfiguration, die außerhalb der CMC erfolgt sind, werden generell nicht auditiert. Dies gilt auch für Änderungen, die über Central Configuration Manager (CCM) vorgenommen wurden. Änderungen, die über die CMC durchgeführt wurden, können auditiert werden.

8.9 Prüfen der Webvorgänge

Die BI-Plattform gibt Ihnen durch das Aufzeichnen der Webvorgänge und dem möglichen Prüfen und Überwachen der Details einen Einblick in das System. Der Webanwendungsserver bietet die Möglichkeit, die aufzuzeichnenden Webattribute auszuwählen, z.B. Uhrzeit, Datum, IP-Adresse, Portnummer usw. Die Prüfdaten werden auf der Festplatte protokolliert und in kommagetrennten Textdateien gespeichert. Dies vereinfacht das Erstellen von Berichten mit diesen Daten bzw. den Import der Daten in andere Anwendungen.

8.9.1 Schutz vor unberechtigten Anmeldeversuchen

Selbst ein gut gesichertes System weist meistens mindestens eine Schwachstelle auf: nämlich die Stelle, an der Benutzer eine Verbindung mit dem System herstellen. Es ist fast unmöglich, diese Stelle vollständig zu schützen, da das einfache Raten eines gültigen Benutzernamens und Kennworts weiterhin eine durchaus denkbare Methode für den Einbruch in das System bleibt.

In der BI-Plattform sind mehrere Verfahren implementiert, die die Wahrscheinlichkeit verringern, dass ein unberechtigter Benutzer auf das System zugreifen kann. Die verschiedenen nachfolgend aufgeführten Beschränkungen gelten nur für Enterprise-Konten, d.h. sie gelten nicht für Konten, die Sie einer externen Benutzerdatenbank (LDAP oder Windows AD) zugeordnet haben. Normalerweise können Sie jedoch im externen System den externen Konten ähnliche Beschränkungen auferlegen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.9.2 Kennworteinschränkungen

Durch Kennwortbeschränkungen wird sichergestellt, dass bei der Enterprise-Standardauthentifizierung relativ komplexe Kennwörter erstellt werden. Sie können folgende Optionen aktivieren:

- Kennwörter mit Groß- und Kleinschreibung obligatorisch machen

  Diese Option stellt sicher, dass die Kennwörter mindestens zwei von den folgenden Zeichenklassen enthalten: Großbuchstaben, Kleinbuchstaben, Zahlen oder Satzzeichen.
- Mindestens n Zeichen

  Wenn Sie eine Mindestkomplexität für Kennwörter obligatorisch machen, verringern Sie die Wahrscheinlichkeit, dass ein unberechtigter Benutzer einfach das Kennwort eines gültigen Benutzers errät.

8.9.3 Anmeldeeinschränkungen

Anmeldeeinschränkungen sollen hauptsächlich Angriffe auf das Wörterbuch verhindern (ein Verfahren, bei dem ein unberechtigter Benutzer in Besitz eines gültigen Benutzernamens gelangt und dann versucht, das entsprechende Kennwort zu erfahren, indem er jedes im Wörterbuch vorhandene Wort probiert). Mit der Geschwindigkeit der modernen Hardware können bestimmte Programme Millionen von Kennwörtern pro Minute erraten. Die BI-Plattform verhindert Angriffe auf das Wörterbuch mit einem internen Verfahren, das eine Zeitverzögerung (0,5 bis 1,0 Sekunden) zwischen Anmeldeversuchen erzwingt. Die Plattform stellt außerdem mehrere benutzerdefinierbare Optionen bereit, mit denen das Risiko von Angriffen auf das Wörterbuch verringert werden kann:

- Konto nach n fehlgeschlagenen Anmeldeversuchen deaktivieren
- Zähler für fehlgeschlagene Anmeldungen nach n Minuten zurücksetzen
- Konto nach n Minuten wieder aktivieren

8.9.4 Benutzerbeschränkungen

Durch Benutzereinschränkungen wird sichergestellt, dass Benutzer, die die Standard-Enterprise-Authentifizierung verwenden, regelmäßig neue Kennwörter erstellen. Sie können folgende Optionen aktivieren:

- Kennwort muss alle n Tage geändert werden
- Die letzten n Kennwörter dürfen nicht wiederverwendet werden
- Mindestens n Minute(n) bis zur Änderung des Kennworts warten

Diese Optionen sind für vieles nützlich. Erstens muss jeder Benutzer, der einen böswilligen Wörterbuchangriff versucht, bei jedem Ändern des Kennworts von vorne anfangen. Und da Kennwortänderungen auf dem ersten Anmeldezeitpunkt jedes Benutzers basieren, kann der unberechtigte Benutzer nur schwer bestimmen, zu welchem Zeitpunkt ein bestimmtes Kennwort geändert wird. Selbst wenn ein unberechtigter Benutzer die Informationen eines anderen Benutzers errät oder in den Besitz derselben gelangt, sind diese nur für einen begrenzten Zeitraum gültig.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.9.5 Guest-Konto-Einschränkungen

Die BI-Plattform unterstützt die anonyme Einzelanmeldung für das Guest-Konto. Wenn Benutzer ohne Angabe eines Benutzernamens und Kennworts eine Verbindung mit der BI-Plattform herstellen, werden sie automatisch unter dem Guest-Konto angemeldet. Wenn Sie dem Guest-Konto ein sicheres Kennwort zuordnen, oder wenn Sie das Guest-Konto völlig deaktivieren, deaktivieren Sie auch dieses Standardverhalten.

8.10 Verarbeitungserweiterungen

In der BI-Plattform können Sie Ihre Berichtsumgebung durch den Einsatz benutzerdefinierter Verarbeitungserweiterungen weiter absichern. Eine Verarbeitungserweiterung ist eine DLL, die Code enthält, mit dem Ihre Unternehmenslogik auf bestimmte BI-Plattform-Anzeige- oder Zeitsteuerungsanforderungen vor der Verarbeitung angewendet wird.

Durch die Unterstützung von Verarbeitungserweiterungen legt das Administration SDK der BI-Plattform einen Eingriffspunkt frei, an dem Entwickler die Anforderung abfangen können. Entwickler können dann der Anforderung Auswahlformeln vor dem Verarbeiten des Berichts anhängen.

Ein typisches Beispiel ist eine Berichtsverarbeitungserweiterung, die Sicherheit auf der Zeilenebene erzwingt. Bei diesem Sicherheitstyp wird der Datenzugriff nach Zeile in den Datenbanktabellen eingeschränkt. Der Entwickler schreibt eine DLL (Dynamically Loaded Library), die Anzeige- oder Zeitsteuerungsanforderungen für einen Bericht abfängt (bevor die Anforderung von einem Job Server, Processing Server oder Report Application Server verarbeitet wird). Der Code des Entwicklers ermittelt zuerst den Benutzer, der Eigentümer des Verarbeitungsauftrags ist, und ermittelt dann die Datenzugriffsrechte des Benutzers in einem Fremdherstellersystem. Der Code generiert dann eine Datensatzauswahlformel für den Bericht. Diese Formel wird angehängt und schränkt die von der Datenbank ausgegebenen Daten ein. In diesem Fall dient die Verarbeitungserweiterung als Verfahren, mit dem benutzerdefinierte Sicherheit auf der Zeilenebene in die BI-Plattform-Umgebung integriert wird.

Wenn Sie Verarbeitungserweiterungen aktivieren, laden die entsprechenden BI-Plattform-Serverkomponenten die Verarbeitungserweiterungen bei der Ausführung. Das SDK enthält eine komplett dokumentierte API, mit der Entwickler Verarbeitungserweiterungen schreiben können. Weitere Informationen finden Sie in der Entwicklerdokumentation auf Ihrem Produktdatenträger.

8.11 Übersicht über die BI-Plattform-Datensicherheit

Administratoren von BI-Plattform-Systemen verwalten die Sicherung sensibler Daten über folgende Funktionen:

- Eine Sicherheitseinstellung auf Clusterebene, in der festgelegt ist, welche Anwendungen und Clients auf den CMS zugreifen können. Diese Einstellung wird über den Central Configuration Manager verwaltet.
- Ein auf zwei Schlüsseln basierendes kryptografisches System, das sowohl den Zugriff auf das CMS-Repository als auch die Schlüssel zum Ver- bzw. Entschlüsseln von Objekten im Repository steuert. Der Zugriff auf das CMS-Repository wird über den Central Configuration Manager eingestellt, während die Central Management Console über einen speziellen Verwaltungsbereich für Kryptografieschlüssel verfügt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Mit diesen Funktionen können Administratoren für BI-Plattform-Implementierungen bestimmte Konformitätsstufen bezüglich der Datensicherheit einstellen und Schlüssel zum Ver- bzw. Entschlüsseln von Daten im CMS-Repository verwalten.

8.11.1 Sicherheitsmodi für die Datenverarbeitung

Die BI-Plattform kann in zwei möglichen Datenverarbeitungs-Sicherheitsmodi arbeiten:

- Dem Standardsicherheitsmodus für die Datenverarbeitung. In bestimmten Instanzen verwenden Systeme, die in diesem Modus ausgeführt werden, fest programmierte Schlüssel und folgen keinem bestimmten Standard. Der Standardmodus ermöglicht die Abwärtskompatibilität mit früheren Versionen von BI-Plattform-Clienttools und -Anwendungen.
- Ein Datensicherheitsmodus, der auf die Einhaltung der im Federal Information Processing Standard (FIPS) festgelegten Richtlinien ausgerichtet ist – insbesondere FIPS 140-2. In diesem Modus werden FIPS-konforme Algorithmen und Kryptografiemodule verwendet, um sensible Daten zu schützen. Wenn die Plattform im FIPS-konformen Modus ausgeführt wird, werden alle Clienttools und -Anwendungen, die den FIPS-Richtlinien nicht entsprechen, deaktiviert. Die Plattform-Clienttools und -Anwendungen sind mit dem FIPS 140-2-Standard konform. Ältere Clients und Anwendungen funktionieren nicht, wenn die BI-Plattform im FIPS-konformen Modus ausgeführt wird.

Der Datenverarbeitungsmodus ist für Systembenutzer erkennbar. In beiden Sicherheitsmodi für die Datenverarbeitung werden sensible Daten im Hintergrund von einer internen Verschlüsselungs-Engine ver- und entschlüsselt.

Es wird empfohlen, den FIPS-konformen Modus unter folgenden Umständen zu verwenden:

- Für Ihre BI-Plattform-Implementierung ist die Nutzung von oder Interaktion mit älteren BI-Plattform-Clienttools oder -Anwendungen nicht erforderlich.
- Die Datenverarbeitungsstandards und -richtlinien Ihres Unternehmens verbieten die Verwendung von fest programmierten Schlüsseln.
- Ihr Unternehmen muss sensible Daten gemäß den Richtlinien des FIPS 140-2 sichern.

Der Sicherheitsmodus für die Datenverarbeitung wird sowohl auf Windows- als auch auf UNIX-Plattformen über den Central Configuration Manager eingestellt. Jeder Knoten einer geclusterten Umgebung muss auf denselben Modus eingestellt sein.

8.11.1.1 Aktivieren des FIPS-konformen Modus unter Windows

Der FIPS-konforme Modus wird nach der Installation der BI-Plattform standardmäßig deaktiviert. Sie können die FIPS-Konformität jedoch für alle Knoten in Ihrer Implementierung aktivieren.

1. Um den CCM zu starten, wählen Sie **Programme** > **SAP Business Intelligence** > **SAP BusinessObjects Business Intelligence 4** > **Central Configuration Manager**.
2. Klicken Sie im CCM mit der rechten Maustaste auf den Server Intelligence Agent (SIA), und wählen Sie **Stop**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Achtung**
>
> Fahren Sie erst mit Schritt 3 fort, wenn der SIA-Status "Gestoppt" ist.

3. Klicken Sie mit der rechten Maustaste auf den SIA, und wählen Sie **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* wird geöffnet und zeigt die Registerkarte **Eigenschaften** an.
4. Fügen Sie `-fips` im Feld **Befehl** hinzu, und klicken Sie auf **Anwenden**.
5. Klicken Sie auf **OK**, um das Dialogfeld *Eigenschaften* zu schließen.
6. Starten Sie den SIA neu.

Der SIA wird nun im FIPS-konformen Modus ausgeführt.

Sie müssen den FIPS-konformen Modus für alle SIAs in Ihrer BI-Plattform-Implementierung aktivieren.

8.11.1.2 Aktivieren des FIPS-konformen Modus unter UNIX

Alle Knoten in Ihrer BI-Plattform-Implementierung müssen gestoppt werden, bevor Sie folgendes Verfahren ausprobieren.

Der FIPS-konforme Modus wird nach der Installation der BI-Plattform standardmäßig deaktiviert. Gehen Sie folgendermaßen vor, um den FIPS-konformen Modus für alle Knoten in Ihrer Implementierung zu aktivieren.

1. Öffnen Sie im Verzeichnis **`<INSTALLVERZ>`**`/sap_bobj` die Datei `ccm.config` zur Bearbeitung.
2. Fügen Sie `-fips` dem Befehlsparameter zum Starten des Knotens hinzu.

   Der Parameter für den Knotenstartbefehl wird in diesem Format angezeigt: **`<KNOTENNAME>`**`LAUNCH`.
   Beispielsweise lautet für den Knoten “SAP” der Parameter für den Knotenstartbefehl `SAPLAUNCH`.
3. Speichern Sie Ihre Änderungen, und klicken Sie auf **Beenden**
4. Starten Sie den Knoten neu.

Der Knoten wird nun im FIPS-konformen Modus ausgeführt.

Sie müssen den FIPS-konformen Modus für alle Knoten in Ihrer BI-Plattform-Implementierung aktivieren.

8.11.1.3 Deaktivieren des FIPS-konformen Modus unter Windows

Alle Server in Ihrer BI-Plattform-Implementierung müssen gestoppt werden, bevor Sie folgendes Verfahren ausprobieren.

Wenn Ihre Implementierung im FIPS-konformen Modus ausgeführt wird, gehen Sie folgendermaßen vor, um diese Einstellung zu deaktivieren:

1. Klicken Sie im CCM mit der rechten Maustaste auf den Server Intelligence Agent (SIA), und wählen Sie **Stop**.

> **Achtung**
>
> Fahren Sie nicht mit Schritt 2 fort, bis der Knotenstatus als *Gestoppt* markiert ist.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Klicken Sie mit der rechten Maustaste auf den SIA, und wählen Sie **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* wird geöffnet und zeigt die Registerkarte **Eigenschaften** an.
3. Entfernen Sie `-fips` aus dem *Befehl*-Feld, und klicken Sie auf **Anwenden**.
4. Klicken Sie auf **OK**, um das Dialogfeld *Eigenschaften* zu schließen.
5. Starten Sie den SIA neu.

8.12 Verschlüsselung in der BI-Plattform

Sensible Daten

Die Verschlüsselung in der BI-Plattform ist darauf ausgerichtet, sensible Daten im CMS-Repository zu schützen. Zu den sensiblen Daten gehören Anmeldedaten von Benutzern, Verbindungsdaten zu Datenquellen und andere Infoobjekte, in denen Kennwörter gespeichert sind. Diese Daten werden verschlüsselt, um Vertraulichkeit zu gewährleisten, Datenkorruption zu verhindern und den Zugriff zu steuern. Alle erforderlichen Verschlüsselungsressourcen (einschließlich Verschlüsselungs-Engine, RSA-Bibliotheken) werden standardmäßig mit jeder BI-Plattform-Implementierung installiert.

Das BI-Plattform-System verwendet ein Verschlüsselungssystem mit zwei Schlüsseln.

Kryptografieschlüssel

Die Ver- bzw. Entschlüsselung von sensiblen Daten wird im Hintergrund über die SDK abgewickelt, die mit der internen Verschlüsselungs-Engine interagiert. Systemadministratoren verwalten die Datensicherheit über symmetrische Schlüssel, ohne spezifische Datenblöcke direkt zu ver- oder entschlüsseln.

In der BI-Plattform werden symmetrische Kryptografieschlüssel zur Ver- bzw. Entschlüsselung sensibler Daten verwendet. Die Central Management Console verfügt über einen speziellen Verwaltungsbereich für Kryptografieschlüssel. Verwenden Sie die *Kryptografieschlüssel*, um Schlüssel anzuzeigen, zu generieren, zu deaktivieren, zurückzunehmen und zu löschen. Das System stellt sicher, dass Schlüssel, die für die Verschlüsselung von sensiblen Daten notwendig sind, nicht gelöscht werden.

Clusterschlüssel

Clusterschlüssel sind symmetrische, andere Schlüssel einschließende Schlüssel, die die im CMS-Repository gespeicherten Kryptografieschlüssel schützen. Mithilfe symmetrischer Schlüsselalgorithmen stellen Clusterschlüssel eine Ebene der Zugriffssteuerung für das CMS-Repository bereit. Jedem Knoten in der BI-Plattform wird während des Installationssetups ein Clusterschlüssel zugeordnet. Systemadministratoren können den Clusterschlüssel mithilfe des CCM zurücksetzen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.12.1 Arbeiten mit Clusterschlüsseln

Während der Installationseinrichtung für die BI-Plattform wird ein Clusterschlüssel mit acht Zeichen für den Server Intelligence Agent erstellt. Dieser Schlüssel wird zum Verschlüsseln aller Kryptografieschlüssel im CMS-Repository verwendet. Ohne den korrekten Clusterschlüssel können Sie nicht auf CMS zugreifen.

Der Clusterschlüssel wird im verschlüsselten Format in der Datei `dbinfo` gespeichert. Der Dateiname `dbinfo` entspricht folgender Konvention: `_boe_<sia_Name>.dbinfo`, wobei `<sia_Name>` der Name des Server-Intelligence-Agent für den Cluster ist.

Unter Windows ist die Datei in folgendem Verzeichnis abgelegt: `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.

Auf Unix-Systemen ist die Datei im Plattformverzeichnis unter `<INSTALLVERZ>/sap_bobj/enterprise_xi40/` gespeichert:

UNIX-Plattform	Plattformverzeichnis
AIX	`<INSTALLVERZ>/sap_bobj/enterprise_xi40/aix_rs6000_64 /`
Solaris	`<INSTALLVERZ>/sap_bobj/enterprise_xi40/solaris_sparcv9/`
Linux	`<INSTALLVERZ>/sap_bobj/enterprise_xi40/linux_x64/`

> **Hinweis**
>
> Der Clusterschlüssel für einen gegebenen Knoten kann aus der Datei `dbinfo` abgerufen werden. Es wird empfohlen, dass Systemadministratoren durchdachte und umsichtige Maßnahmen ergreifen, um die Clusterschlüssel zu schützen.

Nur Benutzer mit Administratorenrechten können Clusterschlüssel zurücksetzen. Setzen Sie gegebenenfalls den Clusterschlüssel für jeden Knoten der Implementierung mit dem CCM zurück. Neue Clusterschlüssel werden automatisch dazu verwendet, die Kryptografieschlüssel in das CMS-Repository einzubinden.

8.12.1.1 Zurücksetzen eines Clusterschlüssels unter Windows

Bevor Sie den Clusterschlüssel für Ihren Knoten zurücksetzen, vergewissern Sie sich, dass alle von diesem Server Intelligence Agent verwalteten Server gestoppt wurden.

1. Um den CCM zu starten, wählen Sie **Programme** > **SAP Business Intelligence** > **SAP BusinessObjects Business Intelligence 4** > **Central Configuration Manager**.
2. Klicken Sie im CCM mit der rechten Maustaste auf den Server Intelligence Agent (SIA), und wählen Sie **Stop**.

   > **Achtung**
   >
   > Fahren Sie erst mit Schritt 3 fort, wenn der SIA-Status "Gestoppt" ist.

3. Klicken Sie mit der rechten Maustaste auf den Server Intelligence Agent (SIA), und wählen Sie **Eigenschaften**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Das Dialogfeld *Eigenschaften* wird angezeigt.

4. Klicken Sie auf die Registerkarte **Konfiguration**.
5. Klicken Sie unter **Konfiguration des CMS-Clusterschlüssels** auf *Ändern*.
   Daraufhin wird eine Warnmeldung angezeigt.
6. Klicken Sie auf **Ja**, um fortzufahren.
   Das Dialogfeld *Clusterschlüssel ändern* wird geöffnet.
7. Geben Sie in die Felder **Neuer Clusterschlüssel** und **Neuen Clusterschlüssel bestätigen** denselben achtstelligen Schlüssel ein.

   > **Hinweis**
   >
   > Unter Windows muss der Clusterschlüssel eine Kombination von Groß- und Kleinbuchstaben enthalten. Alternativ können die Benutzer auch einen Zufallsschlüssel erzeugen. Ein Zufallsschlüssel ist für die FIPS-Konformität erforderlich.

8. Klicken Sie auf **OK** , um den neuen Clusterschlüssel an das System weiterzuleiten.
   Eine Meldung wird angezeigt, in der Ihnen bestätigt wird, dass der Clusterschlüssel erfolgreich zurückgesetzt wurde.
9. Starten Sie den SIA neu.

In einem Cluster mit mehreren Knoten müssen Sie die Clusterschlüssel für alle SIAs in Ihrer BI-Plattform-Implementierung auf den neuen Schlüssel zurücksetzen.

8.12.1.2 Zurücksetzen eines Clusterschlüssels unter UNIX

Bevor Sie den Clusterschlüssel für einen Knoten zurücksetzen, vergewissern Sie sich, dass alle von diesem Knoten verwalteten Server angehalten wurden.

1. Navigieren Sie zum Verzeichnis `<INSTALLVERZ>/sap_bobj`.
2. Geben Sie `./cmsdbsetup.sh` ein, und drücken Sie die **Eingabetaste**.
   Der Bildschirm *CMS-Datenbankeinrichtung* wird angezeigt.
3. Geben Sie den Namen des Knotens ein, und drücken Sie die **Eingabetaste**.
4. Geben Sie `2` ein, um den Clusterschlüssel zu ändern.
   Daraufhin wird eine Warnmeldung angezeigt.
5. Klicken Sie auf **Ja**, um fortzufahren.
6. Geben Sie einen neuen, achtstelligen Clusterschlüssel in das angezeigte Feld ein, und drücken Sie die **Eingabetaste**.

   > **Hinweis**
   >
   > Auf UNIX-Plattformen kann ein gültiger Clusterschlüssel eine beliebige Kombination von acht Zeichen enthalten, ohne Einschränkungen.

7. Geben Sie den neuen Clusterschlüssel in das entsprechende Feld noch einmal ein, und drücken Sie die **Eingabetaste**.
   Eine Meldung wird angezeigt, in der Ihnen mitgeteilt wird, dass der Clusterschlüssel erfolgreich zurückgesetzt wurde.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8. Starten Sie den Knoten neu.

Sie müssen alle Knoten in Ihrer BI-Plattform-Implementierung zurücksetzen, um denselben Clusterschlüssel zu verwenden.

8.12.2 Verschlüsselungsbeauftragte

Um Kryptografieschlüssel in der CMC verwalten zu können, müssen Sie Mitglied der Gruppe "Verschlüsselungsbeauftragte" sein. Das Standardadministratorkonto, das für die BI-Plattform erstellt wird, ist ebenfalls ein Element der Gruppe "Verschlüsselungsbeauftragte". Verwenden Sie dieses Konto, um Benutzer nach Bedarf der Gruppe "Verschlüsselungsbeauftragte" hinzuzufügen. Es wird empfohlen, die Mitgliedschaft in der Gruppe auf eine beschränkte Anzahl von Benutzern zu begrenzen.

> **Hinweis**
>
> Wenn Benutzer der Gruppe "Administratoren" hinzugefügt werden, erben sie nicht die erforderlichen Rechte, um Verwaltungsaufgaben an Kryptografieschlüsseln ausführen zu können.

8.12.2.1 Hinzufügen eines Benutzers zur Gruppe "Verschlüsselungsbeauftragte"

Ein Benutzerkonto muss in der BI-Plattform vorhanden sein, bevor es der Gruppe "Verschlüsselungsbeauftragte" hinzugefügt werden kann.

> **Hinweis**
>
> Sie müssen sowohl zur Gruppe *Administratoren* als auch zur Gruppe *Verschlüsselungsbeauftragte* gehören, um Benutzer zur Gruppe "Verschlüsselungsbeauftragte" hinzufügen zu können.

1. Wählen Sie im Verwaltungsbereich *Benutzer und Gruppen* der CMC die Gruppe **Verschlüsselungsbeauftragte** aus.
2. Klicken Sie auf **Aktionen** > **Elemente zur Gruppe hinzufügen**.
   Das Dialogfeld *Hinzufügen* wird angezeigt.
3. Klicken Sie auf **Benutzerliste**.
   Die Liste **Verfügbare Benutzer oder Gruppen** wird regeneriert und enthält alle Benutzerkonten im System.
4. Verschieben Sie das Benutzerkonto, das Sie der Gruppe "Verschlüsselungsbeauftragte" hinzufügen möchten, aus der Liste **Verfügbare Benutzer oder Gruppen** in die Liste **Ausgewählte Benutzer oder Gruppen**.

   > **Tipp**
   >
   > Um einen bestimmten Benutzer zu suchen, verwenden Sie das Suchfeld.

5. Klicken Sie auf **OK**.

Als Element der Gruppe "Verschlüsselungsbeauftragte" hat das neu hinzugefügte Konto Zugriff auf den *Kryptografieschlüssel*-Verwaltungsbereich in der CMC.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.12.2.2 Anzeigen von Kryptografieschlüsseln in der CMC

Die CMC-Anwendung enthält einen dedizierten Verwaltungsbereich für die vom BI-Plattform-System verwendeten Kryptografieschlüssel. Der Zugriff auf diesen Bereich ist auf Mitglieder der Verschlüsselungsbeauftragtengruppe beschränkt.

1. Um die CMC zu starten, klicken Sie auf **Programme** > **SAP Business Intelligence** > **SAP BusinessObjects Business Intelligence 4** > **Central Management Console von SAP BusinessObjects Business Intelligence**.
   Die CMC-Startseite wird angezeigt.
2. Klicken Sie auf die Registerkarte **Kryptografieschlüssel**.
   Der Verwaltungsbereich *Kryptografieschlüssel* wird angezeigt.
3. Doppelklicken Sie auf den Kryptografieschlüssel, für den Sie weitere Einzelheiten anzeigen möchten.

Weitere Informationen

Anzeigen der einem Kryptografieschlüssel zugeordneten Objekte [Seite 171]

8.12.3 Verwalten von Kryptografieschlüsseln in der CMC

Im Verwaltungsbereich *Kryptografieschlüssel* können Verschlüsselungsbeauftragte Schlüssel, die zum Schutz im CMS-Repository gespeicherter sensibler Daten verwendet werden, überprüfen, generieren, deaktivieren, sperren und löschen.

Alle derzeit im System definierten Kryptografieschlüssel werden im Verwaltungsbereich *Kryptografieschlüssel* aufgeführt. Grundlegende Informationen zu den einzelnen Schlüsseln sind unter den in der folgenden Tabelle beschriebenen Überschriften zu finden:

Überschrift	Beschreibung
title	Namen, der den Kryptografieschlüssel identifiziert
Status	Aktueller Status des Schlüssels
Letzte Statusänderung	Datums- und Zeitstempel der letzten mit dem Kryptografieschlüssel zusammenhängenden Änderung
Objekte	Anzahl der dem Schlüssel zugeordneten Objekte

Weitere Informationen

Status von Kryptografieschlüsseln [Seite 170]
Erstellen eines neuen Kryptografieschlüssels [Seite 171]
Löschen eines Kryptografieschlüssels aus dem System [Seite 173]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Sperren eines Kryptografieschlüssels [Seite 173]
Anzeigen der einem Kryptografieschlüssel zugeordneten Objekte [Seite 171]
Kryptografieschlüssel als gefährdet markieren [Seite 172]

8.12.3.1 Status von Kryptografieschlüsseln

In der folgenden Tabelle sind alle möglichen Statusoptionen für Kryptografieschlüssel in der BI-Plattform aufgelistet:

Status	Beschreibung
Aktiv	Nur ein Kryptografieschlüssel kann im System den Status *Aktiv* besitzen. Dieser Schlüssel wird zum Verschlüsseln aktueller sensibler Daten verwendet, die in der CMS-Datenbank gespeichert werden. Der Schlüssel wird außerdem zum Entschlüsseln aller Objekte in der entsprechenden Objektliste verwendet. Sobald ein neuer Kryptografieschlüssel erstellt wird, wird der Schlüssel, der aktuell *Aktiv* ist, auf *Deaktiviert* gesetzt. Ein aktiver Schlüssel kann nicht aus dem System gelöscht werden.
Deaktiviert	Ein Schlüssel mit dem Status *Deaktiviert* kann nicht länger zum Verschlüsseln von Daten verwendet werden. Er kann aber zum Entschlüsseln aller Objekte in der entsprechenden Objektliste verwendet werden. Sie können einen einmal deaktivierten Schlüssel nicht wieder aktivieren. Ein als *Deaktiviert* markierter Schlüssel kann nicht aus dem System gelöscht werden. Sie müssen den Status eines Schlüssels auf *Gesperrt* setzen, bevor Sie ihn löschen können.
Gefährdet	Ein Kryptografieschlüssel, der als unsicher eingeschätzt wird, kann als "Gefährdet" markiert werden. Wenn Sie einen solchen Schlüssel markieren, haben Sie später die Möglichkeit, Objekte neu zu verschlüsseln, die diesem Schlüssel noch zugeordnet sind. Wenn ein Schlüssel als "Gefährdet" markiert ist, muss er zurückgenommen werden, bevor er aus dem System gelöscht werden kann.
Gesperrt	Wenn ein Kryptografieschlüssel gesperrt wird, wird ein Prozess ausgelöst, mit dem alle diesem Schlüssel aktuell zugeordneten Objekte mit dem aktuellen "aktiven" Kryptografieschlüssel neu verschlüsselt werden. Sobald ein Schlüssel gesperrt wurde, kann er sicher aus dem System gelöscht werden. Durch den Rücknahmemechanismus wird sichergestellt, dass die Daten in der CMS-Datenbank jederzeit verschlüsselt werden können. Ein einmal zurückgenommener Schlüssel kann nicht wieder aktiviert werden.
Deaktiviert: Neuverschlüsselung wird ausgeführt	Zeigt an, dass der Kryptografieschlüssel gerade gesperrt wird. Sobald der Prozess abgeschlossen ist, wird der Schlüssel als *Gesperrt* markiert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Status	Beschreibung
Deaktiviert: Neuverschlüsselung angehalten	Zeigt an, dass der Prozess zum Zurücknehmen eines Kryptografieschlüssels angehalten wurde. Dies tritt in der Regel dann auf, wenn der Prozess absichtlich angehalten wurde oder wenn ein dem Schlüssel zugeordnetes Datenobjekt nicht verfügbar ist.
Gesperrt-Gefährdet	Ein Schlüssel wird als "Gesperrt-Gefährdet" markiert, wenn er als "Gefährdet" markiert wurde und alle vorher diesem Schlüssel zugeordneten Daten mit einem anderen Schlüssel verschlüsselt wurden. Wenn ein als *Deaktiviert* gekennzeichneter Schlüssel als "Gefährdet" markiert wird, haben Sie die Wahl, ob Sie nichts unternehmen oder den Schlüssel sperren. Sobald ein gefährdeter Schlüssel zurückgenommen wurde, kann er gelöscht werden.

8.12.3.2 Anzeigen der einem Kryptografieschlüssel zugeordneten Objekte

1. Wählen Sie den Schlüssel im *Kryptografieschlüssel* -Verwaltungsbereich der CMC aus.
2. Klicken Sie auf **Verwalten** > **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* des Kryptografieschlüssels wird angezeigt.
3. Klicken Sie auf *Objektliste* im Navigationsbereich auf der linken Seite des Dialogfelds *Eigenschaften*.
   Alle diesem Kryptografieschlüssel zugeordneten Objekte werden links vom Navigationsbereich angezeigt.

> **Tipp**
>
> Verwenden Sie die Suchfunktion, um nach einem bestimmten Objekt zu suchen.

8.12.3.3 Erstellen eines neuen Kryptografieschlüssels

> **Achtung**
>
> Wenn Sie einen neuen Kryptografieschlüssel erstellen, wird der aktuelle *Aktive* Schlüssel automatisch durch das System deaktiviert. Sobald ein Schlüssel deaktiviert wurde, kann er nicht mehr als *Aktiver* Schlüssel wiederhergestellt werden.

1. Klicken Sie im Verwaltungsbereich *Kryptografieschlüssel* der CMC auf **Verwalten** > **Neu** > **Kryptografieschlüssel**.
   Das Dialogfeld *Neuen Kryptografieschlüssel erstellen* wird angezeigt.
2. Klicken Sie auf **Weiter**, um einen neuen Kryptografieschlüssel zu erstellen.
3. Geben Sie den Namen und eine Beschreibung des neuen Kryptografieschlüssels ein; klicken Sie auf **OK**, um die Angaben zu speichern.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Der neue Schlüssel wird im Verwaltungsbereich *Kryptografieschlüssel* als einziger aktiver Schlüssel aufgeführt. Der vorherige *Aktive* Schlüssel wird nun als *Deaktiviert* angegeben.

Alle neuen in der CMS-Datenbank generierten und gespeicherten sensiblen Daten, werden nun mit dem neuen Kryptografieschlüssel verschlüsselt. Sie haben die Möglichkeit, den vorherigen Schlüssel zu sperren und alle zugehörigen Datenobjekte mit dem neuen aktiven Schlüssel erneut zu verschlüsseln.

8.12.3.4 Kryptografieschlüssel als gefährdet markieren

Wenn ein Kryptografieschlüssel aus irgendwelchen Gründen nicht mehr als sicher gilt, können Sie ihn als gefährdet markieren. Dies ist sinnvoll zu Tracking-Zwecken, und Sie können dann identifizieren, welche Datenobjekte dem Schlüssel zugeordnet sind. Bevor ein Kryptografieschlüssel als gefährdet markiert werden kann, muss er deaktiviert werden.

> **Hinweis**
>
> Wenn ein Schlüssel gesperrt wurde, muss er ebenfalls als gefährdet markiert werden.

1. Wechseln Sie zum Verwaltungsbereich *Kryptografieschlüssel* der CMC.
2. Wählen Sie den Kryptografieschlüssel aus, den Sie als gefährdet markieren möchten.
3. Klicken Sie auf **Aktionen** > **Als gefährdet markieren**.
   Das Dialogfeld *Als gefährdet markieren* wird angezeigt.
4. Klicken Sie auf **Continue** (Weiter).
5. Wählen Sie im Dialogfeld *Als gefährdet markieren* eine der folgenden Optionen aus:
   - **Ja**: startet den Prozess zum erneuten Verschlüsseln aller Datenobjekte, die dem gefährdeten Schlüssel zugeordnet sind.
   - **Nein**: das Dialogfeld *Als gefährdet markieren* wird geschlossen, und der Kryptografieschlüssel wird im Verwaltungsbereich *Kryptografieschlüssel* als *Gefährdet* markiert.

     > **Hinweis**
     >
     > Wenn Sie **Nein** wählen, sind sensible Daten weiterhin dem gefährdeten Schlüssel zugeordnet. Der gefährdete Schlüssel wird durch das System zum Entschlüsseln der zugeordneten Objekte verwendet.

Weitere Informationen

Sperren eines Kryptografieschlüssels [Seite 173]
Status von Kryptografieschlüsseln [Seite 170]
Anzeigen der einem Kryptografieschlüssel zugeordneten Objekte [Seite 171]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.12.3.5 Sperren eines Kryptografieschlüssels

Ein deaktivierter Kryptografieschlüssel kann noch immer von den mit ihm verknüpften Datenobjekten verwendet werden. Um den Mechanismus zwischen den verschlüsselten Objekten und dem deaktivierten Schlüssel zu unterbrechen, müssen Sie den Schlüssel sperren.

1. Wählen Sie den zu sperrenden Schlüssel unter den im Verwaltungsbereich *Kryptografieschlüssel* aufgeführten Schlüsseln aus.
2. Klicken Sie auf **Aktionen** > **Sperren**.
   Das Dialogfeld *Sperren* wird angezeigt.
3. Klicken Sie auf **OK**.
   Ein Prozess zum Verschlüsseln aller Objekte des Schlüssels mit dem aktuellen aktiven Schlüssel wird gestartet. Wenn der Schlüssel mit vielen Datenobjekten verknüpft ist, wird er als *Deaktiviert: Neuverschlüsselung wird ausgeführt* markiert, bis der Neuverschlüsselungsprozess abgeschlossen ist.

Nachdem ein Kryptografieschlüssel gesperrt wurde, kann er sicher vom System entfernt werden, da er von keinem sensiblen Datenobjekt zur Verschlüsselung benötigt wird.

8.12.3.6 Löschen eines Kryptografieschlüssels aus dem System

Bevor Sie einen Kryptografieschlüssel aus der BI-Plattform löschen können, müssen Sie sicherstellen, dass keine Datenobjekte im System den Schlüssel benötigen. Durch diese Einschränkung wird sichergestellt, dass alle im CMS-Repository gespeicherten sensiblen Daten jederzeit entschlüsselt werden können.

Nachdem Sie einen Kryptografieschlüssel gesperrt haben, folgen Sie den unten stehenden Anweisungen, um den Schlüssel aus dem System zu löschen.

1. Wechseln Sie zum Verwaltungsbereich *Kryptografieschlüssel* der CMC.
2. Wählen Sie den zu löschenden Kryptografieschlüssel aus.
3. Klicken Sie auf **Verwalten** > **Löschen**.
   Das Dialogfeld *Löschen* wird angezeigt.
4. Klicken Sie auf **Löschen**, um den Kryptografieschlüssel aus dem System zu löschen.
   Der gelöschte Schlüssel wird nicht mehr im Verwaltungsbereich *Kryptografieschlüssel*der CMC angezeigt.

> **Hinweis**
>
> Sobald ein Kryptografieschlüssel aus dem System gelöscht wurde, kann er nicht mehr wiederhergestellt werden.

Weitere Informationen

Sperren eines Kryptografieschlüssels [Seite 173]
Status von Kryptografieschlüsseln [Seite 170]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.13 Konfigurieren von Servern für SSL

Sie können das SSL-Protokoll (Secure Sockets Layer) für die gesamte Netzwerkkommunikation zwischen Clients und Servern in der BI-Plattform-Implementierung verwenden.

Um SSL für die gesamte Serverkommunikation einzurichten, führen Sie folgende Schritte aus:

- Implementieren Sie die BI-Plattform mit aktiviertem SSL.
- Erstellen Sie Schlüssel- und Zertifikatdateien für jeden Rechner innerhalb Ihrer Implementierung.
- Konfigurieren Sie den Speicherort dieser Dateien im Central Configuration Manager (CCM) und in Ihrem Webanwendungsserver.
- Oder konfigurieren Sie SSL für von einer Zertifizierungsstelle verwaltete Zertifikate.

> **Hinweis**
>
> Bei Verwendung von Thick-Clients wie z.B. Crystal Reports müssen diese auch für SSL konfiguriert werden, wenn von diesen Thick-Clients aus eine Verbindung zum CMS hergestellt werden soll. Wenn Sie andernfalls versuchen, von einem Thick-Client aus, der nicht genauso konfiguriert wurde, eine Verbindung zu einem für SSL konfigurierten CMS herzustellen, treten Fehler auf.

8.13.1 Erstellen von Schlüssel- und Zertifikatdateien

Um das SSL-Protokoll für die Serverkommunikation einzurichten, erstellen Sie mit dem SSLC-Befehlszeilentool je eine Schlüssel- und Zertifikatdatei für jeden Rechner innerhalb Ihrer Implementierung.

> **Hinweis**
>
> Schlüssel und Zertifikate müssen für alle Rechner in der Implementierung erstellt werden, auch für Rechner, auf denen Thick-Client-Komponenten wie Crystal Reports ausgeführt werden. Bei diesen Clientrechnern verwenden Sie zur Konfiguration das Befehlszeilentool `sslconfig`.

> **Hinweis**
>
> Um maximale Sicherheit zu gewährleisten, sollten alle privaten Schlüssel gesichert sein und nicht über unsichere Kommunikationskanäle verbreitet werden.

> **Hinweis**
>
> Für frühere Versionen der BI-Plattform erstellte Zertifikate sind auf SAP BI Plattform 4.0 nicht anwendbar. Diese Zertifikate müssen neu erstellt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.13.1.1 Erstellen von Schlüssel- und Zertifikatdateien für einen Rechner

1. Führen Sie das `sslc`-Befehlszeilentool aus.

   Das SSLC-Tool wird mit der BI-Plattform-Software installiert. (Unter Windows ist das Installationsverzeichnis standardmäßig **<INSTALLDIR>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.)

2. Geben Sie folgenden Befehl ein:

   ```
   sslc req -config sslc.cnf -new -out cacert.req
   ```

   Durch diesen Befehl werden zwei Dateien erstellt, eine Certificate-Authority-Zertifikatanforderung (`cacert.req`) und ein privater Schlüssel (`privkey.pem`).

3. Zum Entschlüsseln des privaten Schlüssels geben Sie folgenden Befehl ein:

   ```
   sslc rsa -in privkey.pem -out cakey.pem
   ```

   Durch diesen Befehl wird der entschlüsselte Schlüssel `cakey.pem` erstellt.

4. Zum Signieren des CA-Zertifikats geben Sie den folgenden Befehl ein:

   ```
   sslc x509 -in cacert.req -out cacert.pem -req -signkey cakey.pem -days 365
   ```

   Durch diesen Befehl wird das selbstsignierte Zertifikat "`cacert.pem`" erstellt, das nach 365 Tagen abläuft. Wählen Sie entsprechend Ihren Sicherheitsanforderungen die Anzahl der Tage aus.

5. Öffnen Sie mit einem Text-Editor die Datei `sslc.cnf`, die sich im selben Ordner wie das SSLC-Befehlzeilentool befindet.

   > **Hinweis**
   >
   > Für Windows muss ein Text-Editor verwendet werden, da Dateien mit der `.cnf`-Erweiterung von Windows Explorer u.U. nicht erkannt und angezeigt werden.

6. Führen Sie gemäß den Einstellungen in der Datei `sslc.cnf` folgende Schritte aus.

   a) Legen Sie die Dateien `cakey.pem` und `cacert.pem` in den Verzeichnissen ab, die durch die Optionen `certificate` und `private_key` der Datei `sslc.cnf` festgelegt wurden. Die Einstellungen in der Datei "`sslc.cnf`" lauten standardmäßig:

      ```
      certificate = $dir/cacert.pem
      ```

      ```
      private_key = $dir/private/cakey.pem
      ```

   b) Erstellen Sie eine Datei mit dem Namen, der in der Datei `sslc.cnf` unter der Einstellung `database` festgelegt wurde.

      > **Hinweis**
      >
      > Die Datei heißt standardmäßig `$dir/index.txt` und müsste leer sein.

   c) Erstellen Sie eine Datei mit dem Namen, der in der Datei `sslc.cnf` unter der Einstellung `serial` festgelegt wurde.

      Diese Datei muss eine Oktett-Seriennummer (im Hexadezimalformat) aufweisen.

      > **Hinweis**
      >
      > Um sicherzustellen, dass Sie weitere Zertifikate erstellen und signieren können, wählen Sie eine hohe gerade Hexadezimalzahl wie 1111111111111111111111111111111.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

d) Erstellen Sie das Verzeichnis, das in der Datei `sslc.cnf` durch die Einstellung `new_certs_dir` festgelegt wurde.

7. Um eine Zertifikatanforderung und einen privaten Schlüssel zu erstellen, geben Sie folgenden Befehl ein:

   ```
   sslc req -config sslc.cnf -new -out servercert.req
   ```

   Die erstellten Zertifikat- und Schlüsseldateien werden im aktuellen Arbeitsordner abgelegt.

8. Zum Entschlüsseln des Schlüssels in der Datei `privkey-pem` geben Sie folgenden Befehl ein:

   ```
   sslc rsa -in privkey.pem -out server.key
   ```

9. Zum Signieren des Zertifikats mit dem CA-Zertifikat geben Sie den folgenden Befehl ein:

   ```
   sslc ca -config sslc.cnf -days 365 -out servercert.pem -in servercert.req
   ```

   Durch diesen Befehl wird die Datei "`servercert.pem`" erstellt, die das signierte Zertifikat enthält.

10. Verwenden Sie folgende Befehle zum Konvertieren der Zertifikate in DER-codierte Zertifikate:

    ```
    sslc x509 -in cacert.pem -out cacert.der -outform DER
    ```

    ```
    sslc x509 -in servercert.pem -out servercert.der -outform DER
    ```

    > **Hinweis**
    >
    > Das CA-Zertifikat (`cacert.der`) und der zugehörige private Schlüssel (`cakey.pem`) müssen pro Implementierung nur einmal generiert werden. Alle Rechner innerhalb einer Implementierung verwenden dieselben CA-Zertifikate. Alle übrigen Zertifikate müssen mit dem privaten Schlüssel eines CA-Zertifikats signiert werden.

11. Erstellen Sie eine Textdatei `passphrase.txt` zum Speichern des Textes `passphrase`, der zum Entschlüsseln des generierten privaten Schlüssels verwendet wird.

12. Speichern Sie die folgende Schlüssel- und Zertifikatdatei (im selben Verzeichnis) an einem sicheren Ort, auf den andere Rechner innerhalb Ihrer BI-Plattform-Implementierung zugreifen können:

    - vertrauenswürdige Zertifikatdatei (`cacert.der`)
    - generierte Serverzertifikatdatei (`servercert.der`)
    - Serverschlüsseldatei (`server.key`)
    - Kennphrasendatei (`passphrase.txt`)

    Dieser Speicherort wird verwendet, um SSL für den CCM und den Webanwendungsserver zu konfigurieren.

8.13.2 Einrichten von SSL bei Verwaltung des Zertifikats durch eine Zertifizierungsstelle

Führen Sie zum Einrichten von SSL für die Serverkommunikation folgende Schritte aus, wenn das Zertifikat durch eine Zertifizierungsstelle verwaltet wird.

1. Exportieren Sie das gewünschte Zertifikat mit seinem privaten Schlüssel im Format PKCS #12 (.PFX).

   Dies wird als Zertifikat für die Zertifizierungsstelle verwendet.

2. Führen Sie über OpenSSL die folgenden Befehle aus:

   1. Exportieren Sie die Datei mit dem privaten Schlüssel von der .pfx-Datei:

      ```
      openssl pkcs12 - in Dateiname.pfx -nocerts -out privkey.pem
      ```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Exportieren Sie die Zertifikatdatei von der .pfx-Datei:

   ```
   openssl pkcs12 -in Dateiname.pfx -clcerts -nokeys -out cacert.pem
   ```

3. Entfernen Sie die Kennphrase aus dem privaten Schlüssel:

   ```
   openssl rsa -in privkey.pem -out cakey.pem
   ```

3. Richten Sie die erforderlichen Dateien ein:
   - Kopieren Sie `cakey.pem` in `C:\SSL\private\cakey.pem`.
   - Kopieren Sie `cacert.pem` in `C:\SSL\cacert.pem`.
   - Erstellen Sie eine leere Textdatei (eine Datenbank-Indexdatei) mit dem Namen `index.txt` im Ordner `C:\SSL`.
   - Erstellen Sie eine weitere Textdatei: `C:\SSL\serial`.
   - Öffnen Sie die Datei `C:\SSL\serial` in einem Texteditor, geben Sie den folgenden Wert ein, und speichern Sie die Datei: `1111111111111111111`
4. Öffnen Sie die Datei `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86\sslc.cnf` in einem Texteditor.

   Wählen Sie eine der folgenden Optionen:
   - Ändern Sie den Wert der Variablen `policy` in `policy_anything`. Durch diese Änderung können Sie ein Serverzertifikat erstellen, das nicht dieselben Richtlinien wie das Zertifikat Ihrer Zertifizierungsstelle hat.
   - Oder lassen Sie den Wert der `policy`-Variablen unverändert als `policy_match`. Dadurch wird das Serverzertifikat gezwungen, dieselben Richtlinien wie das Zertifikat Ihrer Zertifizierungsstelle zu verwenden. In diesem Fall müssen Sie die `req_distinguished_name`-Eigenschaften entsprechend ändern.
5. Erstellen Sie eine Zertfikatsanforderung und einen privaten Schlüssel.

   Führen Sie in einer Eingabeaufforderung den folgenden Befehl aus:

   ```
   sslc req -config sslc.cnf -new -out servercert.req
   ```

   > **Hinweis**
   >
   > Geben Sie für die `PEM-Kennphrase` ein aus mindestens vier Zeichen bestehendes Kennwort ein.

   > **Hinweis**
   >
   > Geben Sie für `Common Name` den vollständig qualifizierten Domänennamen des Rechners ein, auf dem die BI-Plattform-Server ausgeführt werden.

   > **Hinweis**
   >
   > Die Datei `servercert.req` wird in `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` erstellt.

   > **Hinweis**
   >
   > Die Dateien `.rnd` und `privkey.pem` werden geändert.

6. Entschlüsseln Sie den privaten Schlüssel.

   ```
   sslc rsa -in privkey.pem -out server.key
   ```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7. Unterzeichnen Sie das Zertifikat.

```
sslc ca -config sslc.cnf -days 365 -out servercert.pem -in servercert.req
```

> **Hinweis**
>
> Die Datei `servercert.pem` wird im Verzeichnis `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` erstellt.

> **Hinweis**
>
> Die Datei `1111111111111111111.pem` wird im Verzeichnis `C:\SSL\newcerts` erstellt.

> **Hinweis**
>
> Es wird eine Sicherung der Datei `serial` mit der Bezeichnung `serial.old` erstellt.

> **Hinweis**
>
> Der Wert von `serial` wird von `1111111111111111111` auf `1111111111111111112` erhöht.

8. Konvertieren Sie die Zertifikate in DER-Codierung.

   Führen Sie die folgenden Befehle aus:

```
sslc x509 -in cacert.pem -out cacert.der -outform DER
sslc x509 -in servercert.pem -out servercert.der -outform DER
```

> **Hinweis**
>
> Die Datei `servercert.der` wird im Verzeichnis `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` erstellt.

> **Hinweis**
>
> Die Datei `cacert.der` wird im Verzeichnis `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` erstellt.

9. Erstellen Sie eine Textdatei mit dem Namen `passphrase.txt`.

   Der Kontext der Datei sollte die zuvor von Ihnen verwendete PEM-Kennphrase sein.

10. Legen Sie die folgenden Dateien an einem sicheren Ort ab, z.B. `C:\SSLCerts`.
    - die vertrauenswürdige Zertifikatdatei `cacert.der`
    - die generierte Serverzertifikatdatei `servercert.der`
    - die Serverschlüsseldatei `server.key`
    - die Kennphrasendatei `passphrase.txt`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.13.3 Konfigurieren des SSL-Protokolls

Nachdem Sie Schlüssel und Zertifikate für jeden Rechner innerhalb der Implementierung erstellt und an einem sicheren Ort gespeichert haben, müssen Sie dem Central Configuration Manager (CCM) und dem Webanwendungsserver den sicheren Speicherort mitteilen.

Außerdem sind bestimmte Schritte zur Konfiguration des SSL-Protokolls für den Webanwendungsserver und für jeden Rechner mit einer Thick-Clientanwendung zu auszuführen.

8.13.3.1 Konfigurieren des SSL-Protokolls im CCM

1. Klicken Sie im CCM mit der rechten Maustaste auf den Server Intelligence Agent, und wählen Sie **Eigenschaften**.
2. Klicken Sie im Dialogfeld "Eigenschaften" auf die Registerkarte **Protokoll**.
3. Stellen Sie sicher, dass **SSL aktivieren** ausgewählt ist.
4. Geben Sie den Dateipfad zum Verzeichnis ein, in dem die Schlüssel- und Zertifikatdatei gespeichert wurde.

Feld	Beschreibung
SSL-Zertifikatordner	Ordner, in dem alle erforderlichen SSL-Zertifikate und -Dateien gespeichert sind. Beispiel:`d:\ssl`
Server-SSL-Zertifikatdatei	Name der Datei, die zum Speichern des Server-SSL-Zertifikats verwendet wird. Standardmäßig `servercert.der`
Dateien für vertrauenswürdige SSL-Zertifikate	Name der Datei mit dem vertrauenswürdigen SSL-Zertifikat. Der Name lautet standardmäßig `cacert.der`
Datei für den privaten SSL-Schlüssel	Name der Datei für den privaten SSL-Schlüssel für den Zugriff auf das Zertifikat. Der Name lautet standardmäßig `server.key`
Kennsatzdatei für den privaten SSL-Schlüssel	Name der Textdatei, die den für den Zugriff auf den privaten Schlüssel verwendeten Kennsatz enthält. Der Name lautet standardmäßig `passphrase.txt`

Hinweis

Geben Sie das Verzeichnis für den Rechner an, auf dem der Server ausgeführt wird.

8.13.3.2 Konfigurieren des SSL-Protokolls unter UNIX

Zur Konfiguration des SSL-Protokolls für SIA müssen Sie das Skript `serverconfig.sh` verwenden. Über die Textoberfläche dieses Skripts können Sie Serverinformationen abrufen, Server zur Installation hinzufügen und Server entfernen. Das Skript `serverconfig.sh` befindet sich im Installationsverzeichnis `sap_bobj`.

1. Stoppen Sie den SIA und alle SAP-BusinessObjects-Server mit dem Skript `ccm.sh`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Führen Sie das Script `serverconfig.sh` aus.
3. Wählen Sie **3 – Knoten ändern** aus, und drücken Sie die *Eingabetaste*.
4. Geben Sie den Ziel-SIA ein, und drücken Sie die *Eingabetaste*.
5. Wählen Sie die **1 – Server-Intelligence-Agent-SSL-Konfiguration ändern** aus.
6. Wählen Sie **ssl** aus.
   Geben Sie bei entsprechender Aufforderung die Speicherorte der SSL-Zertifikate an.
7. Wiederholen Sie die Schritte 1 bis 6 für jeden SIA, wenn es sich bei Ihrer BI-Plattform-Implementierung um ein SIA-Cluster handelt.
8. Starten Sie den SIA über das Skript`ccn.sh` und warten Sie, bis die Server gestartet werden.

8.13.3.3 Konfigurieren des SSL-Protokolls für den Webanwendungsserver

1. Falls Sie über einen J2EE-Webanwendungsserver verfügen, führen Sie das Java SDK mit den folgenden Systemeigenschaften aus. Beispiel:

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=d:\ssl -DtrustedCert=cacert.der
-DsslCert=clientcert.der -DsslKey=client.key
-Dpassphrase=passphrase.txt
```

   Die folgende Tabelle enthält die Beschreibungen für diese Beispiele:

Beispiel	Beschreibung
<DcertDir> =d:\ssl	Das Verzeichnis, in dem alle Zertifikate und Schlüssel gespeichert werden.
<DtrustedCert> =cacert.der	Vertrauenswürdige Zertifikatdatei. Mehrere Dateien werden durch Semikolon getrennt.
<DsslCert> =clientcert.der	Im SDK verwendetes Zertifikat.
<DsslKey> =client.key	Privater Schlüssel des SDK-Zertifikats.
<Dpassphrase> =passphrase.txt	Die Datei, in der der Kennsatz für den privaten Schlüssel gespeichert wird.

2. Falls Sie über einen IIS-Webanwendungsserver verfügen, führen Sie das Tool `sslconfig` mit folgenden Konfigurationsschritten von der Befehlszeile aus.

8.13.3.4 Konfigurieren von Thick Clients

Bevor Sie das folgende Verfahren ausführen, müssen Sie alle erforderlichen SSL-Ressourcen wie Zertifikate und private Schlüssel in einem bekannten Verzeichnis erstellt und gespeichert haben.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Im Verfahren unten wird davon ausgegangen, dass Sie die Anweisungen zum Erstellen der folgenden SSL-Ressourcen befolgt haben:

SSL-Ressource	
SSL-Zertifikatordner	**d:\ssl**
Dateiname des Server-SSL-Zertifikats	**servercert.der**
Dateiname des vertrauenswürdigen SSL-Zertifikats oder Stammzertifikats	**cacert.der**
Dateiname des privaten SSL-Schlüssels	**server.key**
Datei mit dem Kennsatz für den Zugriff auf die Datei mit dem privaten SSL-Schlüssel	**passphrase.txt**

Nachdem die obigen Ressourcen erstellt wurden, können Sie Thick Client-Anwendungen wie Central Configuration Manager (CCM) oder das Upgrade-Management-Tool anhand der folgenden Anleitung konfigurieren.

1. Stellen Sie sicher, dass die Thick-Clientanwendung nicht in Betrieb ist.

   Hinweis

   Geben Sie das Verzeichnis für den Rechner an, auf dem der Server ausgeführt wird.

2. Führen Sie das Befehlszeilentool `sslconfig.exe` aus.

   Das SSLC-Tool wird mit der BI-Plattform-Software installiert. (Unter Windows ist das Installationsverzeichnis standardmäßig `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.)

3. Geben Sie den folgenden Befehl ein:

```
sslconfig.exe -dir d:\SSL -mycert servercert.der -rootcert cacert.der -mykey
server.key
-passphrase     passphrase.txt -protocol ssl
```

4. Starten Sie die Thick-Clientanwendung neu.

Weitere Informationen

Erstellen von Schlüssel- und Zertifikatdateien für einen Rechner [Seite 175]

8.13.3.4.1 Konfigurieren der SSL-Anmeldung für das Übersetzungsmanagement-Tool

Damit Benutzer die SSL-Anmeldung mit dem Übersetzungsmanagement-Tool verwenden können, müssen Sie Informationen zu den SSL-Ressourcen in die Konfigurationsdatei (`.ini`) des Tools eintragen.

1. Suchen Sie die Datei `TransMgr.ini` im folgenden Verzeichnis: **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Öffnen Sie die Datei `TransMgr.ini` mit einem Texteditor.
3. Fügen Sie die folgenden Parameter hinzu:

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=<D:\SSLCert>
-DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key
-Dpassphrase=passphrase.txt -jar program.jar
```

4. Speichern Sie die Datei, und schließen Sie den Texteditor.

Benutzer können sich jetzt unter Verwendung von SSL beim Übersetzungsmanagement-Tool anmelden.

8.13.3.4.2 Konfigurieren von SSL für das Berichtskonvertierungstool

Bevor Sie das folgende Verfahren ausführen, müssen Sie alle erforderlichen SSL-Ressourcen wie Zertifikate und private Schlüssel in einem bekannten Verzeichnis erstellt und gespeichert haben. Darüber hinaus muss das Berichtskonvertierungstool im Rahmen der BI-Plattform-Implementierung installiert worden sein.

Im Verfahren unten wird davon ausgegangen, dass Sie die Anweisungen zum Erstellen der folgenden SSL-Ressourcen befolgt haben:

SSL-Ressource	
SSL-Zertifikatordner	**d:\ssl**
Dateiname des Server-SSL-Zertifikats	**servercert.der**
Dateiname des vertrauenswürdigen SSL-Zertifikats oder Stammzertifikats	**cacert.der**
Dateiname des privaten SSL-Schlüssels	**server.key**
Datei mit dem Kennsatz für den Zugriff auf die Datei mit dem privaten SSL-Schlüssel	**passphrase.txt**

Nachdem die obigen Ressourcen erstellt wurden, können Sie SSL für die Verwendung mit dem Berichtskonvertierungstool anhand der folgenden Anleitung konfigurieren.

1. Erstellen Sie die Windows-Umgebungsvariable **<BOBJ_MIGRATION>** auf dem Rechner, der das Berichtskonvertierungstool hostet.

   Tipp

   Die Variable kann auf einen beliebigen Wert festgelegt werden.

2. Öffnen Sie die Datei `migration.bat` mit einem Texteditor im folgenden Verzeichnis:

   `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\scripts\.`

3. Suchen Sie die folgende Zeile:

```
start "" "%JRE%\bin\javaw" -cp migration.jar;*  -Xmx512m -Xss10m
com.bo.migration.MigrationTool
```

4. Fügen Sie nach dem Parameter *-Xss10m* Folgendes hinzu:

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=d:\ssl
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dbusinessobjects.migration
```

> **Hinweis**
>
> Stellen Sie sicher, dass ein Leerschritt zwischen den einzelnen Parametern steht und am Zeilenende keine Leerstellen sind.

5. Speichern Sie die Datei, und schließen Sie den Texteditor.

Benutzer können jetzt unter Verwendung von SSL auf das Berichtskonvertierungstool zugreifen.

Weitere Informationen

Erstellen von Schlüssel- und Zertifikatdateien für einen Rechner [Seite 175]

8.14 Erläuterung der Kommunikation zwischen BI-Plattform-Komponenten

Wenn das gesamte BI-Plattform-System im selben gesicherten Subnetz implementiert wird, müssen die Firewalls nicht speziell konfiguriert werden. Sie können einige Komponenten jedoch auch in unterschiedlichen Subnetzen implementieren, die durch eine oder mehrere Firewalls getrennt sind.

Sie sollten verstehen, wie die Kommunikation zwischen BI-Plattform-Servern, Rich-Clients und dem Webanwendungsserver, der das SAP BusinessObjects SDK hostet, abläuft, bevor Sie Ihr System für die Unterstützung von Firewalls konfigurieren.

Weitere Informationen

Konfigurieren der BI-Plattform für Firewalls [Seite 191]
Beispiele für typische Firewallszenarios [Seite 196]

8.14.1 Überblick über BI-Server und Kommunikationsports

Es ist wichtig, die BI-Server und ihre Kommunikationsports zu verstehen, wenn das System mit Firewalls implementiert wurde.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.14.1.1 Bindung eines jeden BI-Servers an einen Anforderungs-Port

Ein BI-Server, z.B. der Input File Repository Server, wird beim Starten an einen Anforderungs-Port gebunden. Andere BI-Plattform-Komponenten, z.B. Server, Rich-Clients und das auf dem Webanwendungsserver gehostete SDK, können diesen Anforderungs-Port verwenden, um mit dem Server zu kommunizieren.

Die Nummer des Anforderungs-Ports wird vom Server dynamisch beim Start oder Neustart des Servers ausgewählt, sofern er nicht mit einer bestimmten Portnummer konfiguriert wurde. Für Server, die über eine Firewall mit anderen BI-Plattform-Komponenten kommunizieren, muss eine spezifische Anforderungs-Portnummer manuell konfiguriert werden.

8.14.1.2 Jeder BI-Server wird beim CMS registriert

BI-Server werden bei Ihrem Start beim CMS registriert. Der CMS zeichnet bei der Serverregistrierung folgende Informationen auf:

- Hostname (oder IP-Adresse) für den Hostrechner des Servers
- Anforderungsportnummer des Servers

8.14.1.3 Der CMS verwendet zwei Ports.

Der CMS verwendet zwei Ports: den Anforderungsport und den Name Server-Port. Der Anforderungsport wird standardmäßig dynamisch ausgewählt. Der Name Server-Port lautet standardmäßig 6400.

Alle BI-Server und Client-Anwendungen nehmen den ersten Kontakt zum CMS™ über dessen Name Server-Port auf. Der CMS™ reagiert auf die anfängliche Kontaktaufnahme, indem er den Wert seines Anforderungsports zurückgibt. Anschließend verwenden die Server diesen Anforderungsport für die Kommunikation mit dem CMS™.

8.14.1.4 Verzeichnis registrierter Dienste des Central Management Server (CMS)

Der CMS enthält ein Verzeichnis der Dienste, die sich beim CMS registriert haben. Andere BI-Plattform-Komponenten wie Webdienste, Rich-Clients und das auf dem Webanwendungsserver gehostete SDK können den CMS kontaktieren und einen Verweis auf einen bestimmten Dienst anfordern. Ein Dienstverweis enthält die Nummer des Anforderungsports des Diensts und den Hostnamen (oder die IP-Adresse) für den Hostrechner des Servers und die Dienst-ID.

BI-Plattform-Komponenten können sich in einem anderen Teilnetz als der von ihnen verwendete Server befinden. Der im Dienstverweis enthaltene Hostname (bzw. die IP-Adresse) muss vom Rechner der Komponente geroutet werden können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Der Verweis auf einen BI-Plattform-Server enthält standardmäßig den Hostnamen des Serverrechners. (Wenn ein Rechner mehrere Hostnamen hat, wird der primäre Hostname gewählt). Sie können einen Server auch so konfigurieren, dass dessen Verweis stattdessen die IP-Adresse enthält.

Weitere Informationen

Kommunikation zwischen BI-Plattform-Komponenten [Seite 186]

8.14.1.5 Server Intelligence Agents (SIA) kommunizieren mit dem Central Management Server (CMS)

Ihre Implementierung funktioniert nicht, wenn Server Intelligence Agent (SIA) und Central Management Server (CMS) nicht miteinander kommunizieren können. Die Firewall-Ports müssen so konfiguriert sein, dass die Kommunikation zwischen allen SIAs und CMS im Cluster erlaubt ist.

8.14.1.6 Untergeordnete Job Server-Prozesse kommunizieren mit der Datenschicht und dem CMS.

Die meisten Job Server erstellen einen untergeordneten Prozess, um Aufgaben wie das Generieren eines Berichts zu verarbeiten. Der Job Server erstellt einen oder mehrere untergeordnete Prozesse. Jeder untergeordnete Prozess verfügt über einen eigenen Anforderungs-Port.

Standardmäßig wählt ein Job Server für jeden untergeordneten Prozess dynamisch einen Anforderungs-Port aus. Sie können einen Bereich von Portnummern angeben, aus denen der Job Server auswählen kann.

Alle untergeordneten Prozesse kommunizieren mit dem CMS. Wenn dieser Kommunikationspfad eine Firewall passiert, muss

- Geben Sie den Bereich der Portnummern an, unter denen der Jobserver eine Wahl treffen kann, indem Sie die Parameter *-requestJSChildPorts* **`<niedrigster Port>`**-**`<höchster Port>`** und *-requestPort* **`<port>`** zur Befehlszeile des Servers hinzufügen. Achten Sie darauf, dass der Anschlussbereich groß genug ist, um die durch `-maxJobs` angegebene maximale Anzahl untergeordneter Prozesse zu unterstützen.
- der angegebene Anschlussbereich in der Firewall geöffnet werden.

Viele untergeordnete Prozesse kommunizieren mit der Datenschicht. Ein untergeordneter Prozess kann beispielsweise eine Verbindung zur Berichtsdatenbank herstellen, Daten extrahieren und Werte für einen Bericht berechnen. Wenn der untergeordnete Job Server-Prozess über eine Firewall mit der Datenschicht kommuniziert, muss:

- ein Kommunikationspfad in der Firewall geöffnet werden, und zwar von einem beliebigen Anschluss auf dem Job Server-Rechner zum Datenbank-Abhöranschluss auf dem Datenbankserverrechner.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Überblick über Befehlszeilen [Seite 895]

8.14.2 Kommunikation zwischen BI-Plattform-Komponenten

BI-Plattform-Komponenten wie Browserclients, Rich-Clients, Server und das auf dem Webanwendungsserver gehostete SDK kommunizieren während typischer Arbeitsabläufe über das Netzwerk miteinander. Um SAP BusinessObjects-Produkte übergreifend über mehrere, durch eine Firewall getrennte Teilnetze zu implementieren, ist es wichtig, diese Arbeitsabläufe zu verstehen.

8.14.2.1 Anforderungen für die Kommunikation zwischen BI-Plattform-Komponenten

BI-Plattform-Implementierungen müssen die folgenden allgemeinen Voraussetzungen erfüllen.

1. Jeder Server muss in der Lage sein, die Kommunikation mit jedem anderen BI-Server über den Anforderungsport des jeweiligen Servers zu initialisieren.
2. Der Central Management Server verwendet zwei Ports. Alle BI-Plattform-Server, der Rich-Client- sowie der Webanwendungsserver, der das SDK hostet, müssen in der Lage sein, die Kommunikation mit dem CMS über beide Ports zu initialisieren.
3. Jeder untergeordnete Prozess des Job Servers muss in der Lage sein, mit dem CMS zu kommunizieren.
4. Thick-Clients müssen außerdem in der Lage sein, die Kommunikation mit dem Anforderungs-Port des Input und Output File Repository Servers zu initialisieren.
5. Wenn das Auditing für Thick-Clients und Webanwendungen aktiviert ist, muss es diesen möglich sein, die Kommunikation mit den Anforderungsports der Adaptive Processing Server zu initiieren, die den Proxydienst für das Client-Auditing hostet.
6. Der Webanwendungsserver, der das SDK hostet, muss grundsätzlich in der Lage sein, mit den Anforderungsports aller BI-Server zu kommunizieren.

   Hinweis

   Der Webanwendungsserver muss nur mit den BI-Servern kommunizieren, die in der Implementierung verwendet werden. Wenn Crystal Reports beispielsweise nicht verwendet wird, muss der Webanwendungsserver nicht mit den Crystal Reports Cache Servern kommunizieren.

7. Job Server verwenden die Portnummern, die mit dem Befehl `-requestJSChildPorts <niedrigster Port>-<höchster Port>` angegeben werden. Wenn kein Bereich in der Befehlszeile angegeben wurde, verwenden die Server nach dem Zufallsprinzip ausgewählte Portnummern. Damit ein Job Server mit einem CMS-, FTP- oder Mail-Server auf einem anderen Rechner kommunizieren kann, öffnen Sie alle Ports in dem von `-requestJSChildPorts` auf Ihrer Firewall angegebenen Bereich.
8. Die Kommunikation mit dem Überwachungsport der CMS-Datenbank muss vom CMS initialisiert werden können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9. Der Connection Server, die meisten untergeordneten Job Server-Prozesse und jede Systemdatenbank und jeder Audit-Verarbeitungsserver müssen in der Lage sein, die Kommunikation mit dem Überwachungsport der Berichtsdatenbank zu initialisieren.

Weitere Informationen

Portanforderungen der BI-Plattform [Seite 187]

8.14.2.2 Portanforderungen der BI-Plattform

In diesem Abschnitt werden die Kommunikationsports aufgelistet, die von BI-Servern und -Thick-Clients, dem Webanwendungsserver, von dem das SDK gehostet wird, sowie von Drittthersteller-Softwareanwendungen verwendet werden. Wenn die BI-Plattform mit Firewalls implementiert wird, können Sie diese Informationen nutzen, um die Mindestanzahl an Ports in diesen Firewalls zu öffnen.

8.14.2.2.1 Portanforderungen für BI-Plattform-Anwendungen

In dieser Tabelle sind die von BI-Plattform-Anwendungen verwendeten Server und Portnummern aufgelistet.

Produkt	Clientanwendung	Zugeordnete Server	Serverportanforderungen
Crystal Reports	SAP Crystal Reports 2013 Designer	CMS Input FRS Output FRS Crystal Reports 2013 Report Application Server (RAS) Crystal Reports 2013 Processing Server Crystal Reports Cache Server	CMS Name Server-Port (Standard: 6400) CMS-Anforderungsport Input FRS-Anforderungsport Output-FRS-Anforderungsport Crystal Reports 2013 Report-Application-Server-Anforderungsport Crystal-Reports-2013-Processing-Server-Anforderungsport Crystal Reports Cache Server-Anforderungsport
Crystal Reports	SAP Crystal Reports für Enterprise-Designer	CMS Input FRS Output FRS Crystal Reports Processing Server	CMS Name Server-Port (Standard: 6400) CMS-Anforderungsport Input FRS-Anforderungsport Output-FRS-Anforderungsport

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Produkt	Clientanwendung	Zugeordnete Server	Serverportanforderungen
		Crystal Reports Cache Server	Crystal-Reports-Processing-Server-Anforderungsport Crystal Reports Cache Server-Anforderungsport
Dashboards	SAP BusinessObjects Dashboards	CMS Input FRS Output FRS Webdienst-Provideranwendung (`dswsbobje.war`), die die für bestimmte Datenquellenverbindungen benötigten Dashboards-, Live-Office- und QaaWS-Webdienste hostet	CMS Name Server-Port (Standard: 6400) CMS-Anforderungsport Input FRS-Anforderungsport Output-FRS-Anforderungsport HTTP-Port (Standard: 80)
Live Office	Live-Office-Client	Web Services-Provideranwendung (`dswsbobje.war`), die den Live Office-Webdienst hostet	HTTP-Port (Standard: 80)
BI-Plattform	SAP-BusinessObjects-Web-Intelligence-Rich-Client	CMS Input FRS	CMS Name Server-Port (Standard: 6400) CMS-Anforderungsport Input FRS-Anforderungsport
BI-Plattform	Universe-Design-Tool	CMS Input FRS Connection Server	CMS Name Server-Port (Standard: 6400) CMS-Anforderungsport Input FRS-Anforderungsport Connection Server-Anschluss
BI-Plattform	Business View Manager	CMS Input FRS	CMS Name Server-Port (Standard: 6400) CMS-Anforderungsport Input FRS-Anforderungsport
BI-Plattform	Central Configuration Manager (CCM)	CMS Server Intelligence Agent (SIA)	Die folgenden Ports müssen geöffnet sein, damit BI-Remoteserver von CCM verwaltet werden können: CMS Name Server-Port (Standard: 6400) CMS-Anforderungsport Die folgenden Anschlüsse müssen geöffnet sein, damit der CCM SIA-Remoteprozesse verwalten kann:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Produkt	Clientanwendung	Zugeordnete Server	Serverportanforderungen
			Microsoft Directory Services (TCP-Anschluss: 445) NetBIOS Session Service (TCP-Anschluss: 139) NetBIOS Datagram Service (UDP-Anschluss: 138) NetBIOS Name Service (UDP-Anschluss: 137) DNS (TCP-/UDP-Anschluss: 53) (Einige aufgeführte Anschlüsse sind u.U. nicht erforderlich. Wenden Sie sich an Ihren Windows-Administrator).
BI-Plattform	Server Intelligence Agent (SIA))	Jeder BI-Server, einschließlich CMS	SIA-Anforderungsport (Standard: 6410) CMS Name Server-Port (Standard: 6400) CMS-Anforderungsport
BI-Plattform	Berichtskonvertierungstool	CMS Input FRS	CMS Name Server-Port (Standard: 6400) CMS-Anforderungsport Input FRS-Anforderungsport
BI-Plattform	Repository Diagnostic Tool	CMS Input FRS Output FRS	CMS Name Server-Port (Standard: 6400) CMS-Anforderungsport Input FRS-Anforderungsport Output-FRS-Anforderungsport
BI-Plattform	Im Webanwendungsserver gehostetes SDK für die BI-Plattform	Alle von den implementierten Produkten benötigten BI-Plattform-Server. Beispiel: Die Kommunikation mit dem Crystal-Reports-2013-Processing-Server-Anforderungsport ist erforderlich, wenn das SDK Crystal-Reports-Berichte vom CMS abruft und mit diesen interagiert.	CMS Name Server-Port (Standard: 6400) CMS-Anforderungsport Anforderungsport für jeden erforderlichen Server. Beispiel: Der Crystal-Reports-2013-Processing-Server-Anforderungsport.
BI-Plattform	Web Services-Provider	Alle von den Produkte, die auf Webdienste zugreifen, benötigten BI-Server.	CMS Name Server-Port (Standard: 6400) CMS-Anforderungsport

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Produkt	Clientanwendung	Zugeordnete Server	Serverportanforderungen
	(`dswsbobje.war`)	Beispiel: Die Kommunikation mit den Anforderungsports des Dashboards Cache Servers und des Dashboards Processing Servers ist erforderlich, wenn SAP BusinessObjects Dashboards über den Webdienst-Provider auf Enterprise-Datenquellenverbindungen zugreift.	Anforderungsport für jeden erforderlichen Server. Beispiel: Anforderungsports des Dashboards Cache Servers und des Dashboards Processing Servers.
BI-Plattform	SAP BusinessObjects Analysis, Edition für OLAP	CMS Adaptive Processing Server, der den Multi-Dimensional Analysis Service hostet Input FRS Output FRS	CMS Name Server-Port (Standard: 6400) CMS-Anforderungsport Adaptive Processing Server-Anforderungsport Input FRS-Anforderungsport Output-FRS-Anforderungsport

8.14.2.2.2 Portanforderungen für Anwendungen von Drittherstellern

In dieser Tabelle sind Softwareprodukte von Drittherstellern aufgelistet, die von SAP-BusinessObjects-Produkten verwendet werden. Sie umfasst spezifische Beispiele von einigen Softwareanbietern, die verschiedenen Provider stellen jedoch auch unterschiedliche Anforderungen an die Ports.

Dritthersteller-Anwendung	SAP-BusinessObjects-Komponente, die das Dritthersteller-Produkt verwendet	Portanforderung der Dritthersteller-Anwendung	Beschreibung
CMS-Systemdatenbank	Central Management Server (CMS)	Überwachungsport des Datenbankservers	Der CMS ist der einzige Server, der mit der CMS-Systemdatenbank kommuniziert.
CMS-Audit-Datenbank	Central Management Server (CMS)	Überwachungsport des Datenbankservers	Der CMS ist der einzige Server, der mit der CMS-Audit-Datenbank kommuniziert.
Berichtsdatenbank	Connection Server Jeder untergeordnete Job Server-Prozess	Überwachungsport des Datenbankservers	Diese Server rufen Informationen von der Berichtsdatenbank ab.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Dritthersteller-Anwendung	SAP-BusinessObjects-Komponente, die das Dritthersteller-Produkt verwendet	Portanforderung der Dritthersteller-Anwendung	Beschreibung
	Jeder Processing Server		
Webanwendungsserver	Alle SAP-BusinessObjects-Webdienste und -Webanwendungen, einschließlich BI-Launchpad und die CMC	HTTP-Anschluss und HTTPS-Anschluss. Unter Tomcat lautet der HTTP-Standardport beispielsweise 8080 und der HTTPS-Standardport 443.	Der HTTPS-Anschluss ist nur bei Verwendung der sicheren HTTP-Kommunikation erforderlich.
FTP-Server	Jeder Job Server	FTP-Eingang (Anschluss 21) FTP-Ausgang (Anschluss 22)	Die Job Server verwenden die FTP-Anschlüsse, um den *Versand an FTP* zu ermöglichen.
E-Mail-Server	Jeder Job Server	SMTP (Anschluss 25)	Die Job Server verwenden den SMTP-Port, um den *E-Mail-Versand* zu ermöglichen.
Unix-Server, an die die Job Server Inhalt senden können	Jeder Job Server	rexec-Ausgang (Anschluss 512) (Nur UNIX) rsh-Ausgang (Anschluss 514)	(Nur UNIX) Die Job Server verwenden diese Ports, um den *Versand an Datenträger* zu ermöglichen.
Authentication Server	CMS™ Webanwendungsserver, der das SDK hostet Jeder Thick-Client, z.B. Live Office.	Verbindungsanschluss für Dritthersteller-Authentifizierung Der Connection Server für den Oracle LDAP-Server wird beispielsweise vom Benutzer in der Datei "ldap.ora" definiert.	Anmeldedaten von Benutzern werden auf dem Dritthersteller-Authentifizierungsserver gespeichert. Der CMS™, das SDK und die Thick-Clients, die hier aufgeführt sind, müssen mit dem Dritthersteller-Authentifizierungsserver kommunizieren, wenn sich ein Benutzer anmeldet.

8.15 Konfigurieren der BI-Plattform für Firewalls

Dieser Abschnitt enthält schrittweise Anleitungen zum Konfigurieren des BI-Plattform-Systems für die Zusammenarbeit in einer Firewallumgebung.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.15.1 Konfigurieren des Systems für Firewalls

1. Ermitteln Sie, welche BI-Plattform-Komponenten über eine Firewall hinweg kommunizieren müssen.
2. Konfigurieren Sie manuell den Anforderungs-Port für jeden BI-Plattform-Server, der über eine Firewall hinweg kommunizieren muss.
3. Konfigurieren Sie einen Portbereich für alle untergeordneten Elemente des Job Servers, die durch eine Firewall kommunizieren müssen. Fügen Sie hierzu der Befehlszeile des Servers `-requestJSChildPorts<niedrigster Port>-<höchster Port> und -requestPort <Port>` hinzu.
4. Konfigurieren Sie die Firewall für die Kommunikation mit den Anforderungs-Ports und dem Portbereich des Job Servers auf den BI-Servern, die Sie im vorherigen Schritt konfiguriert haben.
5. (Optional) Konfigurieren Sie die Datei "hosts" auf allen Rechnern, die einen BI-Plattform-Server hosten, der über eine Firewall hinweg kommunizieren muss.

Weitere Informationen

Kommunikation zwischen BI-Plattform-Komponenten [Seite 186]
Konfigurieren von Portnummern [Seite 401]
Überblick über Befehlszeilen [Seite 895]
Festlegen der Firewallregeln [Seite 192]
Konfigurieren der hosts-Datei für Firewalls, die NAT verwenden. [Seite 193]

8.15.1.1 Festlegen der Firewallregeln

Die Firewall muss konfiguriert werden, um den erforderlichen Datenverkehr zwischen BI-Plattform-Komponenten zu ermöglichen. Ausführliche Informationen dazu, wie diese Regeln festgelegt werden, finden Sie in Ihrer Firewalldokumentation.

Legen Sie für jeden Kommunikationspfad, der die Firewall passiert, eine Zugriffsregel für eingehenden Datenverkehr fest. Es ist unter Umständen nicht erforderlich, eine Zugriffsregel für jeden BI-Plattform-Server hinter der Firewall festzulegen.

Verwenden Sie die Portnummer, die Sie im Feld **Anforderungs-Port** des Servers auf der Seite "Eigenschaften" des Servers in der CMC angeben. Bedenken Sie, dass jeder Server auf einem Rechner eine eindeutige Portnummer verwenden muss. Einige SAP-Business-Objects-Server verwenden mehrere Ports.

> **Hinweis**
>
> Wenn die BI-Plattform über Firewalls hinweg implementiert wird, die NAT verwenden, benötigt jeder Server auf allen Rechnern eine eindeutige Nummer für den Anforderungs-Port. Dies bedeutet, dass in der gesamten Implementierung kein Server über denselben Anforderungs-Port wie ein anderer Server verfügen darf.

> **Hinweis**
>
> Zugriffsregeln für den ausgehenden Datenverkehr müssen nicht festgelegt werden. BI-Plattform-Server initialisieren keine Kommunikation mit dem Webanwendungsserver oder mit Clientanwendungen. BI-

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Plattform-Server können die Kommunikation mit anderen Plattform-Servern im selben Cluster initiieren. Implementierungen mit geclusterten Servern in einer ausgehenden Firewall-Umgebung werden nicht unterstützt.

Beispiel

Dieses Beispiel veranschaulicht die Zugriffsregeln für den eingehenden Datenverkehr einer Firewall zwischen dem Webanwendungsserver und den BI-Plattform-Servern. In diesem Fall öffnen Sie zwei Ports für den CMS, einen Port für den Input File Repository Server (FRS) und einen Port für den Output FRS. Die Nummern der Anforderungsports entsprechen den Portnummern, die Sie im Feld **Anforderungs-Port** auf der CMC-Konfigurationsseite für einen Server angeben.

Quellcomputer	Port	Zielcomputer	Port	Aktion
Webanwendungsserver	Beliebig	CMS	6400	Zulassen
Webanwendungsserver	Beliebig	CMS	<Nummer des Anforderungs-Ports>	Zulassen
Webanwendungsserver	Beliebig	Input FRS	<Nummer des Anforderungs-Ports>	Zulassen
Webanwendungsserver	Beliebig	Output FRS	<Nummer des Anforderungs-Ports>	Zulassen
Beliebig	Beliebig	CMS	Beliebig	Zurückweisen
Beliebig	Beliebig	Andere Plattform-Server	Beliebig	Zurückweisen

Weitere Informationen

Kommunikation zwischen BI-Plattform-Komponenten [Seite 186]

8.15.1.2 Konfigurieren der hosts-Datei für Firewalls, die NAT verwenden.

Dieser Schritt ist nur erforderlich, wenn die BI-Plattform-Server über eine Firewall kommunizieren müssen, für die Netzwerkadressumsetzung (Network Address Translation, NAT) aktiviert ist. In diesem Schritt können Clientrechner eine Zuordnung zwischen dem Hostnamen eines Servers und einer routbaren IP-Adresse vornehmen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Die BI-Plattform kann auf Rechnern implementiert werden, die das Domain Name System (DNS) verwenden. In diesem Fall können die Hostnamen des Serverrechners der extern routbaren IP-Adresse auf dem DNS-Server anstatt der `hosts`-Datei jedes Rechners zugeordnet werden.

Netzwerkadressumsetzung (Network Address Translation, NAT)

Eine Firewall wird eingesetzt, um das interne Netzwerk vor nicht autorisiertem Zugriff zu schützen. Firewalls, die *NAT* nutzen, ordnen die IP-Adressen des internen Netzwerks einer anderen Adresse zu, die vom externen Netzwerk genutzt wird. Durch diese *Adressumsetzung* wird die Sicherheit verbessert, indem interne IP-Adressen vor dem externen Netzwerk verborgen werden.

BI-Plattform-Komponenten wie Server, Thick-Clients und Webanwendungsserver, die das BI-Plattform-SDK hosten, verwenden für die Kontaktaufnahme mit einem Server eine Dienstreferenz. Die Dienstreferenz enthält den Hostnamen des Serverrechners. Dieser Hostname muss vom Rechner der BI-Plattform-Komponente geroutet werden können. Das bedeutet, dass die `hosts`-Datei auf dem Rechner der Komponente den Hostnamen zur externen IP-Adresse des Serverrechners zuordnen muss. Die externe IP-Adresse des Serverrechners kann von der externen Seite der Firewall aus geroutet werden, während dies für die interne IP-Adresse nicht zutrifft.

Die Schritte zur Konfiguration der Datei `hosts` weichen in Windows und UNIX voneinander ab.

8.15.1.2.1 Konfigurieren der Datei hosts unter Windows

1. Suchen Sie alle Rechner, auf denen eine BI-Plattform-Komponente ausgeführt wird, die durch eine Firewall kommunizieren muss, für die die *Netzwerkadressumsetzung* (*NAT*) aktiviert wurde.
2. Öffnen Sie auf jedem Rechner aus dem vorangehenden Schritt die `hosts`-Datei mit einem Texteditor wie dem Editor. Die Datei `hosts` befindet sich unter `\Windows\System32\drivers\etc\hosts`.
3. Befolgen Sie die Anweisungen in der Datei `hosts`, um Einträge für die einzelnen Rechner hinter der Firewall hinzuzufügen, auf denen ein oder mehrere BI-Plattform-Server ausgeführt werden. Ordnen Sie den Hostnamen oder vollständig qualifizierten Domänennamen des Serverrechners der externen IP-Adresse zu.
4. Speichern Sie die Datei `hosts`.

8.15.1.2.2 Konfigurieren der Datei "hosts" unter UNIX

> **Hinweis**
>
> Das UNIX-Betriebssystem muss so konfiguriert werden, dass zuerst in der *hosts*-Datei und erst dann auf dem DNS nachgesehen wird, um Domänennamen aufzulösen. Weitere Informationen finden Sie in der Dokumentation zum UNIX-System.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Suchen Sie alle Rechner, auf denen eine BI-Plattform-Komponente ausgeführt wird, die durch eine Firewall kommunizieren muss, für die die *Netzwerkadressumsetzung* (*NAT*) aktiviert wurde.
2. Öffnen Sie die Datei *hosts* in einem Editor wie `vi`. Die Datei `hosts` befindet sich im Verzeichnis `\etc`.
3. Befolgen Sie die Anweisungen in der Datei `hosts`, um Einträge für die einzelnen Rechner hinter der Firewall hinzuzufügen, auf denen ein oder mehrere BI-Plattform-Server ausgeführt werden. Ordnen Sie den Hostnamen oder vollständig qualifizierten Domänennamen des Serverrechners der externen IP-Adresse zu.
4. Speichern Sie die Datei `hosts`.

8.15.2 Debuggen einer Firewall-Implementierung

Falls ein oder mehrere BI-Plattform-Server nicht funktionieren, wenn die Firewall aktiviert ist, obwohl die erforderlichen Ports auf der Firewall geöffnet sind, können Sie anhand der Ereignisprotokolle ermitteln, welcher Server welche Ports oder IP-Adressen überwacht. Sie können diese Ports dann entweder auf Ihrer Firewall öffnen oder die Portnummern oder IP-Adressen, die diese Server versuchen zu überwachen, über die Central Management Console (CMC) ändern.

Beim Start eines BI-Plattform-Servers schreibt dieser folgende Informationen für jeden Anforderungs-Port, an den er sich binden möchte, in das Ereignisprotokoll.

- *Server*: Der Name des Servers und ob dieser erfolgreich gestartet wurde.
- *Veröffentlichte Adressen*: Eine Liste der IP-Adressen und Portkombinationen, die an den Namensdienst gesendet werden, der von anderen Servern für die Kommunikation mit diesem Server genutzt wird.

Wenn ein Server erfolgreich eine Bindung an einen Port herstellt, zeigt die Protokolldatei auch die *Verfügbaren Ports*, die IP-Adressen und den Portnummer an, die vom Server verwendet wird. Wenn der Server keine Bindung an den Port herstellen kann, zeigt die Protokolldatei die Meldung *Abhören von Port(s) fehlgeschlagen* sowie die IP-Adresse und den Port an, den der Server versucht hat abzuhören.

Beim Starten eines Central Management Servers, schreibt er außerdem Informationen zu "Veröffentlichte Adressen", "Verfügbare Ports" und "Nicht verfügbare Ports" für den Namensdienst-Port des Servers.

Hinweis

Wenn ein Server für die Verwendung eines automatisch zugeordneten Ports und eines ungültigen Hostnamens oder einer ungültigen IP-Adresse konfiguriert wurde, zeigt das Ereignisprotokoll an, dass das Abhören des Hostnamens oder der IP-Adresse und des Ports “0” fehlgeschlagen ist. Wenn ein angegebener Hostname oder eine IP-Adresse ungültig ist, schlägt der Server fehl, bevor das Hostbetriebssystem einen Port zuweisen kann.

Beispiel

Das folgende Beispiel zeigt einen Eintrag für einen Central Management Server, der erfolgreich zwei Anforderungs-Ports und einen Namensdienstport abhört.

```
Server mynode.cms1 successfully started.
Request Port :
     Published Address(es): mymachine.corp.com:11032, mymachine.corp.com:8765
     Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:11032,
10.90.172.216:8765
Name Service Port :
     Published Address(es): mymachine.corp.com:6400
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
     Listening on port(s):  [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:6400,
10.90.172.216:6400
```

8.15.2.1 Debuggen einer Firewall-Implementierung

1. Lesen Sie das Ereignisprotokoll, um festzustellen, ob die Bindung des Servers an den von Ihnen angegebenen Port erfolgreich war.

   Konnte der Server nicht erfolgreich an einen Port gebunden werden, besteht wahrscheinlich ein Portkonflikt zwischen dem Server und einem anderen Prozess, der auf dem Rechner ausgeführt wird. Der Eintrag in *Abhören von Port(s) fehlgeschlagen:* gibt den Port an, den der Server abzuhören versucht. Führen Sie ein Dienstprogramm z.B. netstat aus, um herauszufinden, welcher Prozess den Port belegt hat, und konfigurieren Sie dann den anderen Prozess oder den Server so, dass er einen anderen Port abhört.
2. Wurde der Server erfolgreich an einen Port gebunden, gibt das Feld *Abhören von Port(s):* an, welchen Port der Server abhört. Wenn der Server einen Port abhört und trotzdem nicht ordnungsgemäß arbeitet, müssen Sie entweder sicherstellen, dass der Port in der Firewall geöffnet ist, oder den Server so konfigurieren, dass er einen geöffneten Port abhört.

Wenn alle Central Management Server in der Implementierung versuchen, Ports oder IP-Adressen abzuhören, die nicht verfügbar sind, dann werden die CMS nicht gestartet, und Sie können sich nicht bei der CMC anmelden. Wenn Sie die Portnummer oder IP-Adresse, die der CMS abzuhören versucht, ändern möchten, müssen Sie über den Central Configuration Manager (CCM) eine gültige Portnummer oder IP-Adresse eingeben.

Weitere Informationen

Konfigurieren von Portnummern [Seite 401]

8.16 Beispiele für typische Firewallszenarios

Dieser Abschnitt enthält Beispiele mit typischen Szenarien für die Firewallimplementierung.

8.16.1 Beispiel: Implementierung der Anwendungsschicht in einem getrennten Netzwerk

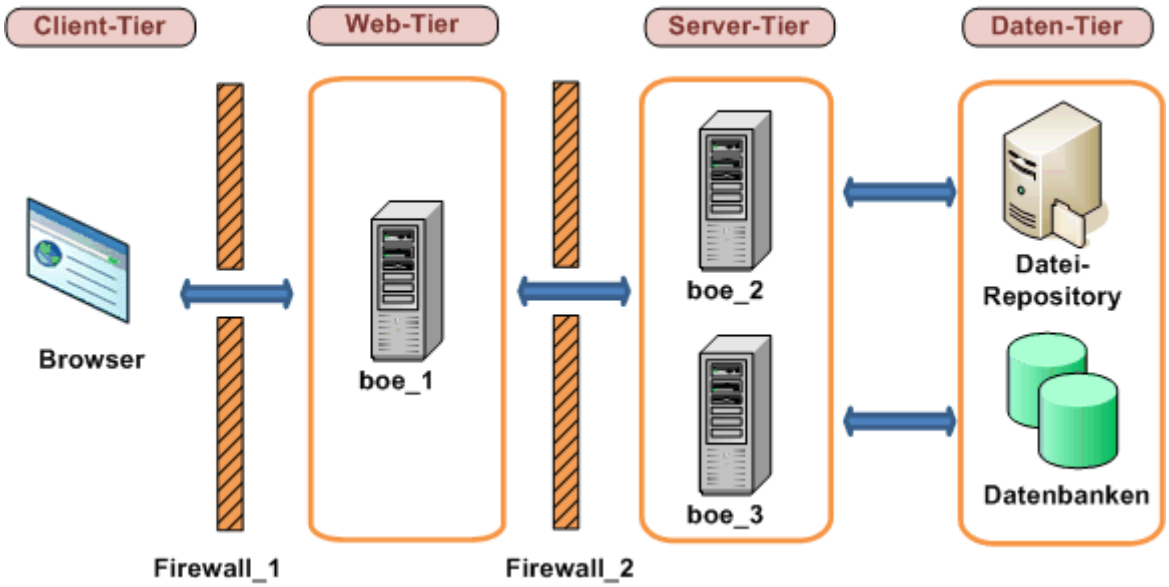
Dieses Beispiel veranschaulicht, wie eine Firewall und die BI-Plattform für die Zusammenarbeit in einer Implementierung konfiguriert werden, in der der Webanwendungsserver durch die Firewall von anderen BI-Plattform-Servern getrennt wird.

In diesem Beispiel werden die BI-Plattform-Komponenten auf folgenden Rechnern implementiert:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Rechner `boe_1` hostet den Webanwendungsserver und das SDK.
- Rechner `boe_2` hostet die Server der Verwaltungsschicht, einschließlich Central Management Server, Input File Repository Server, Output File Repository Server und Event Server.
- Rechner `boe_3` hostet die Server der Verarbeitungsschicht, darunter den Adaptive Job Server, Web-Intelligence-Verarbeitungsserver, Report Application Server, Crystal Reports Cache Server und Crystal Reports Processing Server.

Abbildung 10: Implementierung der Anwendungsschicht in einem getrennten Netzwerk



8.16.1.1 Konfigurieren einer im getrennten Netzwerk implementierten Anwendungsschicht

In den folgenden Schritten wird die Konfiguration dieses Beispiels erläutert.

1. Für dieses Beispiel gelten folgende Kommunikationsvoraussetzungen:
   - Der Webanwendungsserver, der das SDK hostet, muss in der Lage sein, mit dem CMS über beide Ports zu kommunizieren.
   - Der Webanwendungsserver, der das SDK hostet, muss in der Lage sein, mit allen BI-Plattform-Servern zu kommunizieren.
   - Der Browser muss Zugriff auf den HTTP- oder HTTPS-Anforderungs-Port des Webanwendungsservers haben.
2. Der Webanwendungsserver muss mit allen BI-Plattform-Servern auf Rechner `boe_2` und `boe_3` kommunizieren. Konfigurieren Sie die Portnummern für jeden Server auf diesen Rechnern. Sie können beliebige freie Ports von 1.025 bis 65.535 verwenden.
   Die für dieses Beispiel ausgewählten Portnummern sind in der Tabelle aufgelistet:

Server	Portnummer
Central Management Server	6400

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Server	Portnummer
Central Management Server	6411
Input File Repository Server	6415
Output File Repository Server	6420
Event Server	6425
Adaptive Job Server	6435
Crystal Reports Cache Server	6440
Web Intelligence Processing Server	6460
Report Application Server	6465
Crystal Reports Processing Server	6470

3. Konfigurieren Sie die Firewalls `Firewall_1` und `Firewall_2`, um die Kommunikation mit den festen Ports der Server und des Webanwendungsservers zu ermöglichen, der im vorherigen Schritt konfiguriert wurde.

   In diesem Beispiel wird der HTTP-Port für den Tomcat-Anwendungsserver geöffnet.

   Tabelle 9: Konfiguration für Firewall_1

Port	Zielcomputer	Port	Aktion
Beliebig	boe_1	8080	Zulassen

   Tabelle 10: Konfiguration für Firewall_2

Quellcomputer	Port	Zielcomputer	Port	Aktion
boe_1	Beliebig	boe_2	6400	Zulassen
boe_1	Beliebig	boe_2	6411	Zulassen
boe_1	Beliebig	boe_2	6415	Zulassen
boe_1	Beliebig	boe_2	6420	Zulassen
boe_1	Beliebig	boe_2	6425	Zulassen
boe_1	Beliebig	boe_3	6435	Zulassen
boe_1	Beliebig	boe_3	6440	Zulassen
boe_1	Beliebig	boe_3	6460	Zulassen
boe_1	Beliebig	boe_3	6465	Zulassen
boe_1	Beliebig	boe_3	6470	Zulassen

4. Da diese Firewall nicht NAT-fähig ist, muss die Datei `hosts` nicht konfiguriert werden.

Weitere Informationen

Konfigurieren von Portnummern [Seite 401]
Erläuterung der Kommunikation zwischen BI-Plattform-Komponenten [Seite 183]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.16.2 Beispiel: Trennung von Thick-Client und Datenbankschicht von BI-Plattform-Servern durch eine Firewall

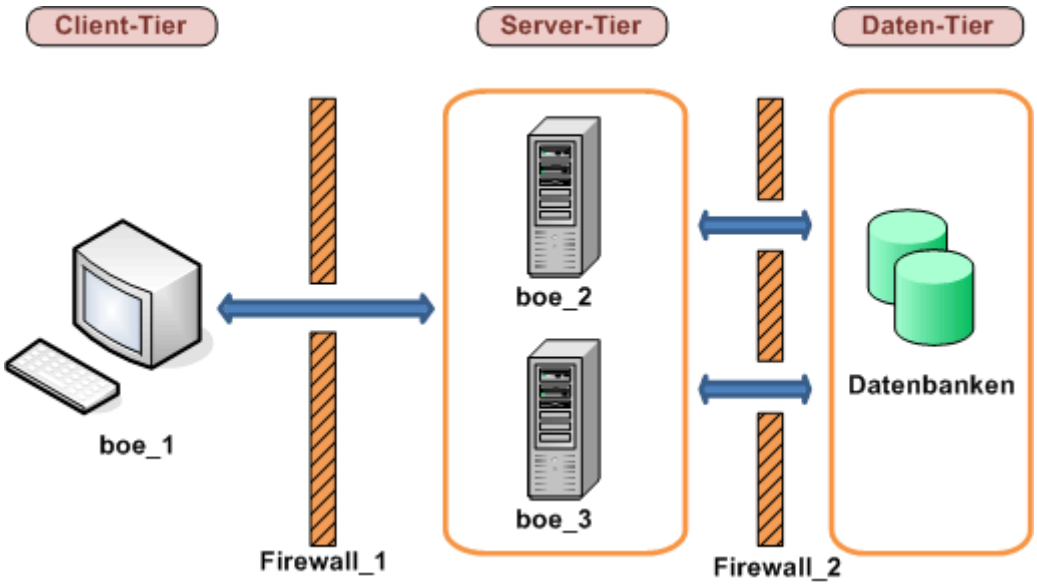
Dieses Beispiel veranschaulicht die Konfiguration einer Firewall und der BI-Plattform für die Zusammenarbeit in einem Implementierungsszenario mit folgenden Voraussetzungen:

- Eine Firewall trennt einen Thick Client von den BI-Plattform-Servern.
- Eine Firewall trennt die BI-Plattform-Server von der Datenbankschicht.

In diesem Beispiel werden die BI-Plattform-Komponenten auf folgenden Rechnern implementiert:

- Rechner `boe_1` hostet den Publishing-Assistenten. Der Publishing-Assistent ist ein BI-Plattform-Thick-Client.
- Rechner `boe_2` hostet die Server der Intelligence-Schicht, einschließlich Central Management Server (CMS), Input File Repository Server, Output File Repository Server und Event Server.
- Rechner `boe_3` hostet die Server der Verarbeitungsschicht, darunter den Adaptive Job Server, den Web-Intelligence-Verarbeitungsserver, den Report Application Server, den Crystal Reports Processing Server und den Crystal Reports Cache Server.
- Der `Datenbankrechner` hostet die CMS-Systemdatenbank und -Audit-Datenbank und die Berichtsdatenbank. Beachten Sie, dass beide Datenbanken auf demselben Datenbankserver oder jede Datenbank auf einem eigenen Datenbankserver implementiert werden kann. In diesem Beispiel werden alle CMS-Datenbanken und die Berichtsdatenbank auf demselben Datenbankserver implementiert.

Abbildung 11: Implementierung von Rich-Client und Datenbankschicht in getrennten Netzwerken



8.16.2.1 Konfigurieren von durch eine Firewall von BI-Plattform-Servern getrennten Schichten

In den folgenden Schritten wird die Konfiguration dieses Beispiels erläutert.

1. Für dieses Beispiel gelten die folgenden Kommunikationsvoraussetzungen:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Der Publishing-Assistent muss in der Lage sein, die Kommunikation mit dem CMS™ über beide CMS-Ports zu initialisieren.
- Der Publishing-Assistent muss in der Lage sein, die Kommunikation mit dem Input File Repository Server und dem Output File Repository Server zu initialisieren.
- Connection Server, jeder untergeordnete Job Server-Prozess und alle Processing Server benötigen Zugriff auf den Abhöranschluss auf dem Berichtsdatenbankserver.
- Der CMS™ erfordert Zugriff auf den Datenbank-Abhöranschluss auf dem CMS™-Datenbankserver.

2. Konfigurieren Sie einen bestimmten Port für den CMS™, Input FRS und Output FRS. Sie können beliebige freie Ports von 1.025 bis 65.535 verwenden.
   Die für dieses Beispiel ausgewählten Portnummern sind in der Tabelle aufgelistet:

Server	Portnummer
Central Management Server™	6411
Input File Repository Server	6415
Output File Repository Server	6416

3. Es muss kein Anschlussbereich für die untergeordneten Job Server-Prozesse konfiguriert werden, da die Firewall zwischen den Job Servern und Datenbankservern so konfiguriert wird, dass die Kommunikation über einen beliebigen Port initialisiert werden kann.
4. Konfigurieren Sie **`<Firewall_1>`** für die Kommunikation mit den festen Ports auf den Plattform-Servern, die Sie im vorherigen Schritt konfiguriert haben. Beachten Sie, dass Port 6400 der Standardport für den CMS™ Name Server-Port ist und im vorherigen Schritt nicht explizit konfiguriert werden musste.

Port	Zielcomputer	Port	Aktion
Beliebig	boe_2	6400	Zulassen
Beliebig	boe_2	6411	Zulassen
Beliebig	boe_2	6415	Zulassen
Beliebig	boe_2	6416	Zulassen

   Konfigurieren Sie **`<Firewall_2>`** für die Kommunikation mit dem Datenbankserver-Abhöranschluss. Der CMS™ (auf *boe_2*) muss Zugriff auf die CMS™-Systemdatenbank und -Audit-Datenbank haben, und die Job Server (auf *boe_3*) benötigen Zugriff auf die Systemdatenbank und die Audit-Datenbank. Beachten Sie, dass kein Anschlussbereich für untergeordnete Job Server-Prozesse konfiguriert werden musste, da für die Kommunikation mit dem CMS keine Firewall passiert werden musste.

Quellcomputer	Port	Zielcomputer	Port	Aktion
boe_2	Beliebig	Databases	3306	Zulassen
boe_3	Beliebig	Databases	3306	Zulassen

5. Da diese Firewall nicht NAT-fähig ist, muss die Datei `hosts` nicht konfiguriert werden.

Weitere Informationen

Erläuterung der Kommunikation zwischen BI-Plattform-Komponenten [Seite 183]
Konfigurieren der BI-Plattform für Firewalls [Seite 191]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.17 Firewall-Einstellungen für integrierte Umgebungen

Im folgenden Abschnitt werden spezifische Überlegungen und Porteinstellungen für BI-Plattform-Implementierungen erläutert, die in die folgenden ERP-Umgebungen integriert werden.

- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Zu den BI-Plattform-Komponenten gehören beispielsweise Browserclients, Rich-Clients, Server und das auf dem Webanwendungsserver gehostete SDK. Systemkomponenten können auf mehreren Rechnern installiert werden. Bevor Sie das System für die Arbeit mit Firewalls konfigurieren, sollten Sie sich Grundkenntnisse der Kommunikation mit der BI-Plattform und den ERP-Komponenten aneignen.

Portanforderungen für die BI-Server

Die folgenden Ports werden für die entsprechenden Server in der BI-Plattform benötigt:

Server-Portanforderungen
• Name Server-Port des Central Management Servers • Anforderungs-Port des Central Management Servers • Input FRS-Anforderungs-Port • Output FRS-Anforderungs-Port • Anforderungs-Port des Report Application Servers • Anforderungs-Port des Crystal Reports Cache Servers • Anforderungs-Port des Crystal Reports Page Servers • Anforderungs-Port des Crystal Reports Processing Servers

8.17.1 Spezifische Firewall-Richtlinien für die SAP-Integration

In Ihrer BI-Plattformumgebung müssen folgende Kommunikationsregeln eingehalten werden:

- Der CMS muss in der Lage sein, die Kommunikation mit einem SAP-System über den Port für das SAP-System-Gateway zu initiieren.
- Der Adaptive Job Server und der Crystal Reports Processing Server müssen (wie auch die Datenzugriffskomponenten) in der Lage sein, die Kommunikation mit einem SAP-System auf dem Port für das SAP-System-Gateway zu initiieren.
- Die BW Publisher-Komponente muss in der Lage sein, die Kommunikation mit einem SAP-System auf dem Port für das SAP-System-Gateway zu initiieren.
- BI-Plattform-Komponenten, die auf dem SAP Enterprise Portal implementiert sind (z.B. iViews und KMC), müssen in der Lage sein, die Kommunikation mit BI-Plattform-Webanwendungen über HTTP/HTTPS-Ports zu initiieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Der Webanwendungsserver muss in der Lage sein, die Kommunikation über den SAP-System-Gateway-Dienst zu initiieren.
- Crystal Reports muss in der Lage sein, die Kommunikation mit dem SAP-Host auf dem Port für das SAP-System-Gateway und dem Port für den SAP-System-Dispatcher zu initiieren.

Der Port, den der SAP-Gateway-Dienst abhört, entspricht dem bei der Installation angegebenen Port.

> **Hinweis**
>
> Wenn für die Verbindungsherstellung zwischen einer Komponente und einem SAP-System ein SAP-Router erforderlich ist, können Sie die Komponente mithilfe der SAP-Router-Zeichenfolge konfigurieren. Beispiel: Wenn Sie ein SAP-Berechtigungssystem für den Import von Rollen und Benutzern konfigurieren, kann die SAP-Router-Zeichenfolge durch den Namen des Anwendungsservers ersetzt werden. Dadurch wird sichergestellt, dass der CMS über den SAP-Router mit dem SAP-System kommuniziert.

Weitere Informationen

Installieren eines lokalen SAP-Gateways [Seite 808]

8.17.1.1 Detaillierte Portanforderungen

Portanforderungen für SAP

Die BI-Plattform kommuniziert über den SAP Java Connector (SAP JCO) mit SAP NetWeaver (ABAP). Sie müssen die Verfügbarkeit der folgenden Ports konfigurieren und sicherstellen:

- Abhörport des SAP Gateway-Dienstes (z.B. 3300).
- Abhörport des SAP Dispatcher-Dienstes (z.B. 3200).

In der folgenden Tabelle sind die einzelnen erforderlichen Port-Konfigurationen zusammengefasst.

Quellrechner	Port	Zielrechner	Port	Aktion
SAP	Beliebig	BI-Plattform-Webanwendungsserver	HTTP/HTTPS-Port des Webdienstes	Zulassen
SAP	Beliebig	CMS	Name Server-Port des CMS	Zulassen
SAP	Beliebig	CMS	CMS-Anforderungs-Port	Zulassen
Webanwendungsserver	Beliebig	SAP	Port des SAP-System-Gateway-Dienstes	Zulassen
Central Management Server (CMS)	Beliebig	SAP	Port des SAP-System-Gateway-Dienstes	Zulassen

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Quellrechner	Port	Zielrechner	Port	Aktion
Crystal Reports™	Beliebig	SAP	Port des SAP-System-Gateway-Dienstes und Port des SAP-System-Dispatchers	Zulassen

8.17.2 Firewall-Konfiguration für die JD Edwards EnterpriseOne-Integration

Implementierungen der BI-Plattform, die mit JD-Edwards-Software kommunizieren, müssen den folgenden allgemeinen Kommunikationsregeln entsprechen:

- Die Webanwendungen der Central Management Console müssen in der Lage sein, die Kommunikation mit JD Edwards EnterpriseOne über den JDENET-Port und einen beliebig wählbaren Port zu initiieren.
- Crystal Reports mit Client-seitiger Datenkonnektivität muss in der Lage sein, die Kommunikation mit JD Edwards EnterpriseOne über den JDNET-Port zu initiieren. Zum Abrufen der Daten muss JD Edwards EnterpriseOne in der Lage sein, über einen beliebigen Port, der nicht kontrolliert werden kann, mit dem Treiber zu kommunizieren.
- Der Central Management Server muss in der Lage sein, die Kommunikation mit JD Edwards EnterpriseOne über den JDENET-Port und einen beliebig wählbaren Port zu initiieren.
- Die Nummer des JDENET-Ports finden Sie in der Konfigurationsdatei für den JD Edwards EntepriseOne-Anwendungsserver (`JDE.INI`) unter "JDNET".

Portanforderungen für die BI-Server

Produkt	Serverportanforderungen
SAP BusinessObjects Business Intelligence	• Port für BI-Plattform-Anmeldeserver

Portanforderungen für JD Edwards EnterpriseOne

Produkt	Portanforderung	Beschreibung
JD Edwards EnterpriseOne	JDENET-Port und ein beliebig gewählter Port	Wird für die Kommunikation zwischen der BI-Plattform und dem JD-Edwards-EntepriseOne-Anwendungsserver verwendet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Konfigurieren des Webanwendungsservers für die Kommunikation mit JD Edwards

In diesem Abschnitt wird veranschaulicht, wie eine Firewall und die BI-Plattform für die Zusammenarbeit in einer Implementierung konfiguriert werden, in der der Webanwendungsserver durch die Firewall von anderen Plattformservern getrennt wird.

Informationen zur Firewall-Konfiguration mit BI-Servern und -Clients finden Sie im Abschnitt *Portanforderungen für die BI-Server* in diesem Handbuch. Für die Kommunikation mit JD Edwards-Servern müssen neben der standardmäßigen Firewall-Konfiguration einige zusätzliche Ports geöffnet werden.

Tabelle 11: Für JD Edwards EnterpriseOne Enterprise

Quellcomputer	Port	Zielcomputer	Port	Aktion
CMS mit Sicherheitskonnektivitätsfunktion für JD Edwards EnterpriseOne	Beliebig	JD Edwards EnterpriseOne	Beliebig	Zulassen
BI-Server mit Datenkonnektivität für JD Edwards EnterpriseOne	Beliebig	JD Edwards EnterpriseOne	Beliebig	Zulassen
Crystal Reports mit clientseitiger Datenkonnektivität für JD Edwards EnterpriseOne	Beliebig	JD Edwards EnterpriseOne	Beliebig	Zulassen
Webanwendungsserver	Beliebig	JD Edwards EnterpriseOne	Beliebig	Zulassen

8.17.3 Spezifische Firewallrichtlinien für Oracle EBS

Ihre Implementierung der BI-Plattform muss zulassen, dass die folgenden Komponenten die Kommunikation mit dem Überwachungsport der Oracle-Datenbank initiieren:

- BI-Plattform-Webkomponenten
- CMS (speziell das Oracle EBS-Sicherheitsplugin)
- BI-Plattform-Backendserver (speziell die EBS Data Access-Komponente)
- Crystal Reports (speziell die EBS Data Access-Komponente)

> **Hinweis**
>
> Der Standardwert für den Überwachungsport der Oracle-Datenbank lautet in allen vorangehenden Fällen "1521".

8.17.3.1 Detaillierte Portanforderungen

Neben der Standard-Firewallkonfiguration für die BI-Plattform müssen weitere Ports für die Arbeit in einer integrierten Oracle EBS-Umgebung geöffnet werden:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Quellcomputer	Port	Zielcomputer	Port	Aktion
Webanwendungsserver	Beliebig	Oracle EBS	Oracle-Datenbank-port	Zulassen
CMS mit Sicherheitskonnektivität für Oracle EBS	Beliebig	Oracle EBS	Oracle-Datenbank-port	Zulassen
BI-Server mit serverseitiger Datenkonnektivität für Oracle EBS	Beliebig	Oracle EBS	Oracle-Datenbank-port	Zulassen
Crystal-Reports-Berichte mit serverseitiger Datenkonnektivität für Oracle EBS	Beliebig	Oracle EBS	Oracle-Datenbank-port	Zulassen

8.17.4 Firewall-Konfiguration für PeopleSoft Enterprise-Integration

Implementierungen der BI-Plattform, die mit PeopleSoft Enterprise kommunizieren, müssen den folgenden allgemeinen Kommunikationsregeln entsprechen:

- Der Central Management Server (CMS) mit der Komponente für die Sicherheitskonnektivität muss in der Lage sein, die Kommunikation mit dem PeopleSoft QAS-Webdienst zu initiieren.
- BI-Server mit der Komponente für die Datenkonnektivität müssen in der Lage sein, die Kommunikation mit dem PeopleSoft QAS-Webdienst zu initiieren.
- Crystal Reports mit der clientseitigen Komponente für die Datenkonnektivität muss in der Lage sein, die Kommunikation mit dem PeopleSoft QAS-Webdienst zu initiieren.
- Enterprise Management (EPM) Bridge muss in der Lage sein, mit dem CMS und dem Input File Repository Server zu kommunizieren.
- Die EPM Bridge muss in der Lage sein, über eine ODBC-Verbindung mit der PeopleSoft-Datenbank zu kommunizieren.

Die Webdienst-Portnummer entspricht dem im PeopleSoft Enterprise-Domänennamen angegebenen Port.

Portanforderungen für BI-Plattform-Server

Produkt	Server-Portanforderungen
SAP BI	• Port für BI-Plattform-Anmeldeserver

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Portanforderungen für PeopleSoft

Produkt	Portanforderung	Beschreibung
PeopleSoft Enterprise: People Tools 8.46 oder höher	HTTP/HTTPS-Port des Webdienstes	Dieser Port ist bei der Verwendung der SOAP-Verbindung für PeopleSoft Enterprise für People Tools 8.46 und neuere Lösungen erforderlich

Konfigurieren der BI-Plattform und PeopleSoft für Firewalls

In diesem Abschnitt wird veranschaulicht, wie die BI-Plattform und PeopleSoft Enterprise für die Zusammenarbeit in einer Implementierung konfiguriert werden, in der der Webanwendungsserver durch die Firewall von anderen BI-Plattform-Server getrennt wird.

Weitere Informationen zur Firewall-Konfiguration bei BI-Plattform-Servern und -Clients finden Sie im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.

Neben der Firewall-Konfiguration mit der BI-Plattform müssen weitere Konfigurationen durchgeführt werden.

Tabelle 12: Für PeopleSoft Enterprise: PeopleTools 8.46 oder höher

Quellcomputer	Port	Zielcomputer	Port	Aktion
CMS mit der Funktion "Sicherheitskonnektivität" für PeopleSoft	Beliebig	PeopleSoft	HTTP-/HTTPS-Port für PeopleSoft-Webdienst	Zulassen
BI-Server mit Datenkonnektivität für PeopleSoft	Beliebig	PeopleSoft	HTTP-/HTTPS-Port für PeopleSoft-Webdienst	Zulassen
Crystal Reports mit clientseitiger Datenkonnektivität für PeopleSoft	Beliebig	PeopleSoft	HTTP-/HTTPS-Port für PeopleSoft-Webdienst	Zulassen
EPM-Brücke	Beliebig	CMS	CMS Name Server-Port	Zulassen
EPM-Brücke	Beliebig	CMS	CMS-Anforderungs-Port	Zulassen
EPM-Brücke	Beliebig	Input File Repository Server	Input-FRS-Port	Zulassen
EPM-Brücke	Beliebig	PeopleSoft	PeopleSoft-Datenbank-Port	Zulassen

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.17.5 Firewall-Konfiguration für die Siebel-Integration

In diesem Abschnitt werden die spezifischen Ports beschrieben, die für die Kommunikation zwischen der BI-Plattform und Siebel eBusiness-Anwendungssystemen erforderlich sind, wenn diese durch Firewalls voneinander getrennt sind.

- Die Webanwendung muss in der Lage sein, die Kommunikation mit dem BI-Plattform-Anmeldeserver für Siebel zu initiieren. Für den Enterprise-Anmeldeserver für Siebel werden drei Ports benötigt:
  1. Der Echo-Port 7 (TCP) zum Überprüfen des Zugriffs auf den Anmeldeserver.
  2. Der Port für BI-Plattform-Anmeldeserver für Siebel (Standardeinstellung: 8448) für CORBA IOR-Abhörport.
  3. Ein beliebiger POA-Port für die CORBA-Kommunikation, der nicht kontrolliert werden kann. Es müssen daher alle Ports geöffnet werden.
- Der CMS muss in der Lage sein, die Kommunikation mit dem BI-Plattform-Anmeldeserver für Siebel zu initiieren. CORBA IOR-Abhörport ist für jeden Anmeldeserver konfiguriert (zum Beispiel 8448). Sie müssen außerdem eine beliebige POA-Portnummer öffnen, die unbekannt bleibt, bis Sie die BI-Plattform installiert haben.
- Der BI-Plattform-Anmeldeserver für Siebel muss in der Lage sein, die Kommunikation mit dem SCBroker-Port (Siebel-Verbindungsbroker) (z.B. 2321) einzuleiten
- Die BI-Plattform-Backend-Server (Siebel-Datenzugriffskomponente) müssen in der Lage sein, die Kommunikation mit dem SCBroker-Port (Siebel-Verbindungsbroker) (z.B. 2321) einzuleiten.
- Crystal Reports (Siebel-Datenzugriffskomponente) muss in der Lage sein, die Kommunikation mit dem SCBroker-Port (Siebel-Verbindungsbroker) (z.B. 2321) einzuleiten.

Detaillierte Beschreibung der Ports

In diesem Abschnitt werden die von der BI-Plattform verwendeten Ports aufgeführt. Wenn die BI-Plattform mit Firewalls implementiert wird, können Sie diese Informationen nutzen, um die Mindestanzahl an Ports in den Firewalls zu öffnen, die für die Integration mit Siebel erforderlich sind.

Tabelle 13: Portanforderungen für BI-Plattform-Server

Produkt	Server-Portanforderungen
SAP BI	• Port für BI-Plattform-Anmeldeserver

Tabelle 14: Portanforderung für Siebel

Produkt	Portanforderung	Beschreibung
Siebel eBusiness-Anwendung	2321	SCBroker-Standardport (Siebel-Verbindungsbroker)

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Konfigurieren der BI-Plattform-Firewalls für die Integration mit Siebel

In diesem Abschnitt wird erläutert, wie eine Firewall für Siebel und die BI-Plattform für die Zusammenarbeit in einem Implementierungsszenario konfiguriert wird, in dem der Webanwendungsserver durch die Firewall von anderen Plattformservern getrennt wird.

Quellcomputer	Port	Zielcomputer	Port	Aktion
Webanwendungsserver	Beliebig	BI-Plattform-Anmeldeserver für Siebel	Beliebig	Zulassen
CMS	Beliebig	BI-Plattform-Anmeldeserver für Siebel	Beliebig	Zulassen
BI-Plattform-Anmeldeserver für Siebel	Beliebig	Siebel	SCBroker-Port	Zulassen
BI-Server mit serverseitiger Datenkonnektivität für Siebel	Beliebig	Siebel	SCBroker-Port	Zulassen
Crystal Reports mit clientseitiger Datenkonnektivität für Siebel	Beliebig	Siebel	SCBroker-Port	Zulassen

8.18 BI-Plattform und Reverse-Proxy-Server

Die BI-Plattform kann in einer Umgebung mit einem oder mehreren Reverse-Proxy-Servern implementiert werden. Ein Reverse Proxy-Server wird normalerweise vor den Webanwendungsservern implementiert, um sie hinter einer einzelnen IP-Adresse zu verbergen. In dieser Konfiguration wird der gesamte an private Webanwendungsserver gerichtete Internet-Datenverkehr über den Reverse Proxy-Server geroutet, während die privaten IP-Adressen unerkannt bleiben.

Da der Reverse Proxy-Server die öffentlichen URLs in interne URLs übersetzt, muss er mit den URLs der BI-Plattform-Webanwendungen konfiguriert werden, die im internen Netzwerk implementiert sind.

8.18.1 Unterstützte Reverse Proxy-Server

Die BI-Plattform unterstützt die folgenden Reverse-Proxy-Server:

- IBM Tivoli Access Manager WebSEAL 6
- Apache 2.2
- Microsoft ISA 2006

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.18.2 Allgemeine Informationen zur Implementierung von Webanwendungen

BI-Plattform-Webanwendungen werden auf einem Webanwendungsserver implementiert. Die Anwendungen werden automatisch während der Installation durch das WDeploy-Tool implementiert. Das Tool kann auch zur manuellen Implementierung der Anwendungen verwendet werden, nachdem die BI-Plattform implementiert wurde. Die Webanwendungen befinden sich im folgenden Verzeichnis in einer Standardinstallation unter Windows:

```
C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles
\webapps
```

WDeploy wird zur Implementierung von WAR-Dateien wie den folgenden verwendet:

- *BOE*: beinhaltet die Central Management Console (CMC), BI-Launchpad und OpenDocument
- *dswsbobje*: beinhaltet die Webdienstanwendung

Wenn sich der Webanwendungsserver hinter einem Reverse Proxy-Server befindet, sollte der Reverse Proxy-Server mit den korrekten Kontextpfaden der WAR-Dateien konfiguriert werden. Um die gesamte BI-Plattform-Funktionalität verfügbar zu machen, konfigurieren Sie einen Kontextpfad für jede installierte WAR-Datei der BI-Plattform.

8.19 Konfigurieren von Reverse Proxy-Servern für BI-Plattform-Webanwendungen

In Implementierungen, in denen BI-Plattform-Webanwendungen hinter einem Reverse Proxy-Server implementiert sind, muss der Reverse Proxy-Server für die Zuordnung eingehender URL-Anforderungen zur richtigen Webanwendung konfiguriert werden.

Diese Abschnitt enthält spezifische Konfigurationsbeispiele für einige unterstützte Reverse Proxy-Server. Weitere Informationen finden Sie in der Produktdokumentation Ihres Reverse Proxy-Servers.

8.19.1 Ausführliche Anweisungen zur Konfiguration von Reverse Proxy-Servern

Konfigurieren der WAR-Dateien

BI-Plattform-Webanwendungen werden als WAR-Dateien auf einem Webanwendungsserver implementiert. Stellen Sie sicher, dass Sie auf dem Reverse Proxy-Server eine Direktive für die WAR-Datei konfigurieren, die für die Implementierung benötigt wird. Zur Implementierung der WAR-Dateien `BOE` oder `dswsbobje` können Sie WDeploy verwenden. Weitere Informationen zu WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Angeben von BOE-Eigenschaften im benutzerdefinierten Konfigurationsverzeichnis

Die Datei `BOE.war` enthält globale und anwendungsspezifische Eigenschaften. Verwenden Sie das benutzerdefinierte Konfigurationsverzeichnis, wenn Sie die Eigenschaften ändern müssen. Das Verzeichnis befindet sich standardmäßig unter `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Achtung

Um zu vermeiden, dass im Standardverzeichnis Dateien überschrieben werden, ändern Sie die Eigenschaften im Verzeichnis `config\default` nicht. Die Benutzer sollten das Verzeichnis `custom` verwenden.

Hinweis

Auf manchen Webanwendungsservern wie der mit der BI-Plattform gebündelten Tomcat-Version können Sie direkt auf die Datei `BOE.war` zugreifen. In einem solchen Szenario können Sie die benutzerdefinierten Einstellungen direkt und ohne die WAR-Datei zu deinstallieren, festlegen. Wenn Sie nicht auf `BOE.war` zugreifen können, müssen Sie die Datei deinstallieren, anpassen und dann erneut implementieren.

Konsistente Verwendung von Schrägstrichen (/)

Definieren Sie die Kontextpfade im Reverse Proxy-Server auf dieselbe Weise, wie sie in eine Browser-URL eingegeben werden. Beispiel: Wenn in der Direktive am Ende des Spiegelpfads auf dem Reverse-Proxy-Server ein Schrägstrich (/) enthalten ist, geben Sie auch einen Schrägstrich am Ende der Browser-URL ein.

Stellen Sie sicher, dass der Schrägstrich (/) in Quell-URL und Ziel-URL in der Direktive des Reverse Proxy-Servers konsistent verwendet wird. Wenn der Schrägstrich (/) am Ende der Quell-URL hinzugefügt wird, muss er auch am Ende der Ziel-URL hinzugefügt werden.

8.19.2 Konfigurieren der Reverse Proxy-Server

Die folgenden Schritte sind auszuführen, damit BI-Plattform-Webanwendungen hinter einem unterstützten Reverse Proxy-Server arbeiten können.

1. Stellen Sie sicher, dass der Reverse Proxy-Server entsprechend den Anweisungen des Providers und der Netzwerktopologie der Implementierung ordnungsgemäß konfiguriert ist.
2. Stellen Sie fest, welche BI-Plattform-WAR-Datei benötigt wird.
3. Konfigurieren Sie den Reverse Proxy-Server für jede BI-Plattform-WAR-Datei. Beachten Sie, dass für jeden Reverse Proxy-Servertyp unterschiedliche Regeln gelten.
4. Führen Sie besondere Konfigurationsschritte aus, die u.U. erforderlich sind. Für einige Webanwendungen sind bei der Implementierung auf bestimmten Webanwendungsservern besondere Konfigurationsschritte erforderlich.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.19.3 Konfigurieren des Apache-2.2-Reverse Proxy-Servers für die BI-Plattform

In diesem Abschnitt wird der Workflow zur Konfiguration der BI-Plattform und von Apache 2.2 für deren Zusammenarbeit beschrieben.

1. Stellen Sie sicher, dass die BI-Plattform und Apache 2.2 auf separaten Rechnern installiert sind.
2. Apache 2.2 muss, wie in der Dokumentation des Providers beschrieben, als Reverse Proxy-Server installiert und konfiguriert sein.
3. Konfigurieren Sie `ProxyPass` für jede WAR-Datei, die hinter dem Reverse Proxy-Server implementiert wird.
4. Konfigurieren Sie `ProxyPassReverseCookiePath` für jede Webanwendung, die hinter dem Reverse Proxy-Server implementiert wird. Beispiel:

```
ProxyPass /C1/BOE/ http://<appservername>:80/BOE/
ProxyPassReverseCookiePath /BOE/C1/BOE/
ProxyPassReverse /C1/BOE/ http://<appservername>:80/BOE/
ProxyPass /C1/explorer/ http://<appservername>:80/explorer/
ProxyPassReverseCookiePath /BOE/C1/explorer/
ProxyPassReverse /C1/explorer/ http://<appservername>:80/explorer/
```

8.19.4 Konfigurieren des WebSEAL-6.0-Reverse Proxy-Servers für die BI-Plattform

In diesem Abschnitt wird die Konfiguration der BI-Plattform für die Zusammenarbeit mit WebSEAL 6.0 erläutert.

Die empfohlene Konfigurationsmethode besteht darin, eine einzelne Standardverknüpfung zu erstellen, durch die alle auf einem internen Webanwendungsserver oder Webserver gehosteten BI-Plattform-Webanwendungen einem einzigen Bereitstellungspunkt zugeordnet werden.

1. Stellen Sie sicher, dass die BI-Plattform und WebSEAL 6.0 auf separaten Rechnern installiert sind.

   Obwohl die BI-Plattform und WebSEAL 6.0 auf demselben Rechner implementiert werden können, wird davon abgeraten. Hinweise zur Konfiguration dieses Implementierungsszenarios finden Sie in der WebSEAL 6.0-Produktdokumentation.
2. Stellen Sie sicher, dass WebSEAL 6.0 entsprechend den Anweisungen in der Herstellerdokumentation installiert und konfiguriert ist.
3. Starten Sie das Befehlszeilen-Dienstprogramm **pdadmin** von WebSEAL. Melden Sie sich als Benutzer mit Administratorrechten bei einer sicheren Domäne wie **sec_master** an.
4. Geben Sie den folgenden Befehl an der **pdadmin sec_master**-Eingabeaufforderung ein:

```
server task <instance_name-webseald-host_name> create -t
<type> -h <host_name> -p <port> <junction_point>
```

   Dabei entspricht

   - `<Instanzenname-webseald-Hostname>` dem vollständigen Servernamen der installierten WebSEAL-Instanz. Verwenden Sie diesen vollständigen Servernamen im selben Format wie in der Ausgabe des Befehls `server list`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- `<Typ>` dem Typ der Junction. Verwenden Sie `tcp`, wenn die Junction einem internen HTTP-Port zugeordnet wird. Verwenden Sie `ssl`, wenn die Junction einem internen HTTPS-Port zugeordnet wird.
- `<Hostname>` dem DNS-Hostnamen oder der IP-Adresse des internen Servers, bei dem die Anforderungen eingehen.
- `<Port>` dem TCP-Port des internen Servers, bei dem die Anforderungen eingehen.
- `<Junction_Punkt>` dem Verzeichnis im geschützten WebSEAL-Objektraum, in dem der Dokumentraum des internen Servers bereitgestellt wird.

Beispiel

```
server task default-webseald-webseal.rp.sap.com
create -t tcp -h 10.50.130.123 -p 8080/hr
```

8.19.5 Konfigurieren von Microsoft ISA 2006 für die BI-Plattform

In diesem Abschnitt wird die Konfiguration der BI-Plattform für die Zusammenarbeit mit ISA 2006 erläutert.

Die empfohlene Konfigurationsmethode besteht darin, eine einzelne Standardverknüpfung zu erstellen, durch die alle auf einem internen Webanwendungsserver oder Webserver gehosteten BI-Plattform-WAR-Dateien einem einzigen Bereitstellungspunkt zugeordnet werden. Je nach Webanwendungsserver ist eine zusätzliche Konfiguration auf dem Anwendungsserver erforderlich, damit er zusammen mit ISA 2006 funktioniert.

1. Stellen Sie sicher, dass die BI-Plattform und ISA 2006 auf separaten Rechnern installiert sind.

   Obwohl die BI-Plattform und ISA 2006 auf demselben Rechner implementiert werden können, wird davon abgeraten. Hinweise zur Konfiguration dieses Implementierungsszenarios finden Sie in der ISA 2006-Dokumentation.
2. Stellen Sie sicher, dass ISA 2006 entsprechend den Anweisungen in der Herstellerdokumentation installiert und konfiguriert ist.
3. Starten Sie das Dienstprogramm "ISA Server-Verwaltung".
4. Verwenden Sie den Navigationsbereich, um eine neue Veröffentlichungsregel zu starten.
   a) Fahren Sie fort mit...

      Arrays > **Rechnername** > **Firewallrichtlinie** > **Neu** > **Website-Veröffentlichungsregel**

      Nicht vergessen

      Ersetzen Sie `Rechnername` durch den Namen des Rechners, auf dem ISA 2006 installiert ist.

   b) Geben Sie unter **Name der Webveröffentlichungsregel** einen Regelnamen ein, und klicken Sie auf **Weiter**.
   c) Wählen Sie **Zulassen** als Regelaktion, und klicken Sie auf **Weiter**.
   d) Wählen Sie **Einzelne Website oder Lastausgleich veröffentlichen** als Veröffentlichungstyp, und klicken Sie auf **Weiter**.
   e) Wählen Sie einen Verbindungstyp zwischen dem ISA-Server und der veröffentlichten Website, und klicken Sie auf **Weiter**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wählen Sie beispielsweise **Nicht sichere Verbindungen verwenden, um eine Verbindung zum veröffentlichten Webserver oder zur Serverfarm herzustellen**.

f) Geben Sie den internen Namen der Website, die Sie veröffentlichen (z.B. den Namen des Rechners, auf dem die BI-Plattform gehostet wird) in **Interner Sitename** ein, und klicken Sie auf **Weiter**.

> **Hinweis**
>
> Wenn der Rechner, auf dem ISA 2006 gehostet wird, keine Verbindung zum Zielserver herstellen kann, wählen Sie **Name oder IP-Adresse eines Computers verwenden, um eine Verbindung zum veröffentlichten Server herzustellen** und geben den Namen oder die IP-Adresse in das vorgegebene Feld ein.

g) Wählen Sie in *Details des öffentlichen Namens* den Domänennamen (z.B.**Beliebiger Domänenname**) aus, und geben Sie interne Veröffentlichungsdetails (z.B. `/*`) ein. Klicken Sie auf **Weiter**.
Anschließend erstellen Sie einen neuen Weblistener, der eingehende Webanforderungen überwacht.

5. Klicken Sie auf **Neu**, um den Assistenten für neue Weblistenerdefinitionen zu starten.
   a) Geben Sie einen Namen in **Weblistenername** ein, und klicken Sie auf **Weiter**.
   b) Wählen Sie einen Verbindungstyp zwischen dem ISA-Server und der veröffentlichten Website, und klicken Sie auf **Weiter**.
   Wählen Sie beispielsweise **Keine sicheren SSL-Verbindungen mit Clients erforderlich**.
   c) Wählen Sie im Bereich *Weblistener-IP-Adressen* Folgendes aus, und klicken Sie auf **Weiter**.
      - Intern
      - Extern
      - Lokaler Host
      - Alle Netzwerke

   Der ISA Server ist jetzt für die ausschließliche Veröffentlichung über HTTP konfiguriert.
   d) Wählen Sie eine Option für die *Authentifizierungseinstellung* aus, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
   Der neue Listener ist jetzt für die Webveröffentlichungsregel konfiguriert.
6. Klicken Sie unter **Benutzersätze** auf *Weiter* und dann auf **Fertig stellen**.
7. Klicken Sie auf **Übernehmen**, um alle Einstellungen für die Webveröffentlichungsregel zu speichern und die ISA 2006-Konfiguration zu aktualisieren.
   Anschließend müssen die Eigenschaften der Webveröffentlichungsregel aktualisiert werden, um die Pfade für die Webanwendungen zuzuordnen.
8. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf die von Ihnen konfigurierte Firewallrichtlinie, und wählen Sie **Eigenschaften**.
9. Klicken Sie auf der Registerkarte *Pfade* auf **Hinzufügen**, um SAP BusinessObjects-Webanwendungen Routen zuzuordnen.
10. Wählen Sie auf der Registerkarte *Öffentlicher Name* die Option **Anforderungen für die folgenden Websites**, und klicken Sie auf **Hinzufügen**.
11. Geben Sie im Dialogfeld *Öffentlicher Name* Ihren ISA 2006-Servernamen ein, und klicken Sie auf **OK**.
12. Klicken Sie auf **Übernehmen**, um alle Einstellungen für die Webveröffentlichungsregel zu speichern und die ISA 2006-Konfiguration zu aktualisieren.
13. Überprüfen Sie die Verbindungen, indem Sie folgende URL aufrufen:

```
http://<ISA-Server-Hostname>:<Portnummer des Weblisteners>/<Externer Pfad der
Anwendung>
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Beispiel: **http://myISAserver:80/Product/BOE/CMC**

> **Hinweis**
>
> Der Browser muss u.U. mehrere Male aktualisiert werden.

Die HTTP-Richtlinie für die gerade konfigurierte Regel muss geändert werden, um sicherzustellen, dass Sie sich bei der CMC anmelden können. Klicken Sie mit der rechten Maustaste auf die Regel, die Sie im Dienstprogramm "ISA Server-Verwaltung" erstellt haben, und wählen Sie **HTTP konfigurieren**. Anschließend deaktivieren Sie im Bereich *URL-Schutz* die Option **Normalisierung überprüfen**.

Für den Remotezugriff auf die BI-Plattform muss eine Zugriffsregel erstellt werden.

8.20 Spezielle Konfiguration für die BI-Plattform in Reverse-Proxy-Umgebungen

Für einige BI-Plattform-Produkte sind zusätzliche Konfigurationsschritte erforderlich, damit sie in Reverse Proxy-Umgebungen ordnungsgemäß funktionieren. In diesem Abschnitt wird die zusätzliche Konfiguration beschrieben.

8.20.1 Aktivieren eines Reverse Proxys für Webdienste

In diesem Abschnitt werden die Schritte beschrieben, die zum Aktivieren von Reverse Proxys für Webdienste ausgeführt werden müssen.

8.20.1.1 So aktivieren Sie einen Reverse Proxy unter Tomcat

Um Reverse Proxys auf dem Tomcat Web Application Server zu aktivieren, ändern Sie die Datei `server.xml`. Die erforderlichen Änderungen umfassen das Einstellen von `proxyPort` als Abhöranschluss für den Reverse Proxy-Server und das Hinzufügen eines neuen `proxyName`. In diesem Abschnitt wird das Verfahren erläutert.

1. Stoppen Sie Tomcat.
2. Öffnen Sie die Datei `server.xml` für Tomcat.

   Unter Windows befindet sich `server.xml` in `C:\Programme (x86)\SAP BusinessObjects\Tomcat\conf`

   Unter UNIX befindet sich `server.xml` in `<CATALINA_HOME>/conf`. Der Standardwert von `<CATALINA_HOME>` lautet `<INSTALLVERZ>/sap_bobj/tomcat`.
3. Suchen Sie den folgenden Abschnitt in der Datei "server.xml":

```
<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!--See proxy documentation for more information about using
                 this.-->
<!--
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
    <Connector port="8082"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
                enableLookups="false"
    acceptCount="100" debug="0" connectionTimeout="20000"
                proxyPort="80" disableUploadTimeout="true" />
    -->
```

4. Entfernen Sie den Kommentar für das Connector-Element, indem Sie `<!--` und `-->` löschen.
5. Ändern Sie den Wert von `proxyPort` in den Abhöranschluss des Reverse Proxy-Servers.
6. Fügen Sie der Connector-Attributliste ein neues `proxyName`-Attribut hinzu. Der Wert von `proxyName` muss dem Proxy-Servernamen entsprechen, der von Tomcat in die richtige IP-Adresse aufgelöst werden muss.

   Beispiel:

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082 -->
                <!--See proxy documentation for more information about using
                  this.-->
                <Connector port="8082"
                maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
                enableLookups="false"
                acceptCount="100" debug="0"
connectionTimeout="20000"
                proxyName="my_reverse_proxy_server.domain.com"
                proxyPort="ReverseProxyServerPort"
                disableUploadTimeout="true" />
```

   `Mein_Reverse_Proxy_Server.Domäne.com` und `ReverseProxyServerPort` sollten dabei durch den richtigen Reverse Proxy-Servernamen und dessen Abhöranschluss ersetzt werden.
7. Speichern und schließen Sie die Datei `server.xml`.
8. Starten Sie Tomcat neu.
9. Stellen Sie sicher, dass der virtuelle Pfad des Reverse Proxy-Servers dem richtigen Tomcat-Connector-Port zugeordnet wird. Im vorangehenden Beispiel lautet die Portnummer 8082.

   Im folgenden Beispiel finden Sie eine Beispielkonfiguration für Apache HTTP Server 2.2, der als Reverse-Proxy-Server für die auf Tomcat implementierten SAP-BusinessObjects™-Webdienste fungiert:

```
ProxyPass /XI3.0/dswsbobje http://internalServer:8082/dswsbobje
                ProxyPassReverseCookiePath /dswsbobje /XI3.0/
dswsbobje
```

Zum Aktivieren von Webdiensten müssen Proxyname und Portnummer für den Connector identifiziert werden.

8.20.1.2 Aktivieren von Reverse Proxys für Webdienste auf anderen Webanwendungsservern als Tomcat

Bei den folgenden Schritten wird vorausgesetzt, dass die BI-Plattform-Webanwendungen erfolgreich für den ausgewählten Webanwendungsserver konfiguriert werden. Beachten Sie, dass bei `wsresources` die Groß-/Kleinschreibung berücksichtigt wird.

1. Halten Sie den Webanwendungsserver an.
2. Geben Sie die externe URL der Webdienste in der Datei `dsws.properties` an.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Diese Datei befindet sich in der Webanwendung `dswsbobje`. Wenn Ihre externe URL beispielsweise `http://my_reverse_proxy_server.domain.com/dswsbobje/` lautet, aktualisieren Sie die Eigenschaften in der Datei "dsws.properties" wie folgt:

- `wsresource1=ReportEngine|reportengine web service alone|http://Mein_Reverse_Proxy_Server.Domäne.com/SAP/dswsbobje/services/ReportEngine`
- `wsresource2=BICatalog|bicatalog web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BICatalog`
- `wsresource3=Publish|publish web service alone|http://Mein_Reverse_Proxy_Server.Domäne.com/SAP/dswsbobje/services/Publish`
- `wsresource4=QueryService|query web service alone|http://Mein_Reverse_Proxy_Server.Domäne.com/SAP/dswsbobje/services/QueryService`
- `wsresource5=BIPlatform|BIPlatform web service|http://Mein_Reverse_Proxy_Server.Domäne.com/SAP/dswsbobje/services/BIPlatform`
- `wsresource6=LiveOffice|Live Office web service|http://Mein_Reverse_Proxy_Server.Domäne.com/SAP/dswsbobje/services/LiveOffice`

3. Speichern und schließen Sie die Datei `dsws.properties`.
4. Starten Sie den Webanwendungsserver neu.
5. Stellen Sie sicher, dass der virtuelle Pfad des Reverse Proxy-Servers dem richtigen Connector-Port des Webanwendungsservers zugeordnet wird. Im Folgenden finden Sie eine Beispielkonfiguration für Apache HTTP Server 2.2, der als Reverse Proxy-Server für die unter dem gewünschten Webanwendungsserver implementierten BI-Plattform-Webdienste fungiert:

   ```
   ProxyPass /SAP/dswsbobje http://internalServer:<Überwachungsport> /dswsbobje
   ```

   ```
   ProxyPassReverseCookiePath /dswsbobje /SAP/dswsbobje
   ```

   Dabei entspricht `<Überwachungsport>` dem Überwachungsport des Webanwendungsservers.

8.20.2 Aktivieren des Stammpfads für Sitzungscookies für ISA 2006

In diesem Abschnitt wird beschrieben, wie Sie bestimmte Webanwendungsserver so konfigurieren, dass der Stammpfad für Sitzungscookies mit ISA 2006 als Reverse Proxy-Server funktioniert.

8.20.2.1 Konfigurieren von Apache Tomcat

Um den Stammpfad so zu konfigurieren, dass Sitzungscookies mit ISA 2006 als Reverse Proxy-Server funktionieren, fügen Sie dem `<Connector>`-Element in `server.xml` Folgendes hinzu:

```
emptySessionPath="true"
```

1. Stoppen Sie Tomcat.
2. Öffnen Sie die Datei "server.xml" an folgendem Speicherort:

   `<CATALINA_HOME>\conf`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Suchen Sie in der Datei "server.xml" den folgenden Abschnitt:

```
<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this -->
<!--
<Connector port="8082"
maxThreads="150" minSpareThreads="25" maxS
pareThreads="75" enableLookups="false"
acceptCount="100" debug="0" connectionTimeout="20000"
proxyPort="80" disableUploadTimeout="true" />
-->
```

4. Entfernen Sie den Kommentar für das Connector-Element, indem Sie `<!--` und `-->` löschen.
5. Um den Stammpfad so zu konfigurieren, dass Sitzungscookies mit ISA 2006 als Reverse Proxy-Server funktionieren, fügen Sie dem `<Connector>`-Element in `server.xml` Folgendes hinzu:

```
emptySessionPath="true"
```

6. Ändern Sie den Wert von `proxyPort` in den Abhöranschluss des Reverse Proxy-Servers.
7. Fügen Sie der Connector-Attributliste ein neues `proxyName`-Attribut hinzu. Der Wert muss einem Proxy-Servernamen entsprechen, der von Tomcat in die richtige IP-Adresse aufgelöst werden muss.

   Beispiel:

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082
-->
<!-- See proxy documentation for more information about using
this -->
<Connector port="8082"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" emptySessionPath="true"
acceptCount="100" debug="0" connectionTimeout="20000"
proxyName="my_reverse_proxy_server.domain.com"
proxyPort="ReverseProxyServerPort"
disableUploadTimeout="true" />
```

8. Speichern und schließen Sie die Datei `server.xml`.
9. Starten Sie Tomcat neu.

Stellen Sie sicher, dass der virtuelle Pfad des Reverse Proxy-Servers dem richtigen Tomcat-Connector-Port zugeordnet wird. Im vorangehenden Beispiel lautet die Portnummer 8082.

8.20.2.2 Konfigurieren von Sun Java 8.2

Die Datei `sun-web.xml` muss für jede BI-Plattform-Webanwendung geändert werden.

1. Gehen Sie zu **<SUN_WEBAPP_DOMAIN>**\generated\xml\j2ee-modules\webapps\BOE\WEB-INF.
2. Öffnen Sie `sun-web.xml`.
3. Fügen Sie nach dem Container `<context-root>` Folgendes hinzu:

```
        <session-config>
                <cookie-properties>
                        <property name="cookiePath" value="/" />
                </cookie-properties>
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
        </session-config>
    <property name="reuseSessionID" value="true"/>
```

4. Speichern und schließen Sie `sun-web.xml`.
5. Wiederholen Sie die Schritte 1 bis 4 für jede Webanwendung.

8.20.2.3 Konfigurieren von Oracle Application Server 10gR3

Es ist erforderlich, die Datei `global-web-application.xml` oder `orion-web.xml` für das Implementierungsverzeichnis jeder BI-Plattform-Webanwendung zu ändern.

1. Gehen Sie zu **<ORACLE_HOME>**`\j2ee\home\config\`.
2. Öffnen Sie `global-web-application.xml` oder `orion-web.xml`.
3. Fügen Sie dem Container `<orion-web-app>` folgende Zeile hinzu:

```
<session-tracking cookie-path="/" />
```

4. Speichern und schließen Sie die Konfigurationsdatei.
5. Melden Sie sich bei der Oracle Admin-Konsole an:
   a) Rufen Sie **OC4J:home** > **Administration** > **Servereigenschaften** auf.
   b) Wählen Sie unter *Befehlszeilenoptionen* den Eintrag **Optionen**.
   c) Klicken Sie auf **Weitere Zeile hinzufügen**, und geben Sie Folgendes ein:

```
Doracle.useSessionIDFromCookie=true
```

6. Starten Sie den Oracle-Server neu.

8.20.2.4 Konfigurieren der WebSphere Community Edition 2.0

1. Öffnen Sie die WebSphere Community Edition 2.0 Admin Console.
2. Suchen Sie im linken Navigationsbereich *Server*, und wählen Sie **Web Server**.
3. Wählen Sie die Connectors aus, und klicken Sie auf **Bearbeiten**.
4. Aktivieren Sie das Kontrollkästchen **emptySessionPath**, und klicken Sie auf **Save** (Speichern).
5. Geben Sie Ihren ISA-Servernamen in **ProxyName** ein.
6. Geben Sie die Portnummer des ISA-Listeners in **ProxyPort** ein.
7. Stoppen und starten Sie den Connector neu.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8.20.3 Aktivieren von Reverse Proxys für SAP BusinessObjects Live Office

Um die SAP BusinessObjects Live Office-Funktion "Objekt in Webbrowser anzeigen" für Reverse Proxys zu aktivieren, passen Sie die Standard-Viewer-URL an. Dazu verwenden Sie die Central Management Console (CMC) oder die Live Office-Optionen.

> **Hinweis**
>
> Dieser Abschnitt setzt voraus, dass Reverse Proxy Server für BI-Launchpad- und BI-Plattform-Webdienste erfolgreich aktiviert wurden.

8.20.3.1 Anpassen der Standard-Viewer-URL in der CMC

1. Melden Sie sich bei der CMC an.
2. Klicken Sie auf der Seite *Anwendungen* auf **Central Management Console**.
3. Wählen Sie **Aktionen** > **Verarbeitungseinstellungen** aus.
4. Wählen Sie im Feld **URL** die richtige Standardanzeige-URL aus, und klicken Sie auf **Speichern und schließen**. Beispiel:

   ```
   http://ReverseProxyServer:ReverseProxyServerPort/BOE/OpenDocument.jsp?
   sIDType=CUID&iDocID=%SI_CUID%
   ```

   `ReverseProxyServer` und `ReverseProxyServerPort` entsprechen dem richtigen Reverse Proxy-Servernamen und dessen Abhöranschluss.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9 Authentifizierung

9.1 Authentifizierungsoptionen in der BI-Plattform

Bei der Authentifizierung wird die Identität eines Benutzers verifiziert, der versucht, auf das System zuzugreifen. Bei der Rechteverwaltung wird geprüft, ob der Benutzer über die nötigen Rechte verfügt, um die gewünschte Aktion für das angegebene Objekt auszuführen.

Mithilfe von Sicherheits-Plugins können Sie Vorgehensweisen der BI-Plattform bei der Authentifizierung von Benutzern erweitern und anpassen. Sicherheits-Plugins vereinfachen die Kontoerstellung und -verwaltung, da Sie Benutzerkonten und Gruppen von Systemen von Drittherstellern in der BI-Plattform zuweisen können. Benutzerkonten oder Gruppen von Drittherstellern lassen sich vorhandenen BI-Plattform-Benutzerkonten oder -Gruppen zuordnen. Außerdem können Sie neue Enterprise-Benutzerkonten oder -Gruppen erstellen, die jedem zugeordneten Objekt im externen System entsprechen.

Die aktuelle Version unterstützt die folgenden Authentifizierungsmethoden:

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Da sich die BI-Plattform komplett anpassen lässt, können sich die Authentifizierung und die Prozesse von System zu System unterscheiden.

Weitere Informationen

Übersicht über die Enterprise-Authentifizierung [Seite 225]
Konfigurieren der SAP-Authentifizierung [Seite 299]
Verwenden der LDAP-Authentifizierung [Seite 239]
Windows AD unterstützt Anforderungen und die Erstkonfiguration [Seite 262]
Aktivieren der JD Edwards EnterpriseOne-Authentifizierung [Seite 345]
Aktivieren der Oracle-EBS-Authentifizierung [Seite 356]
Aktivieren der PeopleSoft Enterprise-Authentifizierung [Seite 329]
Aktivieren der Siebel-Authentifizierung [Seite 350]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.1.1 Primäre Authentifizierung

Die primäre Authentifizierung findet statt, wenn ein Benutzer zum ersten Mal versucht, auf das System zuzugreifen. Während der primären Authentifizierung kann eine der beiden folgenden Situationen auftreten:

- Wenn die Einzelanmeldung nicht konfiguriert ist, gibt der Benutzer seine Anmeldedaten wie Benutzernamen, Kennwort und Authentifizierungstyp an.

  Diese Angaben werden von den Benutzern im Anmeldefenster eingegeben.
- Wenn eine Einzelanmeldungsmethode konfiguriert ist, werden die Anmeldedaten für die Benutzer im Hintergrund weitergegeben.

  Diese Angaben werden unter Verwendung anderer Methoden, wie Kerberos oder SiteMinder, extrahiert.

Als Authentifizierungstyp kann Enterprise, LDAP, Windows AD, SAP, Oracle EBS, Siebel, JD Edwards EnterpriseOne oder PeopleSoft Enterprise verwendet werden. Dies hängt von den Typen ab, die Sie im Verwaltungsbereich "Authentifizierung" der Central Management Console (CMC) eingerichtet und aktiviert haben. Der Webbrowser des Benutzers übermittelt die Informationen per HTTP an Ihren Webserver, der die Informationen an den CMS oder den geeigneten Plattform-Server weiterleitet.

Der Webanwendungsserver übergibt die Benutzerinformationen in einem serverseitigen Skript. Das Skript kommuniziert intern mit dem SDK. Letztendlich authentifiziert das entsprechende Sicherheits-Plugin den Benutzer in der Benutzerdatenbank.

Wenn sich der Benutzer beispielsweise bei BI-Launchpad anmeldet und die Enterprise-Authentifizierung angibt, stellt das SDK sicher, dass das BI-Plattform-Sicherheits-Plugin die Authentifizierung ausführt. Mit dem Sicherheits-Plugin überprüft der Central Management Server (CMS) den Benutzernamen und das Kennwort in der Systemdatenbank. Wenn der Benutzer eine andere Authentifizierungsmethode angegeben hat, authentifiziert das SDK den Benutzer mithilfe des entsprechenden Sicherheits-Plugins.

Wenn das Sicherheits-Plugin eine Übereinstimmung von Anmeldedaten meldet, gewährt der CMS dem Benutzer eine aktive Systemidentität, und die folgenden Aktionen werden ausgeführt:

- Der CMS erstellt eine Enterprise-Sitzung für den Benutzer. Während die Sitzung aktiv ist, wird eine Benutzerlizenz im System konsumiert.
- Der CMS generiert und codiert ein Anmeldetoken, das an den Webanwendungsserver gesendet wird.
- Der Webanwendungsserver speichert die Benutzerinformationen in einer Sitzungsvariablen im Arbeitsspeicher. Während die Sitzung aktiv ist, werden Informationen gespeichert, mit denen die BI-Plattform Benutzeranfragen beantworten kann.

  > **Hinweis**
  >
  > In der Sitzungsvariablen ist das Kennwort des Benutzers nicht enthalten.

- Der Webanwendungsserver speichert das Anmeldetoken in einem Cookie auf dem Clientbrowser. Dieses wird nur zu Failover-Zwecken verwendet, beispielsweise wenn Sie über einen geclusterten CMS verfügen oder wenn BI-Launchpad für die Sitzungsaffinität geclustert wird.

  > **Hinweis**
  >
  > Das Anmeldetoken kann deaktiviert werden. In diesem Fall wird jedoch auch die Failover-Funktion deaktiviert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.1.2 Sicherheits-Plugins

Mithilfe von Sicherheits-Plugins können Sie Vorgehensweisen der BI-Plattform bei der Authentifizierung von Benutzern erweitern und anpassen. Die BI-Plattform wird derzeit mit den folgenden Plugins ausgeliefert:

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Sicherheits-Plugins ermöglichen die Kontoerstellung und -verwaltung, da Sie Benutzerkonten und Gruppen aus Drittherstellersystemen der BI-Plattform zuweisen können. Benutzerkonten oder Gruppen von Drittherstellern lassen sich vorhandenen BI-Plattform-Benutzerkonten oder -Gruppen zuordnen. Außerdem können Sie neue Enterprise-Benutzerkonten oder -Gruppen erstellen, die jedem zugeordneten Objekt im externen System entsprechen.

Die Sicherheits-Plugins verwalten die Benutzer- und Gruppenlisten des Drittherstellers dynamisch. Nachdem Sie der BI-Plattform eine externe Gruppe zugeordnet haben, können sich alle Benutzer, die dieser Gruppe angehören, erfolgreich bei der BI-Plattform anmelden. Wenn Sie anschließend die Mitgliedschaften in der Gruppe des Drittherstellers ändern, muss die Liste in der BI-Plattform nicht aktualisiert oder regeneriert werden. Wenn Sie der BI-Plattform zum Beispiel eine LDAP Gruppe zuordnen und dann der Gruppe einen neuen Benutzer hinzufügen, erstellt das Sicherheits-Plugin dynamisch einen Alias für den neuen Benutzer, wenn sich dieser zum ersten Mal mit gültigen LDAP-Anmeldedaten bei der BI-Plattform anmeldet.

Außerdem können Sie mit Sicherheits-Plugins Benutzern und Gruppen Rechte konsistent zuordnen, da die zugewiesenen Benutzer und Gruppen genau wie Enterprise-Konten behandelt werden. Beispiel: Sie ordnen einige Benutzerkonten oder Gruppen von Windows AD und einige von einem LDAP-Verzeichnisserver zu. Wenn Sie dann Rechte zuordnen oder neue benutzerdefinierte Gruppen in der BI-Plattform, erstellen möchten, nehmen Sie alle Einstellungen in der CMC vor.

Jedes Sicherheits-Plugin übernimmt die Funktion eines Authentifizierungsproviders, der Anmeldedaten in der entsprechenden Benutzerdatenbank verifiziert. Wenn sich Benutzer an der BI-Plattform anmelden, wählen sie Authentifizierungstypen aus, die Sie im Verwaltungsbereich "Authentifizierung" der CMC eingerichtet und aktiviert haben.

> **Hinweis**
>
> Das Windows AD-Sicherheits-Plugin kann Benutzer nicht authentifizieren, wenn die BI-Plattform-Serverkomponenten unter UNIX ausgeführt werden.

9.1.3 Einzelanmeldung bei der BI-Plattform

Die Einzelanmeldung bei der BI-Plattform bedeutet, dass Benutzer nach ihrer Anmeldung am Betriebssystem auf Anwendungen, die die Einzelanmeldung unterstützen, zugreifen können, ohne ihre Anmeldedaten erneut

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

einzugeben. Wenn sich ein Benutzer anmeldet, wird ein Sicherheitskontext für ihn erstellt. Dieser Kontext kann an die BI-Plattform zur SSO-Ausführung übergeben werden.

Der Begriff “anonyme Einzelanmeldung” bezieht sich auch auf die Einzelanmeldung bei der BI-Plattform, im engeren Sinn ist damit jedoch die Einzelanmeldung unter dem Benutzerkonto "Guest" gemeint. Sobald das Benutzerkonto "Guest" aktiviert ist (was standardmäßig der Fall ist), kann sich jeder Benutzer als Guest bei der BI-Plattform anmelden und auf das System zugreifen.

9.1.3.1 Unterstützung der Einzelanmeldung

Der Begriff "Einzelanmeldung" bezieht sich auf verschiedene Szenarios. Im einfachsten Einzelfall-Szenario kann ein Benutzer auf mindestens zwei Anwendungen bzw. Systeme zugreifen, während er seine Anmeldedaten nur einmal eingibt. Dadurch wird die Interaktion mit dem System vereinfacht.

Die Einzelanmeldung bei BI-Launchpad kann je nach Anwendungsservertyp und Betriebssystem über die BI-Plattform oder mithilfe eines der anderen Authentifizierungstools erfolgen.

Die folgenden Einzelanmeldungsmethoden sind bei Verwendung eines Java-Anwendungsservers unter Windows verfügbar:

- Windows AD mit Kerberos
- Windows AD mit SiteMinder

Die folgenden Einzelanmeldungsmethoden sind bei Verwendung von IIS unter Windows verfügbar:

- Windows AD mit Kerberos
- Windows AD mit NTLM
- Windows AD mit SiteMinder

Wenn Sie einen der von der Plattform unterstützten Webanwendungsserver verwenden, werden diese Einzelanmeldungsmethoden unter Windows oder Unix unterstützt.

- LDAP mit SiteMinder
- Vertrauenswürdige Authentifizierung
- Windows AD mit Kerberos
- LDAP über Kerberos auf SUSE 11
- SAP-NetWeaver-Einzelanmeldung durch vertrauenswürdige Authentifizierung

> **Hinweis**
>
> Windows AD mit Kerberos wird unterstützt, wenn die Java-Anwendung unter UNIX ausgeführt wird. Die BI-Plattform-Dienste müssen jedoch auf einem Windows-Server ausgeführt werden.

In der folgenden Tabelle werden die Methoden der Einzelanmeldungsunterstützung für BI-Launchpad beschrieben.

Authentifizierungsmodus	CMS-Server	Optionen	Anmerkungen
Windows AD	nur Windows	Nur Windows AD mit Kerberos	Die Windows AD-Authentifizierung bei BI-Launchpad und der CMC sind direkt einsatzfähig.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Authentifizierungsmodus	CMS-Server	Optionen	Anmerkungen
LDAP	Beliebige unterstützte Plattform	Unterstützte LDAP-Verzeichnisserver, nur mit SiteMinder	Die LDAP-Authentifizierung bei BI-Launchpad und der CMC ist direkt einsatzfähig. Für die Einzelanmeldung bei BI-Launchpad und der CMC ist SiteMinder erforderlich.
Enterprise	Beliebige unterstützte Plattform	Vertrauenswürdige Authentifizierung	Die Authentifizierung bei BI-Launchpad und der CMC ist direkt einsatzfähig. Für die Einzelanmeldung mit Enterprise-Authentifizierung bei BI-Launchpad und der CMC ist vertrauenswürdige Authentifizierung erforderlich.

- *Einzelanmeldung bei der BI-Plattform* [Seite 222]
- *Einzelanmeldung bei Datenbanken* [Seite 224]
- *End-to-End-Einzelanmeldung* [Seite 224]

9.1.3.2 Einzelanmeldung bei Datenbanken

Nachdem der Benutzer sich bei der BI-Plattform angemeldet hat, ermöglicht ihm die Einzelanmeldung bei der Datenbank die Ausführung bestimmter Aktionen, die Datenbankzugriff erfordern. Dazu gehören das Anzeigen und Aktualisieren von Berichten, ohne erneut Anmeldedaten eingeben zu müssen. Die Einzelanmeldung bei Datenbanken kann mit der Einzelanmeldung bei der BI-Plattform kombiniert werden, damit Benutzer noch einfacher auf die erforderlichen Ressourcen zugreifen können.

9.1.3.3 End-to-End-Einzelanmeldung

Die End-to-End-Einzelanmeldung beschreibt eine Konfiguration, in der Benutzer sowohl die Einzelanmeldung an der BI-Plattform am Frontend als auch die Einzelanmeldung an Datenbanken am Backend nutzen können. Folglich müssen Benutzer ihre Anmeldedaten nur einmal angeben, wenn sie sich beim Betriebssystem anmelden. Anschließend können sie dann auf die BI-Plattform zugreifen und Aktionen ausführen, die Datenbankzugriff erfordern, z.B. Berichte anzeigen.

In der BI-Plattform wird die End-to-End-Einzelanmeldung über Windows AD und Kerberos unterstützt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.2 Enterprise-Authentifizierung

9.2.1 Übersicht über die Enterprise-Authentifizierung

Die Enterprise-Authentifizierung ist die Standard-Authentifizierungsmethode für die BI-Plattform. Sie wird bei der ersten Installation des Systems automatisch aktiviert und kann nicht deaktiviert werden. Wenn Sie Benutzer und Gruppen hinzufügen und verwalten, speichert die BI-Plattform die Benutzer- und Gruppeninformationen in der eigenen Datenbank.

➔ Tipp

Verwenden Sie die vom System vorgegebene Enterprise-Authentifizierung, wenn Sie für die Arbeit mit der BI-Plattform einzelne Konten und Gruppen erstellen möchten, oder wenn Sie noch keine Benutzer- und Gruppenhierarchie auf einem Verzeichnisserver eines Drittherstellers eingerichtet haben.

Sie müssen die Enterprise-Authentifizierung weder konfigurieren noch aktivieren. Allerdings können Sie die Einstellungen der Enterprise-Authentifizierung ändern, um den jeweiligen Sicherheitsanforderungen Ihres Unternehmens zu entsprechen. Enterprise-Authentifizierungseinstellungen lassen sich nur über die Central Management Console (CMC) ändern.

9.2.2 Einstellungen der Enterprise-Authentifizierung

Einstellungen	Option	Beschreibung
Kennwortbeschränkungen	**Kennwörter mit Groß- und Kleinschreibung obligatorisch machen**	Diese Option stellt sicher, dass die Kennwörter mindestens zwei von den folgenden Zeichenklassen enthalten: Großbuchstaben, Kleinbuchstaben, Zahlen oder Satzzeichen.
	Mindestens N Zeichen	Wenn Sie eine Mindestkomplexität für Kennwörter obligatorisch machen, verringern Sie die Wahrscheinlichkeit, dass ein unberechtigter Benutzer einfach das Kennwort eines gültigen Benutzers errät.
Benutzerbeschränkungen	**Kennwort muss alle n Tage geändert werden**	Diese Option stellt sicher, dass Kennwörter durch regelmäßige Erneuerung nicht zum Problem werden.
	Die letzten N Kennwörter dürfen nicht wiederverwendet werden	Diese Option stellt sicher, dass Kennwörter nicht routinemäßig wiederholt werden.
	Mindestens N Minuten bis zur Änderung des Kennworts warten	Diese Option stellt sicher, dass neue Kennwörter nach Eingabe im System sofort wieder geändert werden können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Einstellungen	Option	Beschreibung
Anmeldebeschränkungen	**Konto nach N fehlgeschlagenen Anmeldeversuchen deaktivieren**	Diese Sicherheitsoption gibt an, wie viele Anmeldeversuche ein Benutzer beim System hat, bevor sein Konto deaktiviert wird.
	Zähler für fehlgeschlagene Anmeldungen nach N Minuten zurücksetzen	Diese Option legt ein Zeitintervall zum Zurücksetzen des Zählers für Anmeldeversuche fest.
	Konto nach N Minuten wieder aktivieren	Diese Option gibt an, wie lang ein Konto nach n fehlgeschlagenen Anmeldeversuchen deaktiviert bleibt.
Datenquellen-Anmeldedaten mit Anmeldedaten synchronisieren	**Die Datenquellen-Anmeldedaten des Benutzers zum Zeitpunkt der Anmeldung aktivieren und aktualisieren**	Diese Option aktiviert Datenquellen-Anmeldedaten nach der Anmeldung des Benutzers.
Vertrauenswürdige Authentifizierung	**Vertrauenswürdige Authentifizierung ist aktiviert**.	Stellt die Einstellungen zum Einrichten der vertrauenswürdigen Authentifizierung bereit

Weitere Informationen

Aktivieren der vertrauenswürdigen Authentifizierung [Seite 227]

9.2.3 Ändern der Enterprise-Einstellungen

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
2. Doppelklicken Sie auf **Enterprise**.
   Das Dialogfeld *Enterprise* wird angezeigt.
3. Ändern Sie die Einstellungen.

   Tipp

   Sie können alle Einstellungen auf die Standardwerte zurücksetzen, indem Sie auf **Zurücksetzen** klicken.

4. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

9.2.3.1 Ändern der allgemeinen Kennworteinstellungen

Hinweis

Konten, die längere Zeit nicht verwendet werden, werden nicht automatisch deaktiviert. Administratoren müssen inaktive Konten automatisch löschen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
2. Doppelklicken Sie auf **Enterprise**.
   Das Dialogfeld *Enterprise* wird angezeigt.
3. Aktivieren Sie das Kontrollkästchen der gewünschten Kennworteinstellungen und geben Sie ggf. einen Wert ein.

   Die folgende Tabelle gibt den Mindest- und den Höchstwert für die einzelnen kennwortbezogenen Einstellungen an, die Sie festlegen können.

Kennworteinstellung	Minimum	Empfohlener Höchstwert
Kennwörter mit Groß- und Kleinschreibung obligatorisch machen	N/A	N/A
Mindestens N Zeichen	0 Zeichen	64 Zeichen
Kennwort muss alle n Tage geändert werden	1 Tag	100 Tage
Die letzten N Kennwörter dürfen nicht wiederverwendet werden	1 Kennwort	100 Kennwörter
Mindestens N Minuten bis zur Änderung des Kennworts warten	0 Minuten	100 Minuten
Konto nach N fehlgeschlagenen Anmeldeversuchen deaktivieren	1 Fehlschläge	100 Fehlschläge
Zähler für fehlgeschlagene Anmeldungen nach N Minuten zurücksetzen	1 Minute	100 Minuten
Konto nach N Minuten wieder aktivieren	0 Minuten	100 Minuten

4. Klicken Sie auf **Aktualisieren**.

> **Hinweis**
>
> Inaktive Enterprise-Konten werden nicht automatisch deaktiviert. Die Systemverwaltung muss Konten, die nicht mehr aktiv sind, manuell löschen.

9.2.4 Aktivieren der vertrauenswürdigen Authentifizierung

Die vertrauenswürdige Enterprise-Authentifizierung wird zum Durchführen der Einzelanmeldung verwendet, wobei dem Webanwendungsserver die Verifizierung der Identität des Benutzers überlassen wird. Bei dieser Authentifizierungsmethode wird Vertrauenswürdigkeit zwischen dem Central Management Server (CMS) und dem die BI-Plattform-Webanwendung hostenden Webanwendungsserver eingerichtet. Anschließend überträgt das System die Verifizierung der Identität eines Benutzers an den Webanwendungsserver. Die vertrauenswürdige

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Authentifizierung kann zur Unterstützung von Authentifizierungsmethoden wie SAML, x.509 und anderen Methoden verwendet werden, die über keine dedizierten Authentifizierungsplugins verfügen.

Die Benutzer ziehen es vor, sich einmal am System anzumelden, ohne Kennwörter mehrere Male während einer Sitzung eingeben zu müssen. Die vertrauenswürdige Authentifizierung stellt eine Java-Einzelanmeldungslösung für die Integration Ihrer BI-Plattform-Authentifizierungslösung in Authentifizierungslösungen anderer Hersteller dar. Anwendungen, die eine Vertrauensstellung beim Central Management Server (CMS) haben, können die vertrauenswürdige Authentifizierung verwenden, damit sich Benutzer ohne Angabe ihres Kennworts anmelden können.

Um die vertrauenswürdige Authentifizierung zu ermöglichen, müssen Sie über die Enterprise-Authentifizierungseinstellungen einen gemeinsamen geheimen Schlüssel auf dem Server konfigurieren, während der Client anhand der für die `BOE.war`-Datei angegebenen Eigenschaften konfiguriert wird.

Hinweis

- Bevor Sie die vertrauenswürdige Authentifizierung verwenden können, müssen entweder Enterprise-Benutzer erstellt oder Dritthersteller-Benutzer zugeordnet werden, die sich bei der BI-Plattform anmelden müssen.
- Die Einzelanmeldungs-URL für BI-Launchpad lautet `http://server:port/BOE/BI`.

Weitere Informationen

Konfigurieren des Servers für die Verwendung der vertrauenswürdigen Authentifizierung [Seite 228]
Konfigurieren der vertrauenswürdigen Authentifizierung für die Webanwendung [Seite 232]

9.2.4.1 Konfigurieren des Servers für die Verwendung der vertrauenswürdigen Authentifizierung

Bevor Sie die vertrauenswürdige Authentifizierung konfigurieren können, sind zunächst Enterprise-Benutzer zu erstellen oder Dritthersteller-Benutzer zuzuordnen, die sich bei der BI-Plattform anmelden müssen.

1. Melden Sie sich an der CMC an.
2. Wechseln Sie zum Verwaltungsbereich *Authentifizierung*.
3. Klicken Sie auf die Option **Enterprise**.
   Das Dialogfeld *Enterprise* wird angezeigt.
4. Unter *Vertrauenswürdige Authentifizierung*:
   a) Klicken Sie auf **Vertrauenswürdige Authentifizierung ist aktiviert**.
   b) Klicken Sie auf **Neuer gemeinsamer geheimer Schlüssel**.
   Die Meldung `Der gemeinsame geheime Schlüssel wurde generiert und steht zum Herunterladen bereit` wird angezeigt.
   c) Klicken Sie auf **Gemeinsamen geheimen Schlüssel herunterladen**.
   Der gemeinsame geheime Schlüssel wird von Client und CMS zum Einrichten der Vertrauenswürdigkeit verwendet. Konfigurieren Sie zuerst den Server und dann den Client für die vertrauenswürdige Authentifizierung.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Das Dialogfeld *Dateidownload* wird angezeigt.

d) Klicken Sie auf **Speichern**, und speichern Sie die Datei `TrustedPrincipal.conf` in einem der folgenden Verzeichnisse:

- `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
- `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`

> **Achtung**
>
> Setzen Sie die Zeitüberschreitung nicht auf `0` (Null). Der Wert `0` bedeutet, dass die Zeit, um die die beiden Uhrzeiten voneinander abweichen können, unendlich ist, wodurch sich Ihr Risiko für Replay-Angriffe erhöht.

e) Geben Sie in das Feld **Gültigkeitsdauer des gemeinsamen geheimen Schlüssels** die Anzahl der Tage ein, für die der gemeinsame geheime Schlüssel gültig ist.

f) Geben Sie in Millisekunden an, wie lange die Uhr des Clients und die Uhr des CMS höchstens für Anforderungen der vertrauenswürdigen Authentifizierung voneinander abweichen dürfen.

5. Klicken Sie auf **Aktualisieren**, um den gemeinsamen geheimen Schlüssel zu übermitteln.

Die BI-Plattform überwacht nicht alle Änderungen an Parametern der vertrauenswürdigen Authentifizierung. Sie müssen alle Informationen der vertrauenswürdigen Authentifizierung manuell sichern.

Der gemeinsame geheime Schlüssel wird von Client und CMS zum Einrichten der Vertrauenswürdigkeit verwendet. Als nächsten Schritt konfigurieren Sie den Client für die vertrauenswürdige Authentifizierung.

9.2.5 Konfiguration der vertrauenswürdigen Authentifizierung für Webanwendungen

Zum Konfigurieren der vertrauenswürdigen Authentifizierung für den Client müssen Sie die globalen Eigenschaften für die Datei `BOE.war` und spezifische Eigenschaften für die Anwendungen BI-Launchpad und OpenDocument ändern.

Verwenden Sie eine der folgenden Methoden, um den gemeinsamen geheimen Schlüssel dem Client zu übergeben:

- Option `WEB_SESSION`
- Datei `TrustedPrincipal.conf`

Verwenden Sie eine der folgenden Methoden, um den Benutzernamen dem Client zu übergeben:

- `REMOTE_USER`
- `HTTP_HEADER`
- `COOKIE`
- `QUERY_STRING`
- `WEB_SESSION`
- `USER_PRINCIPAL`

Unabhängig davon, wie Sie den gemeinsamen geheimen Schlüssel übergeben, muss die verwendete Methode in den globalen Eigenschaften `Trusted.auth.user.retrieval` für die Datei `BOE.war` angepasst werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.2.5.1 Verwenden der vertrauenswürdigen Authentifizierung für die SAML-Einzelanmeldung

Security Assertion Markup Language (SAML) ist ein XML-basierter Standard zur Übertragung von Identitätsdaten. SAML stellt eine sichere Verbindung zur Übertragung von Identitäten und Vertrauensstellungen bereit und liefert damit einen Einzelanmeldungsmechanismus, der vertrauenswürdigen Benutzern, die auf die BI-Plattform zugreifen möchten, zusätzliche Anmeldevorgänge erspart.

Aktivieren der SAML-Authentifizierung

Wenn der Anwendungsserver als SAML-Dienstprovider fungieren kann, können Sie der BI-Plattform über die vertrauenswürdige Authentifizierung die SAML-Einzelanmeldung bereitstellen.

Hierfür müssen Sie den Web-Anwendungsserver zunächst für die SAML-Authentifizierung konfigurieren.

Außerdem müssen Sie den Benutzernamen anhand einer dieser Methoden an den Client übergeben:

- `REMOTE_USER`
- `USER_PRINCIPAL`

Das Beispiel unten enthält eine Web.xml-Datei, die für die SAML-Authentifizierung konfiguriert ist.

```
<security-constraint>
      <web-resource-collection>
        <web-resource-name>InfoView</web-resource-name>
        <url-pattern>*</url-pattern>
      </web-resource-collection>
      <auth-constraint>
        <role-name>j2ee-admin</role-name>
        <role-name>j2ee-guest</role-name>
        <role-name>j2ee-special</role-name>
      </auth-constraint>
      <user-data-constraint>
        <transport-guarantee>NONE</transport-guarantee>
      </user-data-constraint>
    </security-constraint>
    <login-config>
      <auth-method>FORM</auth-method>
      <realm-name>InfoView</realm-name>
      <form-login-config>
        <form-login-page>/logon.jsp</form-login-page>
        <form-error-page>/logon.jsp</form-error-page>
      </form-login-config>
    </login-config>
    <security-role>
      <description>Assigned to the SAP J2EE Engine System Administrators</
description>
      <role-name>j2ee-admin</role-name>
    </security-role>
    <security-role>
      <description>Assigned to all users</description>
      <role-name>j2ee-guest</role-name>
    </security-role>
    <security-role>
      <description>Assigned to a special group of users</description>
      <role-name>j2ee-special</role-name>
    </security-role>
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Anweisungen hierzu entnehmen Sie der Dokumentation des Anwendungsservers, da der Vorgang von Anwendungsserver zu Anwendungsserver variiert.

Verwenden der vertrauenswürdigen Authentifizierung

Wenn der Anwendungsserver für die Rolle als SAML-Dienstprovider konfiguriert ist, können Sie über die vertrauenswürdige Authentifizierung die SAML-Einzelanmeldung bereitstellen.

> **Hinweis**
>
> Die Benutzer müssen entweder in die BI-Plattform importiert werden, oder benötigen Enterprise-Konten.

Zur Ermöglichung der Einzelanmeldung wird dynamisches Aliasing verwendet. Wenn ein Benutzer zum ersten Mal auf die Anmeldeseite über SAML zugreift, wird er aufgefordert, sich manuell mit seinen vorhandenen BI-Plattform-Kontoanmeldedaten anzumelden. Nachdem die Anmeldedaten des Benutzers überprüft wurden, verbindet das System anhand von Aliasing die SAML-Identität des Benutzers mit seinem BI-Plattform-Konto. Nachfolgende Anmeldeversuche des Benutzers werden anhand der Einzelanmeldung vorgenommen, da im System der Identitätsalias des Benutzers dynamisch mit einem vorhandenen Konto abgeglichen wird.

> **Hinweis**
>
> Damit dieser Mechanismus funktioniert, muss eine bestimmte Eigenschaft (`trusted.auth.user.namespace.enabled`) für die BOE.war-Datei aktiviert sein.

9.2.5.2 Eigenschaften der vertrauenswürdigen Authentifizierung für Webanwendungen

In der folgenden Tabelle sind die Einstellungen für die vertrauenswürdige Authentifizierung aufgeführt, die in der standardmäßigen `global.properties`-Datei für `BOE.war` enthalten sind. Um die Einstellungen zu überschreiben, erstellen Sie eine neue Datei in `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Eigenschaft	Standardwert	Beschreibung
`sso.enabled=true`	`sso.enabled=false`	Aktiviert und deaktiviert die Einzelanmeldung (SSO) bei der BI-Plattform. Setzen Sie diese Eigenschaft auf `true`, um die vertrauenswürdige Authentifizierung zu aktivieren.
`trusted.auth.shared.secret`	Keine	Sitzungsvariablenname, der zum Abruf des geheimen Schlüssels für die vertrauenswürdige Authentifizierung verwendet wird. Gilt nur, wenn die Websitzung zur Übergabe des geheimen Schlüssels verwendet wird.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Standardwert	Beschreibung
`trusted.auth.user.param`	Keine	Angeben der Variablen, mit deren Hilfe der Benutzername für die vertrauenswürdige Authentifizierung abgerufen wird.
`trusted.auth.user.retrieval`	Keine	Angeben der Methode, mit deren Hilfe der Benutzername für die vertrauenswürdige Authentifizierung abgerufen wird: • `REMOTE_USER` • `HTTP_HEADER` • `COOKIE` • `QUERY_STRING` • `WEB_SESSION` • `USER_PRINCIPAL` Um die vertrauenswürdige Authentifizierung zu deaktivieren, setzen Sie dies auf einen leeren Wert.
`trusted.auth.user.namespace.enabled`	Keine	Aktivieren und Deaktivieren der dynamischen Bindung von Aliasen an vorhandene Benutzerkonten. Wenn diese Eigenschaft auf `true` gesetzt ist, werden Benutzer von der vertrauenswürdigen Authentifizierung mithilfe der Aliasbindung bei der BI-Plattform authentifiziert. Mithilfe der Aliasbindung kann der Anwendungsserver als SAML-Dienstprovider fungieren und der vertrauenswürdigen Authentifizierung ermöglichen, dem System die SAML-Einzelanmeldung bereitzustellen. Wenn die Eigenschaft leer ist, verwendet die vertrauenswürdige Authentifizierung beim Authentifizieren von Benutzern den Namensabgleich.

9.2.5.3 Konfigurieren der vertrauenswürdigen Authentifizierung für die Webanwendung

Wenn Sie den gemeinsamen geheimen Schlüssel in der Datei `TrustedPrincipal.conf` speichern möchten, stellen Sie sicher, dass die Datei im geeigneten Plattformverzeichnis gespeichert ist:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Plattform	Speicherort von "TrustedPrincipal.conf"
Windows, Standardinstallation	• **<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\win32_x86\ • **<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\win64_x64\
AIX	**<INSTALLVERZ>**/sap_bobj/enterprise_xi40/ aix_rs6000/
Solaris	**<INSTALLVERZ>**/sap_bobj/enterprise_xi40/ solaris_sparc/
Linux	**<INSTALLVERZ>**/sap_bobj/enterprise_xi40/linux_x86

Mehrere Mechanismen füllen die Benutzernamevariable auf, mit der die vertrauenswürdige Authentifizierung für den Client konfiguriert wird, auf dem die Webanwendungen gehostet werden. Konfigurieren oder richten Sie den Webanwendungsserver so ein, dass Ihre Benutzernamen verfügbar gemacht werden, bevor Sie die Methoden zum Abrufen des Benutzernamens verwenden. Unter *http://java.sun.com/j2ee/1.4/docs/api/javax/servlet/http/HttpServletRequest.html* finden Sie weitere Informationen.

Zum Konfigurieren der vertrauenswürdigen Authentifizierung für den Client müssen Sie auf Eigenschaften für die Datei `BOE.war`, die allgemeine und spezifische Eigenschaften für die Webanwendungen BI-Launchpad und OpenDocument enthält, zugreifen und diese ändern.

> **Hinweis**
>
> Je nachdem, wie Sie den Benutzernamen oder den gemeinsamen geheimen Schlüssel abrufen möchten, sind eventuell weitere Schritte erforderlich.

1. Greifen Sie auf den Ordner "custom" für die Datei `BOE.war` auf dem Rechner zu, der die Webanwendungen hostet:

   <INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.

   Sie müssen die geänderte Datei `BOE.war` später erneut implementieren.
2. Erstellen Sie mit Editor oder einem anderen Textbearbeitungsprogramm eine neue Datei.
3. Geben Sie die folgenden Eigenschaften der vertrauenswürdigen Authentifizierung ein:

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=<Methode für Benutzer-ID-Abruf>
   trusted.auth.user.param=<Variable>
   trusted.auth.shared.secret=<WEB_SESSION>
   ```

   Wählen Sie für die Eigenschaft `trusted.auth.shared.secret` eine der folgenden Optionen zum Abrufen des Benutzernamens aus:

Option	Abrufmethode für den Benutzernamen
`HTTP_HEADER`	Der Benutzername wird aus dem Inhalt eines HTTP-Headers abgerufen. Sie geben in der Eigenschaft `trusted.auth.user.param` den HTTP-Header an, den Sie verwenden möchten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Abrufmethode für den Benutzernamen
`QUERY_STRING`	Der Benutzername wird aus einem Parameter der Anforderungs-URL abgerufen. Sie geben die zu verwendende Abfragezeichenfolge in der Eigenschaft `trusted.auth.user.param` an.
`COOKIE`	Der Benutzername wird aus einem angegebenen Cookie abgerufen. Sie geben das zu verwendende Cookie in der Eigenschaft `trusted.auth.user.param` an.
`WEB_SESSION`	Der Benutzername wird aus dem Inhalt einer angegebenen Sitzungsvariablen abgerufen. Sie geben die zu verwendende Websitzungsvariable in der Eigenschaft `trusted.auth.user.param` in `global.properties` an.
`REMOTE_USER`	Der Benutzername wird aus einem Aufruf von `HttpServletRequest.getRemoteUser()` abgerufen.
`USER_PRINCIPAL`	Der Benutzername wird abgerufen, indem ein Aufruf an `getUserPrincipal().getName()` im `HttpServletRequest`-Objekt ausgeführt wird, um die aktuelle Anforderung in einem Servlet oder JSP abzufragen.

Hinweis

Einige Webanwendungsserver setzen voraus, dass die Umgebungsvariable `REMOTE_USER` auf dem Server auf `true` gesetzt ist. Lesen Sie in der Dokumentation Ihres Webanwendungsserver nach, ob diese Einstellung erforderlich ist. Wenn sie erforderlich ist, bestätigen Sie, dass die Umgebungsvariable auf `true` gesetzt ist.

Hinweis

Wenn Sie den Benutzernamen mit `USER_PRINCIPAL` oder `REMOTE_USER` übergeben, lassen Sie `trusted.auth.user.param` leer.

4. Speichern Sie die Datei unter dem Namen `global.properties`.
5. Starten Sie den Webanwendungsserver neu.

Die neuen Eigenschaften werden erst wirksam, nachdem die geänderte BOE-Webanwendung erneut auf dem Rechner implementiert wird, auf dem der Webanwendungsserver ausgeführt wird. Implementieren Sie die WAR-Datei mit WDeploy erneut auf dem Webanwendungsserver. Weitere Informationen zum Umgang mit WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.2.5.3.1 Beispielkonfigurationen

9.2.5.3.1.1 Übergeben des gemeinsamen geheimen Schlüssels über die Datei TrustedPrincipal.conf

In der folgenden Beispielkonfiguration wird davon ausgegangen, dass ein Benutzer namens “JohnDoe” in der BI-Plattform erstellt wurde.

Die Benutzerinformationen werden gespeichert und über die Websitzung übergeben. Der gemeinsame geheime Schlüssel wird über die Datei `TrustedPrincipal.conf` übergeben, die sich standardmäßig im Verzeichnis `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` befindet. Die gebündelte Version von Tomcat ist der Webanwendungsserver.

1. Erstellen Sie mit dem Editor oder einem anderen Textbearbeitungsprogramm im Verzeichnis **`<INSTALLVERZ>`**`\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` eine neue Datei.
2. Geben Sie folgende Werte ein, um Eigenschaften der vertrauenswürdigen Authentifizierung anzugeben:

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=
```

3. Speichern Sie die Datei unter dem Namen **`global.properties`**.
4. Greifen Sie auf die Datei `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp` zu.
5. Ändern Sie den Inhalt der Datei, um folgende Werte einzuschließen:

```
<\!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html;charset=utf-8" %>
<%
//custom Java code
request.getSession().setAttribute("MyUser", "JohnDoe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript" src="noCacheCustomResources/myScript.js"></script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI
launch pad</a>
</body>
</html>
```

6. Erstellen Sie die Datei `myScript.js` im Verzeichnis `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources`.
7. Fügen Sie folgende Werte zu `myScript.js` hinzu:

```
function goToLogonPage() {
    window.location = "logon.jsp"; }
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8. Starten Sie den Webanwendungsserver neu.
9. Implementieren Sie die WAR-Datei mit WDeploy erneut auf dem Webanwendungsserver.

   Informationen zum Umgang mit WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen*.

Um zu überprüfen, ob Sie die vertrauenswürdige Authentifizierung korrekt konfiguriert haben, greifen Sie über folgende URL auf BI Launchpad zu: `http://<[CMS-Name]>:8080/BOE/BI/custom.jsp`, wobei **`<[CMS-Name]>`** der Name des Rechners ist, auf dem der CMS gehostet wird. Der folgende Link sollte angezeigt werden: `Klicken Sie auf diese Verknüpfung, um zur Anmeldeseite von BI-Launchpad zu gelangen.`

9.2.5.3.1.2 Übergeben des gemeinsamen geheimen Schlüssels über die Websitzungsvariable

In der folgenden Beispielkonfiguration wird davon ausgegangen, dass ein Benutzer namens **`<JohnDoe>`** in der BI-Plattform erstellt wurde.

Die Benutzerinformationen werden in der Websitzung gespeichert und von dieser übergeben, während der gemeinsame geheime Schlüssel über die Websitzungsvariable übergeben wird. Von dieser Datei wird angenommen, dass sie sich in folgendem Verzeichnis befindet: `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Sie müssen die Datei öffnen und sich den Inhalt notieren. In dieser Beispielkonfiguration wird davon ausgegangen, dass der gemeinsame geheime Schlüssel wie folgt lautet:

```
9ecb0778edcff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc65773
841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

Die gebündelte Version von Tomcat ist der Webanwendungsserver.

1. Greifen Sie auf das folgende Verzeichnis zu:

   `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`
2. Erstellen Sie eine neue Datei mit einem Texteditor.
3. Geben Sie die Eigenschaften der vertrauenswürdigen Authentifizierung an, indem Sie Folgendes eingeben:

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.user.param=MyUser
   trusted.auth.shared.secret=MySecret
   ```
4. Speichern Sie die Datei unter folgendem Namen:

   `global.properties`
5. Greifen Sie auf die folgende Datei zu:

   `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp`
6. Ändern Sie den Inhalt der Datei, um Folgendes zu berücksichtigen:

   ```
   <\!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
   "http://www.w3.org/TR/html4/loose.dtd">
   <%@ page language="java" contentType="text/html;charset=utf-8" %>
   <%
   ```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
//custom Java code
request.getSession().setAttribute("MySecret","9ecb0778edcff048edae0fcdde1a5db8211
2934
86774a127ec949c1bdb98dae8e0ea388979edc65773841c8ae5d1f675a6bf5d7c66038b6a3f1345
285b55a0a7"
request.getSession().setAttribute("MyUser", "JohnDoe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript" src="noCacheCustomResources/myScript.js"></script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI
launch pad</a>
</body>
</html>
```

7. Erstellen Sie die Datei `myScript.js` im folgenden Verzeichnis:

   `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources`

8. Fügen Sie Folgendes zu `myScript.js` hinzu:

```
function goToLogonPage() {
    window.location = "logon.jsp";
}
```

9. Starten Sie den Webanwendungsserver neu.
10. Implementieren Sie die WAR-Datei mit WDeploy erneut auf dem Webanwendungsserver.

    Informationen zum Umgang mit WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen*.

Um zu überprüfen, ob Sie die vertrauenswürdige Authentifizierung ordnungsgemäß konfiguriert haben, greifen Sie mithilfe der folgenden URL auf die Anwendung BI-Launchpad zu:`http://[cmsname]:8080/BOE/BI/custom.jsp`, wobei [cmsname] dem Namen des Rechners entspricht, auf dem der CMS gehostet wird. Die folgende Verknüpfung sollte angezeigt werden:
Klicken Sie auf diese Verknüpfung, um zur Anmeldeseite von BI-Launchpad zu wechseln.

9.2.5.3.1.3 Übergeben des Benutzernamens über den Benutzerprinzipalname

In der folgenden Beispielkonfiguration wird davon ausgegangen, dass ein Benutzer namens “JohnDoe” in der BI-Plattform erstellt wurde.

Die Benutzerinformationen werden gespeichert und über die Option "Benutzerprinzipalname" übergeben. Der gemeinsame geheime Schlüssel wird über die Datei `TrustedPrincipal.conf` übergeben, die sich standardmäßig im Verzeichnis `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` befindet. Die gebündelte Version von Tomcat ist der Webanwendungsserver.

1. Halten Sie den Tomcat-Server an.
2. Öffnen Sie die Datei `server.xml` für Tomcat, die sich standardmäßig im Verzeichnis `C:\Programme (x86)\SAP BusinessObjects\Tomcat\conf\` befindet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Suchen Sie `<Realm className="org.apache.catalina.realm.UserDatabaseRealm"..../>`, und ändern Sie den Wert in:

```
Realm className="orgapachecatalinarealmMemoryRealm".../
```

4. Öffnen Sie die Datei `tomcat-users.xml`, die sich standardmäßig im Verzeichnis `C:\Programme (x86)\SAP BusinessObjects\Tomcat\conf\` befindet.
5. Suchen Sie das Tag `<tomcat-users>`, und ändern Sie den folgenden Wert:

```
<user name="JohnDoe" password="password"
roles="onjavauser"/>
```

6. Öffnen Sie die Datei `web.xml` im Verzeichnis `C:\Programme (x86)\SAP BusinessObjects\Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.
7. Fügen Sie vor dem Tag `</web-app>` folgende Werte ein:

```
<security-constraint>
    <web-resource-collection>
         <web-resource-name>OnJavaApplication</web-resource-name>
         <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
         <role-name>onjavauser</role-name>
    </auth-constraint>
</security-constraint>

<login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>OnJava Application</realm-name>
</login-config>
```

   Geben Sie eine spezifische Seite für den Parameter `<url-pattern></url-pattern>` ein. Diese Seite sollte jedoch nicht die Standard-URL für BI-Launchpad oder eine andere Webanwendung sein.
8. Öffnen Sie die benutzerdefinierte Datei `global.properties`, und geben Sie folgende Werte ein:

```
trusted.auth.user.retrieval=USER_PRINCIPAL
trusted.auth.user.namespace.enabled=true
```

> **Hinweis**
>
> Die Einstellung `trusted.auth.user.namespace.enabled=true` ist optional. Fügen Sie den Parameter hinzu, wenn Sie einen externen Benutzernamen einem anderen BI-Plattform-Benutzernamen zuordnen möchten.

9. Starten Sie den Webanwendungsserver neu.
10. Implementieren Sie die WAR-Datei mit WDeploy erneut auf dem Webanwendungsserver.

    Informationen zum Umgang mit WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen*.

Bei Verwendung der Remotebenutzermethode sind diese Konfigurationen auf dem Webanwendungsserver die gleichen.

Um zu überprüfen, ob Sie die vertrauenswürdige Authentifizierung ordnungsgemäß konfiguriert haben, greifen Sie über die folgende URL auf die BI-Launchpad-Anwendung zu: `http:<//[cmsname]>:8080/BOE/BI`, wobei

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

`<[cmsname]>` der Name des Rechners ist, auf dem der CMS gehostet wird. Kurz darauf wird ein Anmeldedialogfeld angezeigt.

9.3 LDAP-Authentifizierung

9.3.1 Verwenden der LDAP-Authentifizierung

Dieser Abschnitt bietet eine allgemeine Beschreibung zur Funktionsweise der LDAP-Authentifizierung mit der BI-Plattform. Anschließend werden die Administrationstools eingeführt, mit denen LDAP-Benutzerkonten für die Plattform verwaltet und konfiguriert werden können.

Bei der Installation der BI-Plattform wird das LDAP-Authentifizierungs-Plugin automatisch installiert, jedoch nicht standardmäßig aktiviert. Wenn Sie die LDAP-Authentifizierung einsetzen möchten, müssen Sie zunächst sicherstellen, dass das entsprechende LDAP-Verzeichnis eingerichtet ist. Weitere Informationen hierzu finden Sie in der LDAP-Dokumentation.

LDAP (Lightweight Directory Access Protocol) ist ein gemeinsames, anwendungsunabhängiges Verzeichnis, das es Benutzern ermöglicht, Informationen zwischen verschiedenen Anwendungen auszutauschen und zu verwenden. LDAP basiert auf einem offenen Standard und ermöglicht den Zugriff und das Aktualisieren von Informationen in einem Verzeichnis.

LDAP basiert auf dem X.500-Standard, der mithilfe eines Verzeichniszugriffsprotokolls (DAP) eine Kommunikation zwischen einem Verzeichnisclient und einem Verzeichnisserver ermöglicht. LDAP ist eine Alternative zu DAP, da weniger Ressourcen eingesetzt werden, und einige Vorgänge und Funktionen von X.500 vereinfacht oder weggelassen werden.

In der Verzeichnisstruktur in LDAP sind Objekte in einem bestimmten Schema angeordnet. Jedes Objekt wird vom entsprechenden definierten Namen (DN) oder gemeinsamen Namen (CN) identifiziert. Andere oft verwendete Attribute sind der Organisationseinheitsname (OU) und der Organisationsname (O). Beispiel: Eine Mitgliedsgruppe hat folgende Stellung in der Verzeichnisstruktur: cn=BI-Plattform-Benutzer, ou=Enterprise-Benutzer A, o=Forschung. Nähere Informationen finden Sie in der LDAP-Dokumentation.

Da LDAP anwendungsunabhängig ist, kann jeder Client mit der entsprechenden Berechtigung auf die Verzeichnisse zugreifen. Mithilfe von LDAP können sich Benutzer über eine LDAP-Authentifizierung bei der BI-Plattform anmelden. Es stellt Benutzern Zugriffsrechte für Objekte im System zur Verfügung. Wenn ein oder mehrere LDAP-Server ausgeführt werden und Sie LDAP in den vorhandenen vernetzten Computersystemen einsetzen, können Sie die LDAP-Authentifizierung (zusammen mit der Enterprise- und AD-Authentifizierung) verwenden.

Das im Lieferumfang der BI-Plattform enthaltene LDAP-Sicherheits-Plugin kann auf Wunsch mit dem LDAP-Server über eine SSL-Verbindung kommunizieren, die per Serverauthentifizierung oder per gegenseitiger Authentifizierung hergestellt wurde. Bei der Serverauthentifizierung verfügt der LDAP-Server über ein Sicherheitszertifikat, das die BI-Plattform zur Überprüfung der Vertrauensstellung des Servers verwendet, während der LDAP-Server Verbindungen mit anonymen Clients ermöglicht. Bei gegenseitiger Authentifizierung verfügen sowohl LDAP-Server als auch die BI-Plattform über Sicherheitszertifikate, und der LDAP-Server muss außerdem das jeweilige Clientzertifikat überprüfen, bevor eine Verbindung aufgebaut werden kann.

Das im Lieferumfang der BI-Plattform enthaltene LDAP-Sicherheits-Plugin kann so konfiguriert werden, dass die Kommunikation mit dem LDAP-Server über SSL erfolgt und bei der Überprüfung der Anmeldeinformationen von Benutzern stets eine grundlegende Authentifizierung durchgeführt wird. Bevor Sie die LDAP-Authentifizierung mit

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

der BI-Plattform einsetzen, müssen Sie sich mit den Unterschieden zwischen den LDAP-Authentifizierungstypen vertraut machen. Ausführliche Informationen finden Sie in RFC2251 unter *http://www.faqs.org/rfcs/rfc2251.html* .

Weitere Informationen

Konfigurieren der LDAP-Authentifizierung [Seite 241]
Zuordnen von LDAP-Gruppen [Seite 251]

9.3.1.1 LDAP-Sicherheits-Plugin

Mit dem LDAP-Sicherheits-Plugin können Sie Benutzerkonten und Gruppen vom LDAP-Verzeichnisserver zur BI-Plattform zuweisen. Außerdem können alle Anmeldeanforderungen verifiziert werden, in denen die LDAP-Authentifizierung angegeben ist. Bevor der CMS eine aktive BI-Plattform-Sitzung gewährt, werden Benutzer auf dem LDAP-Verzeichnisserver authentifiziert, und ihre Mitgliedschaft in einer zugeordneten LDAP-Gruppe wird überprüft. Benutzerlisten und Gruppenmitgliedschaften werden dynamisch vom System verwaltet. Um die Sicherheit zu erhöhen, können Sie angeben, dass die Plattform mit dem LDAP-Verzeichnisserver über eine SSL-Verbindung (Secure Sockets Layer) kommunizieren soll.

Die LDAP-Authentifizierung für die BI-Plattform ähnelt der Windows-AD-Authentifizierung insofern, als Sie Gruppen zuordnen, Authentifizierung und Zugriffsrechte einrichten und Aliase erstellen können. Ebenso wie bei der NT- oder AD-Authentifizierung können Sie neue Enterprise-Konten für vorhandene LDAP-Benutzer erstellen und vorhandenen Benutzern LDAP-Aliase zuweisen, wenn die Benutzernamen den Enterprise-Benutzernamen entsprechen. Außerdem können Sie Folgendes tun:

- Zuordnen von Benutzern und Gruppen aus dem LDAP-Verzeichnisdienst.
- Zuordnen von LDAP gegen AD. Wenn Sie LDAP gegen AD konfigurieren, sind einige Einschränkungen zu berücksichtigen.
- Angeben mehrerer Hostnamen und deren Anschlüsse.
- Konfigurieren von LDAP mit SiteMinder

Nach der Zuordnung der LDAP-Benutzer und -Gruppen unterstützen alle BI-Plattform-Clienttools die LDAP-Authentifizierung. Sie können auch eigene Anwendungen erstellen, die LDAP-Authentifizierung unterstützen.

Weitere Informationen

Konfigurieren der SSL-Einstellungen für die LDAP-Serverauthentifizierung oder gegenseitige Authentifizierung [Seite 245]
Zuordnen von LDAP gegen Windows AD [Seite 253]
Konfigurieren des LDAP-Plugins für SiteMinder [Seite 250]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.3.2 Konfigurieren der LDAP-Authentifizierung

Um die Verwaltung zu vereinfachen, unterstützt die BI-Plattform die LDAP-Authentifizierung für Benutzer- und Gruppenkonten. Bevor sich Benutzer mit ihrem LDAP-Benutzernamen und -Kennwort beim System anmelden können, müssen Sie der BI-Plattform deren LDAP-Konten zuordnen. Beim Zuordnen eines LDAP-Kontos können Sie ein neues Konto oder eine Verknüpfung zu einem bestehenden BI-Plattform-Konto erstellen.

Bevor Sie die LDAP-Authentifizierung einrichten und aktivieren, stellen Sie sicher, dass das LDAP-Verzeichnis eingerichtet ist. Für nähere Informationen hierzu schlagen Sie in der LDAP-Dokumentation nach.

Die Konfiguration der LDAP-Authentifizierung umfasst die folgenden Schritte:

- Konfigurieren des LDAP-Hosts
- Vorbereiten des LDAP-Servers für SSL (wenn erforderlich)
- Konfigurieren des LDAP-Plugins für SiteMinder (wenn erforderlich)

> **Hinweis**
>
> Wenn Sie LDAP gegen AD konfigurieren, besteht die Möglichkeit, Benutzer zuzuordnen. Es ist jedoch nicht möglich, die AD-Einzelanmeldung bzw. Einzelanmeldung bei Datenbanken zu konfigurieren. Methoden für die LDAP-Einzelanmeldung wie SiteMinder und vertrauenswürdige Authentifizierung sind weiterhin verfügbar.

9.3.2.1 Konfigurieren des LDAP-Hosts

Es wird empfohlen, den LDAP-Server vor der Konfiguration des LDAP-Hosts zu installieren und auszuführen.

1. Wählen Sie in der Navigationsliste **Authentifizierung**, um in den Verwaltungsbereich der *Authentifizierung* der CMC zu navigieren.
2. Doppelklicken Sie auf **LDAP**.
3. Wenn Sie die LDAP-Authentifizierung zum ersten Mal einrichten, klicken Sie auf **Assistenten für LDAP-Konfiguration starten**.
4. Geben Sie den Namen und die Portnummer des LDAP-Hosts in das Feld **LDAP-Host hinzufügen (hostname:port)** ein (z.B. "meinserver:123"), klicken Sie auf **Hinzufügen** und dann auf **Weiter**.

   > **Tipp**
   >
   > Wiederholen Sie diesen Schritt, um weitere LDAP-Hosts des gleichen Servertyps hinzuzufügen, wenn Sie Hosts hinzufügen möchten, die als Server für Failover fungieren können. Wenn Sie einen Host entfernen möchten, markieren Sie den Hostnamen und klicken auf **Löschen**.

5. Wählen Sie aus der Liste **LDAP-Servertyp** den Servertyp aus.

   > **Hinweis**
   >
   > Wenn Sie LDAP zu AD zuordnen, wählen Sie **Microsoft Active Directory Application Server** als Servertyp.

6. Klicken Sie auf **Attributzuweisungen anzeigen**, wenn Sie die LDAP-Server-Attributzuweisungen oder die Standardattribute für die LDAP-Suche anzeigen oder ändern möchten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Standardmäßig sind die Server-Attributzuweisungen und Suchattribute jedes unterstützten Servertyps bereits eingestellt.

7. Klicken Sie auf **Weiter**.
8. Geben Sie im Feld **Definierter Name/Basis-LDAP** den definierten Namen (z.B. o=SomeBase) für den LDAP-Server ein, und klicken Sie auf **Weiter**.
9. Geben Sie im Bereich *Anmeldedaten für die LDAP-Serveradministration* den eindeutigen Namen und das Kennwort eines Benutzerkontos ein, das über Lesezugriff für das Verzeichnis verfügt.

   Administratoranmeldedaten sind nicht erforderlich.

   Wenn der LDAP-Server die anonyme Bindung zulässt, lassen Sie diesen Bereich leer. Die BI-Plattform-Server und -Clients führen über die anonyme Anmeldung eine Bindung an den primären Host aus.
10. Wenn Sie Weiterleitungen auf Ihrem LDAP-Host konfiguriert haben, geben Sie erst die Authentifizierungsinformationen in den Bereich *Anmeldedaten für die LDAP-Weiterleitung* und anschließend die Anzahl der Weiterleitungs-Hops in das Feld **Maximale Weiterleitungs-Hops** ein.

    Sie müssen den Bereich *Anmeldedaten für die LDAP-Weiterleitung* konfigurieren, wenn alle der folgenden Bedingungen zutreffen:

    - Der primäre Host wurde so konfiguriert, dass er auf einen anderen Verzeichnisserver verweist, der Anfragen für Einträge unter einer vorgegebenen Basis verarbeitet.
    - Der Host, auf den verwiesen wird, wurde so konfiguriert, dass anonyme Bindungen unzulässig sind.
    - Eine Gruppe des Hosts, auf den verwiesen wird, wird der BI-Plattform zugeordnet.

    > **Hinweis**
    >
    > Obwohl Gruppen von mehreren Hosts zugeordnet werden können, können die Anmeldedaten nur einmal festgelegt werden. Bei mehreren Hosts für die Weiterleitung müssen Sie auf jedem Host ein Benutzerkonto erstellen, auf dem der gleiche eindeutige Name und das gleiche Kennwort verwendet werden.

    > **Hinweis**
    >
    > Wenn **Maximale Weiterleitungs-Hops** auf Null gesetzt ist, werden keine Weiterleitungen verfolgt.
11. Klicken Sie auf **Weiter**.
12. Wählen Sie den Typ der verwendeten SSL-Authentifizierung (Secure Sockets Layer) aus:

    - **Standard (kein SSL)**
    - **Server-Authentifizierung**
    - **Gegenseitige Authentifizierung**

    Die Einzelheiten und Voraussetzungen für die Serverauthentifizierung und die gegenseitige Authentifizierung werden in einem nachfolgenden Abschnitt erläutert. Damit die Einrichtung der LDAP-Authentifizierung ungeachtet des verwendeten SSL-Typs erfolgreich verläuft, sollten Sie den Abschnitt *Konfigurieren der SSL-Einstellungen für die LDAP-Serverauthentifizierung oder gegenseitige Authentifizierung* in diesem Dokument durchlesen, bevor Sie die weiteren Schritte dieser Anweisung ausführen.
13. Klicken Sie auf **Weiter** und wählen die Methode der LDAP-Einzelanmeldungsauthentifizierung aus:

    - **Standard (nicht SSO)**
    - **SiteMinder**
14. Klicken Sie auf **Weiter**, und wählen Sie die Art der Zuordnung von Aliasen und Benutzern zu BI-Plattform-Konten aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

a) Wählen Sie unter *Optionen für neuen Alias* aus, wie neue Aliase Enterprise-Konten zugeordnet werden:

- **Jeden hinzugefügten LDAP-Alias einem Konto mit demselben Namen zuweisen**

  Verwenden Sie diese Option, wenn Sie wissen, dass einige Benutzer über ein Enterprise-Konto mit demselben Namen verfügen, d.h. vorhandenen Benutzern werden LDAP-Aliase zugewiesen (die automatische Generierung von Aliasen ist aktiviert). Benutzer ohne Enterprise-Konto oder mit unterschiedlichen Namen für das Enterprise- und das LDAP-Konto werden als neue Benutzer hinzugefügt.

- **Für jeden hinzugefügten LDAP-Alias ein neues Konto erstellen**

  Verwenden Sie diese Option, wenn Sie für jeden Benutzer ein neues Konto erstellen möchten.

b) Wählen Sie im Bereich *Aktualisierungsoptionen für Aliase* aus, wie Aliasaktualisierungen für die Enterprise-Konten verwaltet werden:

- **Neue Aliase bei der Aliasaktualisierung erstellen**

  Aktivieren Sie diese Option, um für jeden LDAP-Benutzer, der der BI-Plattform zugeordnet wurde, automatisch einen neuen Alias zu erstellen. Bei Benutzern ohne BI-Plattform-Konten oder bei Aktivierung der Option **Für jeden hinzugefügten LDAP-Alias ein neues Konto erstellen** werden neue LDAP-Konten für die Benutzer hinzugefügt.

- **Neue Aliase nur bei der Benutzeranmeldung erstellen**

  Aktivieren Sie diese Option, wenn das zuzuordnende LDAP-Verzeichnis viele Benutzer umfasst, von denen jedoch nur wenige die BI-Plattform verwenden werden. Aliase und Enterprise-Konten für alle Benutzer werden vom System nicht automatisch erstellt. Vielmehr werden Aliase (und ggf. Konten) nur für die Benutzer erstellt, die sich an der BI-Plattform anmelden.

c) Geben Sie im Bereich *Optionen für neue Benutzer* an, wie neue Benutzer erstellt werden:

- **Neue Benutzer werden als vordefinierte Benutzer erstellt**

  Neue Benutzerkonten werden für die Verwendung von Namenslizenzen konfiguriert. Namenslizenzen sind mit bestimmten Benutzern verbunden und ermöglichen den Zugriff auf das System auf der Grundlage von Benutzername und Kennwort. Dieser Lizenztyp ermöglicht Benutzern den Zugriff auf das System unabhängig von der Anzahl der derzeit verbundenen Benutzer. Für jedes mit dieser Option erstellte Benutzerkonto muss eine Namenslizenz verfügbar sein.

- **Neue Benutzer werden als gleichzeitige Benutzer erstellt**

  Neue Benutzerkonten werden für die Verwendung von Zugriffslizenzen konfiguriert. Zugriffslizenzen geben die Anzahl der Personen an, die gleichzeitig mit der BI-Plattform verbunden sein können. Dieser Lizenztyp ist sehr flexibel, da mit einer geringen Anzahl von Zugriffslizenzen viele Benutzer unterstützt werden können. Je nach Häufigkeit und Dauer des Zugriffs auf die Plattform können 100 Zugriffslizenzen beispielsweise 250, 500 oder auch 700 Benutzer unterstützen.

15. Führen Sie diesen Schritt aus, wenn Sie Benutzerattributzuweisungen einrichten oder E-Mail-Adressen von dem LDAP-Server importieren möchten. Legen Sie im Bereich *Optionen für die Attributbindung* die Attributbindungspriorität für das LDAP-Plugin fest:

    a) Aktivieren Sie **Vollständigen Namen, E-Mail-Adresse und andere Attribute importieren**.
    Die in den LDAP-Konten verwendeten vollständigen Namen und Beschreibungen werden importiert und mit den Benutzerobjekten im System gespeichert.

    b) Geben Sie eine Option für **Priorität der LDAP-Attributbindung im Verhältnis zu anderen Attributbindungen festlegen** an.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Wenn die Option auf 1 festgelegt ist, haben LDAP-Attribute immer dann Vorrang, wenn LDAP-Plugins und andere Plugins (Windows AD und SAP) aktiviert sind. Wenn die Option auf 3 festgelegt ist, haben Attribute von anderen aktivierten Plugins Priorität.

16. Klicken Sie auf **Fertig stellen** .

Weitere Informationen

Konfigurieren der SSL-Einstellungen für die LDAP-Serverauthentifizierung oder gegenseitige Authentifizierung [Seite 245]

Konfigurieren des LDAP-Plugins für SiteMinder [Seite 250]

9.3.2.2 Verwalten mehrerer LDAP-Hosts

Mithilfe von LDAP und der BI-Plattform können Sie das System um Fehlertoleranz erweitern, indem Sie mehrere LDAP-Hosts hinzufügen. Das System verwendet den ersten Host, den Sie hinzufügen, als primären LDAP-Host. Die weiteren Hosts werden als Hosts für Failover verwendet.

Der primäre LDAP-Host und alle Hosts für Failover müssen in genau gleicher Weise konfiguriert werden, und jeder LDAP-Host muss auf alle weiteren Hosts verweisen, von denen aus Gruppen zugeordnet werden sollen. Weitere Informationen zu LDAP-Hosts und Weiterleitungen finden Sie in der LDAP-Dokumentation.

Geben Sie beim Konfigurieren von LDAP mithilfe des Assistenten für die LDAP-Konfiguration alle Hosts ein, um mehrere LDAP-Hosts hinzuzufügen (weitere Informationen finden Sie unter). Wenn LDAP bereits konfiguriert wurde, wechseln Sie zum Verwaltungsbereich "Authentifizierung" der Central Management Console und klicken auf die Registerkarte "LDAP". Klicken Sie im Bereich "Eigenschaften der LDAP-Serverkonfiguration" auf den Namen des LDAP-Hosts, um die Seite zu öffnen, auf der Sie Hosts hinzufügen oder löschen können.

> **Hinweis**
>
> Fügen Sie zuerst den primären Host und dann die übrigen Hosts für Failover hinzu.

> **Hinweis**
>
> Wenn Sie LDAP-Hosts für Failover verwenden, kann die höchste SSL-Sicherheitsstufe nicht verwendet werden (also die Option "Serverzertifikat akzeptieren, wenn es von einer vertrauenswürdigen Zertifizierungsstelle stammt und das CN-Attribut des Zertifikats mit dem DNS-Hostnamen des Servers übereinstimmt" nicht ausgewählt werden).

Weitere Informationen

Konfigurieren der LDAP-Authentifizierung [Seite 241]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.3.2.3 Konfigurieren der SSL-Einstellungen für die LDAP-Serverauthentifizierung oder gegenseitige Authentifizierung

Dieser Abschnitt enthält ausführliche Informationen zur SSL-basierten Serverauthentifizierung bzw. gegenseitigen Authentifizierung für LDAP. Zur Einrichtung der SSL-basierten Authentifizierung sind vorbereitende Schritte auszuführen. In diesem Abschnitt wird außerdem im Einzelnen beschrieben, wie Sie SSL mit LDAP-Serverauthentifizierung und gegenseitiger Authentifizierung in der CMC konfigurieren. Es wird davon ausgegangen, dass Sie den LDAP-Host konfiguriert und dann eine der folgenden Optionen für die SSL-Authentifizierung ausgewählt haben:

Zusätzliche Informationen oder Konfigurationshinweise für den LDAP-Hostserver finden Sie in der Dokumentation Ihres LDAP-Anbieters.

Weitere Informationen

Konfigurieren des LDAP-Hosts [Seite 241]

9.3.2.3.1 Konfigurieren der LDAP-Serverauthentifizierung oder gegenseitigen Authentifizierung

Ressource	Diese Aktion vor Beginn dieser Aufgabe durchführen
CA-Zertifikat	Diese Aktion ist für die Server- und die gegenseitige Authentifizierung mit SSL erforderlich. 1. Rufen Sie eine Zertifizierungsstelle (Certificate Authority; CA) ab, um ein CA-Zertifikat zu generieren. 2. Fügen Sie das Zertifikat dem LDAP-Server hinzu. Informationen hierzu finden Sie in der Dokumentation des LDAP-Anbieters.
Serverzertifikat	Diese Aktion ist für die Server- und die gegenseitige Authentifizierung mit SSL erforderlich. 1. Fordern Sie ein Serverzertifikat an, und generieren Sie es dann. 2. Autorisieren Sie das Zertifikat, und fügen Sie es anschließend dem LDAP-Server hinzu.
cert7.db oder cert8.db, key3.db	Diese Dateien sind für die Server- und die gegenseitige Authentifizierung mit SSL erforderlich. 1. Laden Sie die Anwendung "certutil", die entweder die Datei `cert7.db` oder `cert8.db` generiert (je nach Anforderungen), von *https://developer.mozilla.org/en-US/docs/NSS/tools* herunter.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ressource	Diese Aktion vor Beginn dieser Aufgabe durchführen

	2. Kopieren Sie das CA-Zertifikat in dasselbe Verzeichnis wie die Anwendung "certutil".
	3. Generieren Sie die Dateien `cert7.db` oder `cert8.db`, `key3.db` und `secmod.db` mit dem folgenden Befehl:
	`certutil -N -d .`
	4. Fügen Sie das CA-Zertifikat mithilfe des folgenden Befehls der Datei `cert7.db` oder `cert8.db` hinzu:
	`certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer`
	5. Speichern Sie die drei Dateien in einem Verzeichnis auf dem Computer, der die BI-Plattform hostet.

cacerts	Diese Datei wird für die Server- oder gegenseitige Authentifizierung mit SSL für Java-Anwendungen wie BI-Launchpad benötigt. 1. Gehen Sie zur Datei `keytool` im Java-Verzeichnis `bin`. 2. Verwenden Sie den folgenden Befehl, um die Datei `cacerts` zu erstellen: `keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore` 3. Speichern Sie die Datei `cacerts` im selben Verzeichnis wie die Dateien `cert7.db` oder `cert8.db` und `key3.db`.
Clientzertifikat	1. Erstellen Sie eigene Clientanforderungen für die Dateien `cert7.db` oder `cert8.db` und `.keystore`: ○ Verwenden Sie zum Konfigurieren des LDAP-Plugins die Anwendung "certutil", um eine Clientzertifikatsanforderung zu generieren. ○ Generieren Sie die Clientzertifikatsanforderung mit folgendem Befehl: `certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .` `<client_dn>` enthält Informationen wie "CN=**<Clientname>**, OU=**<Org-Einheit>**, O=**<Name des Unternehmens>**, L=**<Ort>**, ST=**<Territorialeinheit>** und C=**<Land>**. 2. Authentifizieren Sie die Zertifikatsanforderung mithilfe der Zertifizierungsstelle. Rufen Sie das Zertifikat mithilfe

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ressource	Diese Aktion vor Beginn dieser Aufgabe durchführen

	des folgenden Befehls ab, und fügen Sie es in die Datei `cert7.db` oder `cert8.db` ein:
	`certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name>`
	3. Ermöglichen Sie die Java-Authentifizierung mit SSL:
	○ Generieren Sie mit dem keytool-Dienstprogramm im Java-Verzeichnis `bin` eine Clientzertifikatsanforderung.
	○ Generieren Sie mit folgendem Befehl ein Schlüsselpaar:
	`keytool -genkey -keystore .keystore`
	4. Nachdem Sie Informationen über Ihren Client angegeben haben, erzeugen Sie mithilfe des folgenden Befehls eine Clientzertifikatanforderung:
	`keytool -certreq -file <certificate_request_name> -keystore .keystore`
	5. Fügen Sie nach der Authentifizierung der Clientzertifikatsanforderung durch die Zertifizierungsstelle mit folgendem Befehl das CA-Zertifikat der Datei `.keystore` hinzu:
	`keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore`
	6. Rufen Sie die Clientzertifikatsanforderung aus der Zertifizierungsstelle ab, und fügen Sie sie mit folgendem Befehl der Datei `.keystore` hinzu:
	`keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore`
	7. Speichern Sie die Datei `.keystore` in demselben Verzeichnis wie die Dateien `cert7.db` oder `cert8.db` und `cacerts` auf dem Computer, der die BI-Plattform hostet.

1. Wählen Sie die zu verwendende SSL-Sicherheitsstufe.

   Wenn Sie den Assistenten für die LDAP-Konfiguration zum ersten Mal zur Konfiguration der LDAP-Authentifizierung verwenden, wählen Sie **Gegenseitige Authentifizierung** in der Liste *Typ der SSL-Authentifizierung*, und klicken Sie auf **Weiter**. Wenn Sie die Konfiguration der LDAP-Authentifizierung neu konfigurieren, navigieren Sie zum Bereich **Authentifizierung** der CMC, und doppelklicken Sie auf **LDAP**. Die Seite *Eigenschaften der LDAP-Serverkonfiguration* wird angezeigt. Klicken Sie auf den Wert **SSL-Typ**, und wählen Sie **Gegenseitige Authentifizierung** in der Liste *Typ der SSL-Authentifizierung*.

   ○ **Serverzertifikat immer akzeptieren**

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Hierbei handelt es sich um die Option mit der niedrigsten Sicherheitsebene. Bevor die der BI-Plattform eine SSL-Verbindung mit dem LDAP-Host (zum Authentifizieren von LDAP-Benutzern und -Gruppen) herstellen kann, muss ein vom LDAP-Host gesendetes Sicherheitszertifikat eingehen. Das erhaltene Zertifikat wird von der BI-Plattform nicht geprüft.

- **Serverzertifikat akzeptieren, wenn es von vertrauenswürdiger Zertifizierungsstelle stammt**

  Hierbei handelt es sich um die Option mit mittlerer Sicherheitsebene. Bevor die BI-Plattform eine SSL-Verbindung mit dem LDAP-Host (zum Authentifizieren von LDAP-Benutzern und Gruppen) herstellen kann, muss ein vom LDAP-Host gesendetes Sicherheitszertifikat vorliegen und überprüft werden. Zum Überprüfen des Zertifikats muss das System in der Zertifikatsdatenbank nach der ausstellenden Zertifizierungsstelle suchen.

- **Serverzertifikat akzeptieren, wenn es von vertrauenswürdiger Zertifizierungsstelle stammt und das CN-Attribut des Zertifikats mit dem DNS-Hostnamen des Servers übereinstimmt**

  Hierbei handelt es sich um die Option mit der höchsten Sicherheitsebene. Bevor die BI-Plattform eine SSL-Verbindung mit dem LDAP-Host (zum Authentifizieren von LDAP-Benutzern und Gruppen) herstellen kann, muss ein vom LDAP-Host gesendetes Sicherheitszertifikat vorliegen und überprüft werden. Zum Verifizieren des Zertifikats muss die BI-Plattform die Zertifizierungsstelle, die das Zertifikat ausgestellt hat, in ihrer Zertifikatsdatenbank finden und bestätigen können, dass das CN-Attribut auf dem Serverzertifikat genau mit dem LDAP-Hostnamen übereinstimmt, den Sie im ersten Schritt des Assistenten in das Feld **LDAP-Host hinzufügen** eingegeben haben, falls Sie den LDAP-Hostnamen als `ABALONE.rd.crystald.net:389` angegeben haben. (Die Verwendung von `CN =ABALONE:389` im Zertifikat funktioniert nicht.) .

  Der im Sicherheitszertifikat des Servers genannte Hostname entspricht dem Namen des primären LDAP-Hosts. Bei Aktivierung dieser Option kann kein LDAP-Host als Ausfallsicherung verwendet werden.

> **Hinweis**
>
> Bei Java-Anwendungen werden die erste und letzte Einstellung ignoriert. Das Serverzertifikat wird nur akzeptiert, wenn es von einer vertrauenswürdigen Zertifizierungsstelle ausgegeben wurde.

2. Geben Sie im Feld **SSL-Host** den Hostnamen der einzelnen Computer ein, und klicken Sie auf **Hinzufügen**.

   Anschließend geben Sie den Hostnamen jedes Computers in der BI-Plattform-Implementierung ein, der das BI-Plattform-SDK verwendet. (Dies betrifft den Computer, auf dem der Central Management Server ausgeführt wird, und den Computer, auf dem der Webanwendungsserver ausgeführt wird.)

3. Legen Sie die SSL-Einstellungen für jeden der Liste hinzugefügten SSL-Host fest:
   a) Wählen Sie aus der SSL-Liste die Option **Standard** aus.
   b) Deaktivieren Sie die Kontrollkästchen **Standardwert verwenden**.
   c) Geben Sie einen Wert in das Feld **Pfad zu den Zertifikats- und Schlüsseldatenbankdateien** und in das Feld **Kennwort für die Schlüsseldatenbank** ein.
   d) Wenn Sie Einstellungen für die gegenseitige Authentifizierung festlegen, geben Sie einen Wert in das Feld **Spitzname für das Clientzertifikat in der Zertifikatsdatenbank** ein.

> **Hinweis**
>
> Die Standardeinstellungen werden (für beliebige Hosts) immer dann verwendet, wenn das Kontrollkästchen **Standardwert verwenden** für einen Computer aktiviert ist, dessen Name der Liste der SSL-Hosts nicht hinzugefügt wird.

4. Legen Sie die Standardeinstellungen für jeden Host fest, der sich nicht in der Liste befindet, und klicken Sie auf **Weiter**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Um die Einstellungen für einen anderen Host anzugeben, wählen Sie den Hostnamen aus der Liste links aus und geben die Werte in die Felder auf der rechten Seite ein.

> **Hinweis**
>
> Die Standardeinstellungen werden (für beliebige Hosts) immer dann verwendet, wenn das Kontrollkästchen **Standardwert verwenden** für einen Computer aktiviert ist, dessen Name der Liste der SSL-Hosts nicht hinzugefügt wird.

5. Wählen Sie **Standard (nicht SSO)** oder **SiteMinder** als Methode der LDAP-Einzelanmeldungsauthentifizierung aus.
6. Wählen Sie aus, wie neue LDAP-Benutzer und -Aliase erstellt werden.
7. Klicken Sie auf **Fertig stellen**.

Weitere Informationen

Konfigurieren des LDAP-Plugins für SiteMinder [Seite 250]

9.3.2.4 Ändern der LDAP-Konfigurationseinstellungen

Nach dem Konfigurieren der LDAP-Authentifizierung mithilfe des Assistenten für die LDAP-Konfiguration können Sie auf der Seite *Eigenschaften der LDAP-Serverkonfiguration* die LDAP-Verbindungsparameter und Mitgliedsgruppen ändern.

1. Wechseln Sie zum Verwaltungsbereich **Authentifizierung** der CMC.
2. Doppelklicken Sie auf **LDAP**.

   Falls die LDAP-Authentifizierung konfiguriert ist, wird die Seite *Eigenschaften der LDAP-Serverkonfiguration* angezeigt. Auf dieser Seite können Sie sämtliche Verbindungsparameterbereiche oder -felder ändern und Optionen im Bereich *Zugeordnete LDAP-Mitgliedsgruppen* modifizieren.
3. Löschen Sie aktuell zugewiesene Gruppen, die unter den neuen Verbindungseinstellungen nicht mehr verfügbar sind, und klicken Sie auf **Aktualisieren**.

   Sie können zugewiesene Gruppen löschen, indem Sie die Benutzergruppe auswählen und dann auf die Schaltfläche **Löschen** im Abschnitt *Zugeordnete LDAP-Mitgliedsgruppen* klicken.
4. Ändern Sie die Verbindungseinstellungen, und klicken Sie auf **Aktualisieren**.
5. Ändern Sie die *Optionen für neuen Alias*, die *Aktualisierungsoptionen für Aliase* und die *Optionen für neue Benutzer*, falls erforderlich, und klicken Sie auf **Aktualisieren**.
6. Ordnen Sie die neuen LDAP-Mitgliedsgruppen zu, und klicken Sie auf **Aktualisieren**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.3.2.5 Konfigurieren des LDAP-Plugins für SiteMinder

In diesem Abschnitt wird erläutert, wie Sie die CMC für die Verwendung von LDAP mit SiteMinder konfigurieren. SiteMinder ist ein von einem Drittthersteller entwickeltes Benutzerzugriffs- und Authentifizierungstool, das mit dem LDAP-Sicherheits-Plugin verwendet werden kann, um die Einzelanmeldung bei der BI-Plattform einzurichten.

Um SiteMinder und LDAP mit der BI-Plattform zu verwenden, müssen an zwei Stellen Konfigurationseinstellungen vorgenommen werden:

- LDAP-Plugin über die CMC
- Eigenschaften der Datei `BOE.war`

> **Hinweis**
>
> Stellen Sie sicher, dass der SiteMinder-Administrator die Unterstützung für 4.x-Agenten aktiviert hat. Dies muss unabhängig von der unterstützten SiteMinder-Version geschehen, die Sie verwenden. Weitere Informationen zu SiteMinder sowie Installationshinweise finden Sie in der SiteMinder-Dokumentation.

Weitere Informationen

Konfigurieren des LDAP-Hosts [Seite 241]

9.3.2.5.1 Konfigurieren von LDAP für die Einzelanmeldung mit SiteMinder

1. Öffnen Sie den Bildschirm **Konfigurieren Sie Ihre SiteMinder-Einstellungen** mithilfe einer der folgenden Methoden:
   - Wählen Sie SiteMinder im Bildschirm *Wählen Sie eine Methode der LDAP-Einzelauthentifizierung* im Assistenten für die LDAP-Konfiguration aus.
   - Wählen Sie im Bildschirm für die LDAP-Authentifizierung, der verfügbar ist, wenn Sie LDAP bereits konfiguriert haben und nun SSO hinzufügen, die Verknüpfung **Einzelanmeldungstyp**.
2. Geben Sie im Feld **Richtlinienserver-Host** die Namen der einzelnen Richtlinienserver ein, und klicken Sie dann auf **Hinzufügen**.
3. Geben Sie für jeden Richtlinienserver-Host die Nummer für den **Accounting**-, **Authentifizierungs**- und **Autorisierungsanschluss** an.
4. Geben Sie den **Agentnamen** und **Gemeinsamen geheimen Schlüssel** ein. Geben Sie den gemeinsamen geheimen Schlüssel erneut im Feld *Gemeinsamen geheimen Schlüssel bestätigen* ein.
5. Klicken Sie auf **Weiter**.
6. Fahren Sie mit der Konfiguration der LDAP-Optionen fort.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.3.2.5.2 Aktivieren von LDAP und SiteMinder in der BOE.war-Datei

Neben der Angabe von SiteMinder-Einstellungen für das LDAP-Sicherheits-Plugin müssen SiteMinder-Einstellungen für die BOE.war-Eigenschaften angegeben werden.

1. Navigieren Sie zum Verzeichnis `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` in Ihrer BI-Plattform-Installation.
2. Erstellen Sie mit dem Editor oder einem anderen Textbearbeitungsprogramm eine neue Datei.
3. Geben Sie Folgendes ein:

```
siteminder.authentication=secLDAP
siteminder.enabled=true
```

4. Schließen Sie die Datei und speichern sie unter dem Namen **`global.properties`** ohne Dateierweiterung.
5. Erstellen Sie eine andere Datei im selben Verzeichnis.
6. Geben Sie Folgendes ein:

```
authentication.default=secLDAP
cms.default=[<your cms name>]:[<the CMS port number>]
```

   Beispiel:

```
authentication.default=secLDAP
cms.default=mycms:6400
```

7. Schließen Sie die Datei, und speichern Sie sie unter dem Namen `bilaunchpad.properties`.

Die neuen Eigenschaften werden erst wirksam, nachdem die geänderte BOE-Webanwendung erneut auf dem Rechner implementiert wird, auf dem der Webanwendungsserver ausgeführt wird. Implementieren Sie die WAR-Datei mit WDeploy erneut auf dem Webanwendungsserver. Informationen zum Umgang mit WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen*.

9.3.3 Zuordnen von LDAP-Gruppen

Nach dem Konfigurieren des LDAP-Hosts mithilfe des Assistenten für die LDAP-Konfiguration können Sie LDAP-Gruppen Enterprise-Gruppen zuordnen.

Nachdem Sie LDAP-Gruppen zugeordnet haben, können Sie sie anzeigen, indem Sie im Verwaltungsbereich **Authentifizierung** auf die Option "LDAP" klicken. Wenn die LDAP-Authentifizierung konfiguriert wurde, werden im Bereich "Zugeordnete LDAP-Mitgliedsgruppen" die LDAP-Gruppen angezeigt, die der BI-Plattform zugeordnet wurden.

> **Hinweis**
>
> Sie können auch Windows-AD-Gruppen zuordnen, die in der BI-Plattform über das LDAP-Sicherheits-Plugin authentifiziert werden sollen.

> **Hinweis**
>
> Falls Sie LDAP gegen AD konfiguriert haben, werden durch diese Schritte AD-Gruppen zugeordnet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Zuordnen von LDAP gegen Windows AD [Seite 253]

9.3.3.1 Zuordnen von LDAP-Gruppen mithilfe der BI-Plattform

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
2. Doppelklicken Sie auf **LDAP**.

   Nach dem Konfigurieren der LDAP-Authentifizierung wird die Seite mit der LDAP-Übersicht angezeigt.
3. Geben Sie im Bereich "*Zugeordnete LDAP-Mitgliedsgruppen*" im Feld **LDAP-Gruppe hinzufügen (cn oder dn)** Ihre LDAP-Gruppe ein – entweder den gemeinsamen Namen (CN) oder den definierten Namen (DN) – und klicken Sie auf **Hinzufügen**.

   Um mehrere LDAP-Gruppen hinzuzufügen, wiederholen Sie diesen Schritt. Wenn Sie eine LDAP-Gruppe entfernen möchten, markieren Sie sie, und klicken Sie auf **Löschen**.
4. Wählen Sie im Bereich *Optionen für neuen Alias* eine Option für die Zuordnung von LDAP-Aliasen zu Enterprise-Konten aus:
   - **Jeden hinzugefügten LDAP-Alias einem Konto mit demselben Namen zuweisen**

     Verwenden Sie diese Option, wenn Sie wissen, dass einige Benutzer über ein bereits vorhandenes Enterprise-Konto mit demselben Namen verfügen (d.h. vorhandenen Benutzern werden LDAP-Aliase zugewiesen – die automatische Generierung von Aliasen ist aktiviert). Benutzer ohne Enterprise-Konto oder mit unterschiedlichen Namen für das Enterprise- und das LDAP-Konto werden als neue LDAP-Benutzer hinzugefügt.
   - **Für jeden hinzugefügten LDAP-Alias ein neues Konto erstellen**

     Verwenden Sie diese Option, wenn Sie für jeden Benutzer ein neues Konto erstellen möchten.
5. Wählen Sie im Bereich *Aktualisierungsoptionen für Aliase* eine Option aus, um festzulegen, ob LDAP-Aliase automatisch für neue Benutzer erstellt werden:
   - **Neue Aliase bei der Aliasaktualisierung erstellen**

     Aktivieren Sie diese Option, um für jeden LDAP-Benutzer, der der BI-Plattform zugeordnet wurde, automatisch einen neuen Alias zu erstellen. Neue LDAP-Konten werden für Benutzer ohne BI-Plattform-Konto bzw. für alle Benutzer hinzugefügt, wenn Sie die Option **Für jeden hinzugefügten LDAP-Alias ein neues Konto erstellen** ausgewählt und auf **Aktualisieren** geklickt haben.
   - **Neue Aliase nur bei der Benutzeranmeldung erstellen**

     Aktivieren Sie diese Option, wenn das zuzuordnende LDAP-Verzeichnis viele Benutzer umfasst, von denen jedoch nur wenige die BI-Plattform verwenden werden. Aliase und Enterprise-Konten für alle Benutzer werden vom System nicht automatisch erstellt. Vielmehr werden Aliase (und ggf. Konten) nur für die Benutzer erstellt, die sich an der BI-Plattform anmelden.
6. Falls die Lizenz für Ihre BI-Plattform auf Benutzerrollen basiert, wählen Sie im Bereich *Optionen für neue Benutzer* eine Option aus, um die Eigenschaften für neue Enterprise-Konten festzulegen, die für die Zuordnung zu LDAP-Konten erstellt werden:
   - **Neue Benutzer werden als vordefinierte Benutzer erstellt**

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Neue Benutzerkonten werden für die Verwendung von Namenslizenzen konfiguriert. Namenslizenzen sind mit bestimmten Benutzern verbunden und ermöglichen den Zugriff auf das System auf der Grundlage von Benutzername und Kennwort. Dieser Lizenztyp ermöglicht Namenslizenzbenutzern den Zugriff auf das System, unabhängig von der Anzahl der derzeit verbundenen Benutzer. Für jedes mit dieser Option erstellte Benutzerkonto muss eine Namenslizenz verfügbar sein.

- **Neue Benutzer werden als gleichzeitige Benutzer erstellt**

  Neue Benutzerkonten werden für die Verwendung von Zugriffslizenzen konfiguriert. Zugriffslizenzen geben die Anzahl der Personen an, die gleichzeitig mit der BI-Plattform verbunden sein können. Dieser Lizenztyp ist sehr flexibel, da mit einer geringen Anzahl von Zugriffslizenzen viele Benutzer unterstützt werden können. Je nach Häufigkeit und Dauer des Zugriffs auf das System können 100 Zugriffslizenzen beispielsweise 250, 500 oder auch 700 Benutzer unterstützen.

7. Klicken Sie auf **Aktualisieren**.

9.3.3.2 Aufheben der Zuordnung von LDAP-Gruppen mithilfe der BI-Plattform

1. Wechseln Sie zum Verwaltungsbereich **Authentifizierung** der CMC.
2. Doppelklicken Sie auf **LDAP**.

   Nach dem Konfigurieren der LDAP-Authentifizierung wird die Seite mit der LDAP-Übersicht angezeigt.
3. Wählen Sie im Bereich Zugeordnete LDAP-Mitgliedsgruppen die LDAP-Gruppe aus, die entfernt werden soll.
4. Klicken Sie auf **Löschen** und dann auf **Aktualisieren**.

   Die Benutzer dieser Gruppe können nicht auf die BI-Plattform zugreifen.

   > **Hinweis**
   >
   > Die einzige Ausnahme besteht dann, wenn ein Benutzer über einen Alias für ein Enterprise-Konto verfügt. Um den Zugriff einzuschränken, deaktivieren oder löschen Sie das Enterprise-Konto des Benutzers.

Um die LDAP-Authentifizierung für alle Gruppen außer Kraft zu setzen, deaktivieren Sie das Kontrollkästchen "LDAP-Authentifizierung ist aktiviert", und klicken Sie auf **Aktualisieren**.

9.3.3.3 Zuordnen von LDAP gegen Windows AD

Beim Konfigurieren von LDAP gegen Windows AD gelten die folgenden Einschränkungen:

- Wenn Sie LDAP gegen AD konfigurieren, besteht die Möglichkeit, Benutzer zuzuordnen. Es ist jedoch nicht möglich, die AD-Einzelanmeldung bzw. Einzelanmeldung bei Datenbanken zu konfigurieren. Methoden für die LDAP-Einzelanmeldung wie SiteMinder und vertrauenswürdige Authentifizierung sind weiterhin verfügbar.
- Benutzer, die lediglich den AD-Standardgruppen angehören, können sich nicht anmelden. Benutzer müssen zusätzlich Mitglied einer anderen, explizit in AD erstellten Gruppe sein, die außerdem zugeordnet werden muss. Ein Beispiel für eine solche Gruppe ist die Gruppe "Domänenbenutzer".

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Wenn die einer Domäne zugeordnete lokale Gruppe einen Benutzer aus einer anderen Domäne im Forest enthält, kann sich der Benutzer, der aus einer anderen Domäne im Forest stammt, nicht erfolgreich anmelden.
- Benutzer aus einer universellen Gruppe, die einer anderen Domäne angehören als der als LDAP-Host definierte DC können sich nicht erfolgreich anmelden.
- Sie können das LDAP-Plugin nicht verwenden, um Benutzer und Gruppen aus AD-Forests zuzuordnen, die sich außerhalb des Forests befinden, in dem die BI-Plattform installiert ist.
- Sie können keine Zuordnung in der Gruppe "Domänenbenutzer" in AD vornehmen.
- Sie können keine lokale Gruppe auf einem Rechner zuordnen.
- Wenn Sie den Domänencontroller des globalen Katalogs verwenden, gelten für die Zuordnung von LDAP gegen AD zusätzliche Überlegungen:

Situation	Anmerkungen
Mehrere Domänen, wenn auf den Domänencontroller des globalen Katalogs verwiesen wird	Zulässige Zuordnungen: ○ universelle Gruppen in einer untergeordneten Domäne ○ Gruppen in derselben Domäne, die universelle Gruppen aus einer untergeordneten Gruppe enthält, und ○ universelle Gruppen in einer übergreifenden Domäne Nicht zulässige Zuordnungen: ○ globale Gruppen in einer untergeordneten Domäne ○ lokale Gruppen in einer untergeordneten Domäne ○ Gruppen in derselben Domäne, die eine globale Gruppe aus der untergeordneten Domäne enthalten, und ○ domänenübergreifende globale Gruppen Wenn es sich bei der Gruppe um eine universelle Gruppe handelt, unterstützt diese im Allgemeinen Benutzer aus übergreifenden oder untergeordneten Domänen. Andere Gruppen werden nicht zugeordnet, wenn sie Benutzer aus übergreifenden oder untergeordneten Domänen enthalten. Innerhalb der Domäne, auf die Sie verweisen, können Sie der Domäne lokale, globale und universelle Gruppen zuordnen.
Zuordnen in universellen Gruppen	Für die Zuordnung in universellen Gruppen verweisen Sie auf den Domänencontroller des globalen Katalogs. Darüber hinaus sollten Sie die Portnummer 3268 und nicht die Standardnummer 389 verwenden.

- Wenn Sie mehrere Domänen verwenden, aber nicht auf den Domänencontroller des globalen Katalogs verweisen, können Sie von übergreifenden oder untergeordneten Domänen keine Zuordnung zu einem Gruppentyp vornehmen. Sie können nur von der jeweiligen Domäne aus, auf die Sie verweisen, eine Zuordnung in alle Gruppentypen vornehmen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.3.3.4 Verwenden des LDAP-Plugins zur Konfiguration von SSO für die SAP-HANA-Datenbank

In diesem Abschnitt werden Administratoren über die für die Einrichtung und Konfiguration der Einzelanmeldung (SSO) zwischen der BI-Plattform, die unter SUSE Linux 11 ausgeführt wird, und der SAP-HANA-Datenbank erforderlichen Schritte informiert. Dank der LDAP-Authentifizierung mit Kerberos können AD-Benutzer auf einer BI-Plattform authentifiziert werden, die unter Linux ausgeführt wird, genauer gesagt SUSE. Dieses Szenario unterstützt auch die Einzelanmeldung an SAP HANA als Berichterstellungsdatenbank.

> **Hinweis**
>
> Informationen über das Einrichten der SAP-HANA-Datenbank finden Sie im *Serverinstallations- und Aktualisierungshandbuch für SAP-HANA-Datenbank*. Informationen über das Einrichten der Datenzugriffskomponente für SAP HANA finden Sie im *Datenzugriffshandbuch*.

Übersicht über die Implementierung

Folgende Komponenten sind erforderlich, damit die Kerberos-Einzelanmeldung funktioniert.

Komponente	Anforderung
Domänen-Controller	Muss auf einem Rechner gehostet werden, auf dem Active Directory für die Verwendung der Kerberos-Authentifizierung eingerichtet ist und ausgeführt wird.
Central Management Server	Muss auf einem Rechner, auf dem SUSE Linux Enterprise 11 (SUSE) ausgeführt wird, installiert sein und ausgeführt werden.
Kerberos-V5-Client	Muss zusammen mit den erforderlichen Dienstprogrammen und Bibliotheken auf dem SUSE-Host installiert sein. **Hinweis** Verwenden Sie die neueste Version des Kerberos-V5-Clients. Fügen Sie die Ordner `bin` und `lib` zu den Umgebungsvariablen `PATH` und `LD_LIBRARY_PATH` hinzu.
LDAP-Authentifizierungs-Plugin	Muss auf dem SUSE-Host aktiviert sein.
Kerberos-Anmeldekonfigurationsdatei	Muss auf dem Rechner erstellt werden, auf dem der Webanwendungsserver gehostet wird.

Workflow für die Implementierung

Folgende Aufgaben sind auszuführen, damit BI-Plattform-Benutzer unter Verwendung der Kerberos-Authentifizierung über JDBC die Einzelanmeldung an SAP HANA durchführen können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Einrichten des AD-Hosts.
2. Erstellen von Konten und Keytab-Dateien für den SUSE-Host und die BI-Plattform auf dem AD-Host.
3. Installieren der Kerberos-Ressourcen auf dem SUSE-Host.
4. Konfigurieren des SUSE-Hosts für die Kerberos-Authentifizierung.
5. Konfigurieren der Kerberos-Authentifizierung im LDAP-Authentifizierungsplugin.
6. Erstellen einer Kerberos-Anmeldekonfigurationsdatei für den Webanwendungshost.

9.3.3.4.1 Einrichten eines Domänencontrollers

Sie müssen möglicherweise eine Vertrauensstellung zwischen dem SUSE-Host und dem Domänencontroller einrichten. Befindet sich der SUSE-Host im Windows-Domänencontroller muss die Vertrauensstellung nicht eingerichtet werden. Befinden sich die BI-Plattform-Implementierung und der Domänencontroller dagegen in verschiedenen Domänen, kann die Einrichtung einer Vertrauensstellung zwischen dem SUSE-Linux-Rechner und dem Domänencontroller erforderlich sein. Sie müssen folgende Schritte ausführen:

1. Erstellen Sie ein Benutzerkonto für den SUSE-Rechner, auf dem die BI-Plattform ausgeführt wird.
2. Erstellen Sie einen Host-Dienstprinzipalnamen (SPN).

   Hinweis

   Formatieren Sie den SPN nach den Windows-AD-Konventionen: host/**<hostname>**@**<DNS_REALM_NAME>**. Verwenden Sie für /**<hostname>** einen vollqualifizierten Domänennamen in Kleinschreibung. Verwenden Sie für **<DNS_REALM_NAME>** Großschreibung.

3. Führen Sie den Keytab-Setup-Befehl `ktpass` von Kerberos aus, um den SPN dem Benutzerkonto zuzuordnen:

```
c:\> ktpass -princ host/<hostname>@<DNS_REALM_NAME>-mapuser <username> -pass
Password1 -crypto RC4-HMAC-NT -out <username>base.keytab
```

Führen Sie auf dem Rechner, auf dem der Domänencontroller gehostet wird, folgende Schritte aus:

1. Erstellen Sie ein Benutzerkonto für den Dienst, auf dem die BI-Plattform ausgeführt wird.
2. Klicken Sie auf der Seite *Benutzerkonten* mit der rechten Maustaste auf das neue Dienstkonto, und wählen Sie **Eigenschaften** > **Delegation** aus.
3. Wählen Sie **Benutzer bei Delegierungen aller Dienste vertrauen (nur Kerberos)**.
4. Führen Sie den Keytab-Setup-Befehl `ktpass` von Kerberos aus, um ein SPN-Konto für das neue Dienstkonto zu erstellen:

```
c:\>ktpass -princ <sianame>/<service_name>@<DNS_REALM_NAME> -mapuser
<service_name> -pass <password> -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT -
out <sianame>.keytab
```

   Hinweis

   Formatieren Sie den SPN nach den Windows-AD-Konventionen: sianame/**<dienstname>**@**<DNS_REALM_NAME>**. Geben Sie **<dienstname>** in Kleinbuchstaben an, da die SUSE-Plattform den Namen andernfalls vielleicht nicht auflösen kann. Verwenden Sie für **<DNS_REALM_NAME>** Großschreibung.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Beschreibung
-princ	Angeben des Prinzipalnamens für die Kerberos-Authentifizierung.
-out	Angeben des Namens der zu erzeugenden Kerberos-`Keytab`-Datei. Dieser sollte mit dem **`<sianame>`** übereinstimmen, der in *-princ* verwendet wurde.
-mapuser	Angeben des Namens des Benutzerkontos, dem der SPN zugeordnet ist. Der Server Intelligence Agent wird auf diesem Konto ausgeführt.
-pass	Gibt das vom Dienstkonto verwendete Kennwort an.
-ptype	Angeben des Prinzipaltyps: `-ptype KRB5_NT_PRINCIPAL`
-crypto	Angeben des für das Dienstkonto zu verwendenden Verschlüsselungstyps: `-crypto RC4-HMAC-NT`

Sie haben die erforderlichen Keytab-Dateien für die Vertrauensstellung zwischen dem SUSE-Rechner und dem Domänencontroller generiert.

Sie müssen die Keytab-Datei(en) zum SUSE-Rechner übertragen und im Verzeichnis `/etc` speichern.

9.3.3.4.2 Einrichten des SUSE-Linux-Enterprise-11-Rechners

Für die Einrichtung von Kerberos auf dem SUSE-Linux-Rechner, auf dem die BI-Plattform ausgeführt wird, sind folgende Ressourcen erforderlich:

- Auf dem Domänencontroller erstellte Keytab-Dateien. Die für den BI-Plattform-Dienst erstellte Keytab-Datei ist erforderlich. Die Keytab-Datei für den SUSE-Host ist besonders dann sinnvoll, wenn sich BI-Plattform-Host und Domänencontroller in verschiedenen Domänen befinden.
- Die neueste Kerberos-V5-Bibliothek (einschließlich Kerberos-Client) muss auf dem SUSE-Host installiert sein. Fügen Sie den Speicherort der Binärdateien zu den Umgebungsvariablen `PATH` und `LD_LIBRARY_PATH` hinzu. Um zu überprüfen, ob der Kerberos-Client ordnungsgemäß installiert und konfiguriert wurde, stellen Sie sicher, dass folgende Dienstprogramme und Bibliotheken auf dem SUSE-Host vorhanden sind:
  - `kinit`
  - `ktutil`
  - `kdestroy`
  - `klist`
  - `/lib64/libgssapi_krb5.so.2.2`
  - `/lib64/libkrb5.so.3.3`
  - `/lib/libkrb5support.so.0.1`
  - `/lib64/libk5crypto.so.3`
  - `/lib64/libcom_err.so.2`

> **Tipp**
>
> Führen Sie `rpm -qa | grep krb` aus, um die Version der Bibliotheken zu überprüfen. Weitere Informationen über den neuesten Kerberos-Client, Bibliotheken und die Unix-Host-Konfiguration finden Sie

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

unter *http://web.mit.edu/Kerberos/krb5-1.9/krb5-1.9.2/doc/krb5-install.html#Installing%20Kerberos%20V5* .

Wenn alle erforderlichen Ressourcen auf dem SUSE-Host verfügbar sind, folgen Sie den unten stehenden Anleitungen, um die Kerberos-Authentifizierung einzurichten.

Hinweis

Zur Ausführung dieser Schritte sind root-Privilegien erforderlich.

1. Um die Keytab-Dateien zusammenzuführen, führen Sie folgenden Befehl aus:

```
> ktutil
ktutil: rkt <susemachine>.keytab
ktutil: rkt <BI platform service>.keytab
ktutil: wkt /etc/krb5.keytab
ktutil:q
```

2. Bearbeiten Sie die Datei `/etc/kerb5.conf` so, dass sie auf den Domänencontroller (auf der Windows-Plattform) als Kerberos-Domänencontroller (KDC) verweist.

   Verwenden Sie folgendes Beispiel:

```
[domain_realm]
 .name.mycompany.corp = DOMAINNAME.COM
  name.mycompany.corp = DOMAINNAME.COM

[libdefaults]
        forwardable = true
           default_realm = DOMAINNAME.COM
           default_tkt_enctypes = rc4-hmac
           default_tgs_enctypes = rc4-hmac

[realms]
        DOMAINNAME.COM = {
             kdc = machinename.domainname.com
            }
```

   Hinweis

   Die Datei `krb5.conf` enthält Kerberos-Konfigurationsinformationen, z.B. Speicherorte der KDC und Server für die Kerberos-Bereiche, Kerberos-Anwendungen und Zuordnungen von Hostnamen zu Kerberos-Bereichen. Die Datei `krb5.conf` wird normalerweise im Verzeichnis `/etc` installiert.

3. Fügen Sie den Domänencontroller zu `/etc/hosts` hinzu, damit der SUSE-Host den KDC lokalisieren kann.
4. Führen Sie das Programm `kinit` über das Verzeichnis `/usr/local/bin` aus, um zu überprüfen, ob Kerberos ordnungsgemäß eingerichtet wurde. Überprüfen Sie, ob ein AD-Benutzerkonto sich am SUSE-Rechner anmelden kann.

   Tipp

   Der KDC stellt ein Ticket Granting Ticket (TGT) aus, das im Cache angezeigt werden kann. Zeigen Sie das TGT mithilfe des Programms `klist` an.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Beispiel

```
> kinit <AD user>
Password for <AD user>@<domain>: <AD user password>

> klist
Ticket cache: FILE:/tmp/krb5cc_0Default principal: <AD user>@<domain>
Valid starting Expires Service principal08/10/11 17:33:43 08/11/11 03:33:46
krbtgt/<domain>@<domain>renew until 08/11/11 17:33:43
Kerberos 4 ticket cache: /tmp/tkt0klist: You have no tickets cached

>klist -k
Keytab name: FILE:/etc/krb5.keytabKVNO Principal-3hdb/<FQDN>@<Domain>
```

Testen Sie die SPN außerdem mit `kinit`.

9.3.3.4.3 Konfigurieren der Kerberos-Authentifizierungsoptionen für LDAP

Bevor Sie die Kerberos-Authentifizierung für LDAP konfigurieren, aktivieren und konfigurieren Sie das LDAP-Authentifizierungsplugin der BI-Plattform so, dass eine Verbindung mit dem AD-Verzeichnis hergestellt wird. Wenn Sie die LDAP-Authentifizierung einsetzen möchten, stellen Sie zuerst sicher, dass das entsprechende LDAP-Verzeichnis eingerichtet ist.

Hinweis

Beim Ausführen des *Assistenten für die LDAP-Konfiguration* müssen Sie den **Microsoft Active Directory Application Server** angeben und die erforderlichen Konfigurationsdetails bereitstellen.

Nach Aktivierung der LDAP-Authentifizierung und Herstellung der Verbindung mit dem Microsoft Active Directory Application Server wird der Bereich *Kerberos-Authentifizierung aktivieren* auf der Seite "Eigenschaften der LDAP-Serverkonfiguration" angezeigt. Konfigurieren Sie in diesem Bereich die Kerberos-Authentifizierung, die für die Einzelanmeldung an der SAP-HANA-Datenbank über eine auf SUSE implementierte BI-Plattform erforderlich ist.

1. Wechseln Sie zum Verwaltungsbereich **Authentifizierung** der CMC.
2. Doppelklicken Sie auf **LDAP**.

   Die Seite *Eigenschaften der LDAP-Serverkonfiguration* wird angezeigt, auf der Sie die Verbindungsparameter oder -felder ändern können.
3. Führen Sie folgende Schritte im Bereich *Kerberos-Authentifizierung aktivieren* aus, um die Kerberos-Authentifizierung zu konfigurieren:
   a) Klicken Sie auf **Kerberos-Authentifizierung aktivieren**.
   b) Klicken Sie auf **Cachesicherheitskontext (für SSO bei Datenbank erforderlich)**.

   Hinweis

   Die Aktivierung des Cachesicherheitskontexts ist insbesondere für die Einzelanmeldung an SAP HANA erforderlich.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

c) Geben Sie den Dienstprinzipalnamen (SPN) für das BI-Plattform-Konto in *Dienstprinzipalname* an.

Das Format für die Angabe des SPN lautet **<sianame/dienst>**@**<DNS_REALM_NAME>**, wobei

<sianame>	Name des Server Intelligence Agent
<dienst >	Name des Dienstkontos, mit dem die BI-Plattform ausgeführt wird
DNS_REALM_NAME	Der Domänenname des Domänencontrollers (Großschreibung erforderlich)

> **Tipp**
>
> Beachten Sie, dass bei der Angabe des SPN, dass bei **<sianame/service>** die Groß-/Kleinschreibung berücksichtigt werden muss.

d) Geben Sie unter *Standardmäßiger Kerberos-Bereich* die Domäne für den Domänencontroller an.

e) Geben Sie `userPrincipalName` unter **Benutzerprinzipalname** an.

Mithilfe dieses Werts stellt die LDAP-Authentifizierungsanwendung Benutzer-ID-Werte bereit, die von Kerberos benötigt werden. Der angegebene Wert muss mit dem bei der Erstellung der Keytab-Dateien bereitgestellten übereinstimmen.

4. Klicken Sie auf **Aktualisieren**, um die Änderungen zu senden und zu speichern.

Sie haben die Kerberos-Authentifizierungsoptionen so konfiguriert, dass sie auf Benutzerkonten im AD-Verzeichnis verweisen.

Sie müssen eine Kerberos-Anmeldekonfigurationsdatei, `bscLogin.conf`, erstellen, um die Kerberos-Anmeldung und -Einzelanmeldung zu aktivieren.

Weitere Informationen

Konfigurieren der LDAP-Authentifizierung [Seite 241]

9.3.3.4.4 Erstellen von Konfigurationsdateien für die Kerberos-Anmeldung

Zur Aktivierung der Kerberos-Anmeldung mit Einzelanmeldung müssen Sie eine Anmeldekonfigurationsdatei auf dem Rechner hinzufügen, der den Webanwendungsserver der BI-Plattform hostet.

1. Erstellen Sie eine Datei namens `bscLogin.conf`, und speichern Sie sie im Verzeichnis `/etc`.

> **Hinweis**
>
> Sie können diese Datei an einem anderen Speicherort speichern. In diesem Fall muss der Speicherort jedoch in den Java-Optionen angegeben werden. Es empfiehlt sich, die Datei `bscLogin.conf` und die keytab-Datei von Kerberos im gleichen Verzeichnis zu speichern. In einer verteilten Implementierung muss die Datei `bscLogin.conf` für jeden Rechner hinzugefügt werden, der einen Webanwendungsserver hostet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Fügen Sie der Anmeldekonfigurationsdatei `bscLogin.conf` folgenden Code hinzu:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
com.businessobjects.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
storeKey=true
useKeyTab=true
keyTab="/etc/krb5.keytab"
principal="<principal name>";
};
```

> **Hinweis**
>
> Der folgende Abschnitt wird speziell für die Einzelanmeldung benötigt:
>
> ```
> com.businessobjects.security.jgss.accept {
> com.sun.security.auth.module.Krb5LoginModule required
> storeKey=true
> useKeyTab=true
> keyTab="/etc/krb5.keytab"
> principal="<principal name>";
> };
> ```

3. Speichern und schließen Sie die Datei.

9.3.3.5 Fehlerbehebung für neue LDAP-Konten

- Wenn Sie ein neues LDAP-Benutzerkonto erstellen und das Konto keinem Gruppenkonto angehört, das der BI-Plattform zugeordnet ist, ordnen Sie die Gruppe entweder zu oder fügen das neue LDAP-Benutzerkonto einer Gruppe hinzu, die dem System bereits zugeordnet ist.
- Wenn Sie ein neues LDAP-Benutzerkonto erstellen und das Konto einem Gruppenkonto angehört, das der BI-Plattform zugeordnet ist, aktualisieren Sie die Benutzerliste.

Weitere Informationen

Konfigurieren der LDAP-Authentifizierung [Seite 241]
Zuordnen von LDAP-Gruppen [Seite 251]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.4 Windows AD-Authentifizierung

9.4.1 Verwenden der Windows AD-Authentifizierung

9.4.1.1 Windows AD unterstützt Anforderungen und die Erstkonfiguration

In diesem Abschnitt wird der Prozess der Konfiguration der AD-Authentifizierung (Windows Active Directory) für die BI-Plattform erläutert. Es werden alle erforderlichen durchgängigen Workflows sowie die Validierungstests und vorab durchzuführende Überprüfungen beschrieben.

Voraussetzungen für die Unterstützung

Damit die AD-Authentifizierung auf der BI-Plattform möglich ist, sind die folgenden Voraussetzungen zu berücksichtigen.

- Der CMS muss immer auf einer unterstützten Windows-Plattform installiert werden.
- Obwohl es sich bei Windows 2008 und um unterstützte Plattformen sowohl für die Kerberos- als auch für die NTLM-Authentifizierung handelt, verwenden bestimmte BI-Plattform-Anwendungen unter Umständen nur bestimmte Authentifizierungsmethoden. Beispielsweise unterstützen Anwendungen wie BI-Launchpad und die Central Management Console nur Kerberos.

Empfohlener Workflow für die AD-Einrichtung

Um die manuelle AD-Authentifizierung mit der BI-Plattform anfänglich einzurichten, gehen Sie gemäß des folgenden Workflows vor:

1. Richten Sie den Domänencontroller ein.
2. Konfigurieren Sie die AD-Authentifizierung in der CMC.
3. Konfigurieren Sie das AD-Benutzerkonto auf dem Server Intelligence Agent (SIA).
4. Konfigurieren Sie den Webanwendungsserver für die AD-Authentifizierung mit Kerberos.

> **Hinweis**
>
> Verwenden Sie diesen Workflow ungeachtet dessen, ob Sie die Einzelanmeldung (SSO) benötigen. Der in den folgenden Abschnitten beschriebene Workflow ermöglicht Ihnen zunächst die manuelle Anmeldung an der BI-Plattform (mithilfe eines AD-Benutzernamens und -Kennworts). Nach der erfolgreichen Konfiguration der manuellen AD-Authentifizierung werden Sie in einem Abschnitt Schritt für Schritt durch die Einrichtung von SSO für die AD-Authentifizierung geführt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.4.2 Vorbereiten des Domänencontrollers

9.4.2.1 Einrichten eines Dienstkontos für die AD-Authentifizierung mit Kerberos

Um die BI-Plattform für die Windows-AD-Authentifizierung (Kerberos-Authentifizierung) zu konfigurieren, benötigen Sie ein Dienstkonto. Sie können entweder ein neues Domänenkonto erstellen oder ein vorhandenes verwenden. Das Dienstkonto wird zur Ausführung der BI-Plattform-Server verwendet. Nach Einrichtung des Kontos richten Sie einen SPN für das Konto ein. Mithilfe dieses SPN werden AD-Benutzergruppen in die BI-Plattform importiert.

> **Hinweis**
>
> Wenn Sie AD mit SSO verwenden möchten, müssen Sie später zur Einrichtung des Dienstkontos zurückkehren, um dem Konto entsprechende Rechte zu gewähren und dieses für die eingeschränkte Delegierung zu konfigurieren.

9.4.2.1.1 Einrichten eines Dienstkontos in einer Windows-2008-Domäne

Zur erfolgreichen Aktivierung der Windows AD-Authentifizierung mit dem Kerberos-Protokoll muss ein neues Dienstkonto eingerichtet werden. Dieses Dienstkonto wird primär dazu verwendet, Benutzern in einer bestimmten AD-Gruppe die Anmeldung an BI-Launchpad zu ermöglichen. Die folgende Aufgabe wird auf dem Rechner mit dem AD-Domänencontroller ausgeführt.

1. Erstellen Sie ein neues Dienstkonto mit Kennwort auf dem primären Domänencontroller.
2. Fügen Sie mit dem Befehl `setspn -a` die Dienstprinzipalnamen (Service Principal Names, SPNs) dem Dienstkonto hinzu, das Sie in Schritt 1 erstellt haben. Geben Sie die Dienstprinzipalnamen (SPNs) für das Dienstkonto sowie den Server, den voll qualifizierten Domänenserver und die IP-Adresse für den Rechner an, auf dem BI-Launchpad implementiert ist.
   Beispiel:

   ```
   setspn -a BICMS/service_account_name.domain.com serviceaccountname
   setspn -a HTTP/<Servername> <Servicename>
   setspn -a HTTP/<Servername.Domäne.com> <Servicename>
   setspn -a HTTP/<IP-Adresse des Servers> <Servicename>
   ```

   `BICMS` ist der Name des Rechners, auf dem der SIA ausgeführt wird, **`<Servername>`** ist der Name des Servers, auf dem BI-Launchpad implementiert ist, und **`<ServernameDomäne>`** ist der voll qualifizierte Domänenname.
3. Führen Sie `setspn -l` **`<servicename>`** aus, um zu prüfen, ob die Dienstprinzipalnamen zum Dienstkonto hinzugefügt wurden.
   Die Ausgabe des Befehls sollte alle registrierten SPNs umfassen, wie unten gezeigt:

   ```
   Registered ServicePrincipalNames for
   CN=bo.service,OU=boe,OU=BIP,OU=PG,DC=DOMAIN,DC=com:
   HTTP/<ip address of server>
   HTTP/<Servername>.DOMAIN.com
   ```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
HTTP/<Servername>
<Servername>/<Servicename>DOMAIN.com
```

Im Folgenden eine Beispielausgabe:

```
C:\Users\Admin>setspn -L bossosvcacct

Registered ServicePrincipalNames for
CN=bossosvcacct,OU=svcaccts,DC=domain,DC=com:
        BICMS/bossosvcacct.domain.com
        HTTP/Tomcat HTTP/Tomcat.domain.com
        HTTP/Load_Balancer.domain.com
```

Nach der Erstellung muss das Dienstkonto mit Rechten ausgestattet und zur lokalen Administratorgruppe des Servers hinzugefügt werden. Mit dem SPN werden im nächsten Abschnitt AD-Gruppen importiert.

9.4.3 Konfigurieren der AD-Authentifizierung in der CMC

9.4.3.1 Sicherheits-Plugin für Windows AD

Mit dem Windows-AD-Sicherheits-Plugin können Sie der BI-Plattform Benutzerkonten und -gruppen aus der AD-Benutzerdatenbank (Version 2008) zuordnen. Außerdem kann das System mithilfe dieses Plugins alle Anmeldeanforderungen überprüfen, für die die Windows AD-Authentifizierung festgelegt wurde. Bevor der Central Management Server (CMS) eine aktive Sitzung gewährt, werden Benutzer in der AD-Benutzerdatenbank authentifiziert, und ihre Zugehörigkeit zu einer zugeordneten AD-Gruppe wird überprüft. Sie können mit dem Plugin Aktualisierungen für die importierten AD-Gruppen konfigurieren.

Mit dem Windows AD-Sicherheits-Plugin können Sie Folgendes konfigurieren:

- Windows AD-Authentifizierung mit Kerberos
- Windows AD-Authentifizierung mit NTLM
- Windows AD-Authentifizierung mit SiteMinder für die Einzelanmeldung

Das AD-Sicherheits-Plugin ist kompatibel mit AD-2008-Domänen, die im systemeigenen oder im gemischten Modus betrieben werden.

Nach der Zuordnung der AD-Benutzer und -Gruppen können diese auf BI-Plattform-Clienttools über die **Windows-AD**-Authentifizierung zugreifen.

- Die Windows AD-Authentifizierung funktioniert nur, wenn der CMS unter Windows ausgeführt wird. Damit die Einzelanmeldung bei einer Datenbank funktioniert, müssen die Reporting-Server ebenfalls unter Windows ausgeführt werden. Ansonsten können alle anderen Server und Dienste auf sämtlichen Plattformen ausgeführt werden, die von der BI-Plattform unterstützt werden.
- Das Windows-AD-Plugin für die BI-Plattform unterstützt Domänen innerhalb mehrerer Forests.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.4.3.2 Zuordnen von Windows-AD-Benutzern und -Benutzergruppen

Bevor Sie AD-Benutzergruppen in die BI-Plattform importieren können, müssen folgende Voraussetzungen erfüllt sein:

- Ein Dienstkonto wurde auf dem Domänencontroller für die BI-Plattform erstellt. Das Konto wird zur Ausführung der BI-Plattform-Server verwendet.

  > **Hinweis**
  >
  > Um die AD-Authentifizierung mit Vintela-Einzelanmeldung (SSO) zu aktivieren, stellen Sie einen speziell für diesen Zweck konfigurierten SPN bereit. Mit den nachfolgenden Schritten wird die manuelle AD-Authentifizierung für die BI-Plattform konfiguriert. Nach Konfiguration der manuellen AD-Authentifizierung finden Sie im Abschnitt *Einrichten der Einzelanmeldung* in diesem Kapitel Einzelheiten zum Hinzufügen von SSO zur AD-Authentifizierungskonfiguration.

- Sie haben sich vergewissert, dass der SPN mit dem Namen des Rechners, auf dem der SIA ausgeführt wird, dem Dienstkonto hinzugefügt wurde.

Schritt 1 bis 11 unten sind obligatorisch zum Importieren von AD-Gruppen in die BI-Plattform.

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
2. Doppelklicken Sie auf **Windows AD**.
3. Aktivieren Sie das Kontrollkästchen **Windows Active Directory (AD) aktivieren**.
4. Klicken Sie im Bereich *Eigenschaften der AD-Konfiguration* auf den Link neben **AD-Verwaltungsname**.

   > **Hinweis**
   >
   > Wenn das Windows-AD-Plugin nicht konfiguriert wurde, werden anstelle des Links Anführungszeichen angezeigt. Nach dem Speichern der Konfiguration ist der Link mit AD-Verwaltungsnamen aufgefüllt.

5. Geben Sie Namen und Kennwort eines aktivierten Domänenbenutzerkontos ein.

   Bei den Anmeldedaten für die Verwaltung können die folgenden Formate verwendet werden:

   - NT-Name (`Domänenname\Benutzername`)
   - UPN (`Benutzer@DNS_Domänenname`)

   Die BI-Plattform verwendet dieses Konto, um Informationen von AD abzufragen. Es werden keine Inhalte in AD geändert, dort hinzugefügt oder daraus gelöscht. Die Informationen werden nur gelesen, sodass nur eine entsprechende Leseberechtigung erforderlich ist.

   > **Hinweis**
   >
   > Die AD-Authentifizierung wird abgebrochen, wenn das zum Lesen des AD-Verzeichnisses verwendete Konto ungültig wird (beispielsweise bei Änderung oder Ablauf des Kontokennworts bzw. Deaktivierung des Kontos).

6. Geben Sie die AD-Domäne in das Feld **Standard-AD-Domäne** ein.

   Die Domäne wird als VOLLSTÄNDIGER DOMÄNENNAME in GROSSBUCHSTABEN oder als untergeordneter Domänennamen angegeben, über den sich die meisten Benutzer an der BI-Plattform anmelden. Er sollte mit der Standarddomäne übereinstimmen, die in den Kerberos-Konfigurationsdateien, die zur Konfiguration des Anwendungsservers verwendet werden, angegeben ist. Sie können Gruppen aus der Standarddomäne

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

zuordnen, ohne das Präfix des Domänennamens anzugeben. Wenn der Standard-AD-Domänenname eingegeben wird, müssen Benutzer aus der Standarddomäne den AD-Domänennamen nicht mehr angeben, wenn sie sich über die AD-Authentifizierung an der BI-Plattform anmelden.

7. Geben Sie im Bereich *Zugeordnete AD-Mitgliedsgruppen* die AD-Domäne\-Gruppe unter Verwendung eines der folgenden Formate in das Feld **AD-Gruppe hinzufügen (Domäne\Gruppe)** ein:
   - Security Account Manager-Kontoname (SAM), der auch als NT-Name bezeichnet wird (`Domänenname\Gruppenname`)
   - DN (`cn=Gruppenname, ....., dc=Domänenname, dc=com`)

   Hinweis

   Wenn Sie eine lokale Gruppe zuordnen möchten, verwenden Sie dafür nur das NT-Namensformat: `\\<Servername>\<Gruppenname>`. AD unterstützt lokale Benutzer nicht. Lokale Benutzer, die zu einer zugeordneten lokalen Gruppe gehören, werden nicht der BI-Plattform zugeordnet. Daher können diese nicht auf das System zugreifen.

   Tipp

   Bei der manuellen Anmeldung an BI-Launchpad müssen Benutzer anderer Domänen den Domänennamen in Großbuchstaben an ihren Benutzernamen anhängen. Beispielsweise ist `CHILD.PARENTDOMAIN.COM` die Domäne in

   ```
   user@CHILD.PARENTDOMAIN.COM
   ```

8. Klicken Sie auf **Hinzufügen**.

   Die Gruppe wird der Liste unter *Zugeordnete AD-Mitgliedsgruppen* hinzugefügt.

9. Wählen Sie unter *Authentifizierungsoptionen* die Option **Kerberos-Authentifizierung verwenden**.
10. Geben Sie in das Feld **Dienstprinzipalname** den SPN ein, der dem Dienstkonto zugeordnet ist, das Sie zur Ausführung von BI-Plattform-Servern erstellt haben.

    Hinweis

    Sie müssen den SPN für das Dienstkonto angeben, das den SIA ausführt. Beispiel: `BICMS/bossosvcacct.domain.com`.

11. Klicken Sie auf **Aktualisieren**.

    Achtung

    Fahren Sie nicht fort, wenn Benutzer und/oder Gruppen nicht korrekt zugeordnet wurden. Informationen zur Lösung bestimmter Probleme bei der Zuordnung von AD-Gruppen finden Sie im SAP-Hinweis 1631734.

    Hinweis

    Wenn Sie AD-Gruppenkonten erfolgreich zugeordnet haben und keine AD-Authentifizierungsoptionen oder AD-Gruppen-Aktualisierungen konfigurieren möchten, überspringen Sie die Schritte 12 bis 19. Sie können diese optionalen Einstellungen konfigurieren, nachdem Sie die manuelle AD-Kerberos-Authentifizierung eingerichtet haben.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12. Wenn für die Konfiguration SSO bei einer Datenbank erforderlich ist, wählen Sie **Cachesicherheitskontext** aus.

> **Hinweis**
>
> Handelt es sich hierbei um die erste Konfiguration der AD-Authentifizierung, empfiehlt es sich, zuerst die manuelle AD-Authentifizierung erfolgreich einzurichten, bevor Sie die zusätzliche Konfiguration angehen, die für SSO erforderlich ist.

13. Wählen Sie **Einzelanmeldung für ausgewählten Authentifizierungsmodus aktivieren** aus, wenn SSO für die Konfiguration der AD-Authentifizierung erforderlich ist.
14. Wählen Sie im Bereich *Synchronisierung der Anmeldedaten* eine Option aus, um die Datenquellenanmeldedaten des AD-Benutzers zum Zeitpunkt der Anmeldung zu aktivieren und zu aktualisieren.

    Mit dieser Option wird die Datenquelle mit den aktuellen Anmeldedaten des Benutzers synchronisiert, sodass Berichte mit zeitgesteuerter Verarbeitung ausgeführt werden können, wenn der Benutzer nicht an der BI-Plattform angemeldet und Kerberos-SSO nicht verfügbar ist.
15. Geben Sie im Bereich *Optionen für AD-Aliase* an, wie neue Aliase der BI-Plattform hinzugefügt und auf dieser aktualisiert werden.
    a) Wählen Sie im Bereich *Optionen für neuen Alias* eine Option für die Zuordnung neuer Aliase zu Enterprise-Konten aus:
        - **Jeden neuen AD-Alias einem vorhandenen Benutzerkonto mit demselben Namen zuweisen**

          Wählen Sie diese Option aus, wenn Sie wissen, dass einige Benutzer über ein bereits vorhandenes Enterprise-Konto mit demselben Namen verfügen, d.h. vorhandenen Benutzern werden AD-Aliase zugewiesen (die automatische Generierung von Aliasen ist aktiviert). Benutzer ohne Enterprise-Konto oder mit unterschiedlichen Namen für das Enterprise- und das AD-Konto werden als neue Benutzer hinzugefügt.
        - **Neues Benutzerkonto für jeden neuen AD-Alias erstellen**

          Verwenden Sie diese Option, wenn Sie für jeden Benutzer ein neues Konto erstellen möchten.

    b) Wählen Sie im Bereich *Aktualisierungsoptionen für Aliase* eine Option für die Verwaltung von Aliasaktualisierungen für Enterprise-Konten aus:
        - **Neue Aliase bei der Aliasaktualisierung erstellen**

          Wählen Sie diese Option aus, um für jeden AD-Benutzer, der der BI-Plattform zugeordnet wurde, automatisch einen neuen Alias zu erstellen. Neue AD-Konten werden für Benutzer ohne BI-Plattform-Konten bzw. für alle Benutzer hinzugefügt, wenn Sie die Option **Neues Benutzerkonto für jeden neuen AD-Alias erstellen** ausgewählt und auf **Aktualisieren** geklickt haben.
        - **Neue Aliase nur bei der Benutzeranmeldung erstellen**

          Wählen Sie diese Option, wenn das zuzuordnende AD-Verzeichnis viele Benutzer umfasst, von denen jedoch nur wenige die BI-Plattform werden. Die Plattform erstellt nicht automatisch Aliase und Enterprise-Konten für alle Benutzer. Vielmehr werden Aliase (und ggf. Konten) nur für die Benutzer erstellt, die sich an der BI-Plattform anmelden.

    c) Wählen Sie im Bereich *Optionen für neue Benutzer* eine Option zum Erstellen neuer Benutzer aus:
        - **Neue Benutzer werden als vordefinierte Benutzer erstellt**

          Neue Benutzerkonten werden für die Verwendung von Namenslizenzen konfiguriert. Namenslizenzen sind mit bestimmten Benutzern verbunden und ermöglichen den Zugriff auf die BI-Plattform auf der

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Grundlage von Benutzername und Kennwort. Dieser Lizenztyp ermöglicht Namenslizenzbenutzern den Zugriff auf das System, unabhängig von der Anzahl der derzeit verbundenen Benutzer. Für jedes mit dieser Option erstellte Benutzerkonto muss eine Namenslizenz verfügbar sein.

- **Neue Benutzer werden als gleichzeitige Benutzer erstellt**

  Neue Benutzerkonten werden für die Verwendung von Zugriffslizenzen konfiguriert. Zugriffslizenzen geben die Anzahl der Personen an, die gleichzeitig mit der BI-Plattform verbunden sein können. Dieser Lizenztyp ist sehr flexibel, da mit einer geringen Anzahl von Zugriffslizenzen viele Benutzer unterstützt werden können. Je nach Häufigkeit und Dauer des Zugriffs auf das System können 100 Zugriffslizenzen beispielsweise 250, 500 oder auch 700 Benutzer unterstützen.

16. Klicken Sie auf **Zeitgesteuert verarbeiten**, um zu konfigurieren, wie AD-Aliasaktualisierungen zeitgesteuert verarbeitet werden.
    a) Wählen Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* ein Wiederholungsintervall aus der Liste **Objekt ausführen** aus.
    b) Legen Sie andere Optionen und Parameter der zeitgesteuerten Verarbeitung nach Bedarf fest.
    c) Klicken Sie auf **Zeitgesteuert verarbeiten**.
    Bei der Aliasaktualisierung werden auch die Gruppeninformationen aktualisiert.
17. Legen Sie im Bereich *Optionen für die Attributbindung* die Attributbindungspriorität für das AD-Plugin fest:
    a) Aktivieren Sie das Kontrollkästchen **Vollständigen Namen, E-Mail-Adresse und andere Attribute importieren**.
    Die in AD-Konten verwendeten vollständigen Namen und Beschreibungen werden importiert und mit Benutzerobjekten in der BI-Plattform gespeichert.
    b) Geben Sie eine Option für **Priorität der AD-Attributbindung im Verhältnis zu anderen Attributbindungen festlegen** an.

    Wenn die Option auf 1 festgelegt ist, haben AD-Attribute immer dann Vorrang, wenn AD-Plugins und andere Plugins (LDAP und SAP) aktiviert sind. Wenn die Option auf 3 festgelegt ist, haben Attribute von anderen aktivierten Plugins Priorität. Die Bindungen müssen auf unterschiedliche Werte festgelegt sein. Mehrere Authentifizierungs-Plugins auf denselben Bindungswert festzulegen kann zu unerwarteten Ergebnissen führen.
18. Konfigurieren Sie im Bereich *AD-Gruppenoptionen* AD-Gruppenaktualisierungen:
    a) Klicken Sie auf **Zeitgesteuert verarbeiten**.
    Das Dialogfeld *Zeitgesteuerte Verarbeitung* wird angezeigt.
    b) Wählen Sie ein Wiederholungsintervall aus der Liste **Objekt ausführen** aus.
    c) Legen Sie andere Optionen und Parameter der zeitgesteuerten Verarbeitung nach Bedarf fest.
    d) Klicken Sie auf **Zeitgesteuert verarbeiten**.

    Das System führt die zeitgesteuerte Verarbeitung der Aktualisierung gemäß den von Ihnen angegebenen Zeitsteuerungsinformationen aus. Die nächste zeitgesteuerte Aktualisierung für die AD-Gruppenkonten wird unter *AD-Gruppenoptionen* angezeigt.
19. Wählen Sie im Bereich *AD-Aktualisierung auf Abruf* eine der folgenden Optionen aus:

    - **AD-Gruppen jetzt aktualisieren**

      Wählen Sie diese Option aus, wenn beim Klicken auf **Aktualisieren** mit der Aktualisierung aller zeitgesteuerter AD-Gruppen begonnen werden soll. Die nächste zeitgesteuerte AD-Gruppenaktualisierung ist unter *AD-Gruppenoptionen* aufgeführt.
    - **AD-Gruppen und -Aliase jetzt aktualisieren**

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wählen Sie diese Option aus, wenn beim Klicken auf **Aktualisieren** mit der Aktualisierung aller zeitgesteuerter AD-Gruppen und -Benutzeraliase begonnen werden soll. Die nächsten zeitgesteuerten Aktualisierungen sind unter *AD-Gruppenoptionen* und *Optionen für AD-Aliase* aufgeführt.

- **AD-Gruppen und -Aliase jetzt nicht aktualisieren**

  Beim Klicken auf **Aktualisieren** werden keine AD-Gruppen oder -Benutzeraliase aktualisiert.

20. Klicken Sie auf **Aktualisieren** und dann auf **OK**.

Um zu überprüfen, ob AD-Benutzerkonten tatsächlich importiert wurden, navigieren Sie zu **CMC** > **Benutzer und Gruppen** > **Gruppenhierarchie** und wählen die zugeordnete AD-Gruppe aus, um Benutzer in dieser Gruppe anzuzeigen. Die aktuellen und verschachtelten Benutzer in der AD-Gruppe werden angezeigt.

Weitere Informationen

Erstellen von Kerberos-Konfigurationsdateien [Seite 274]

9.4.3.3 Zeitgesteuerte Aktualisierungen für Windows AD-Gruppen

Mit der BI-Plattform können Administratoren Aktualisierungen für AD-Gruppen und -Benutzeraliase zeitlich steuern. Diese Funktion ist für die AD-Authentifizierung mit Kerberos oder NTLM verfügbar. Über die CMC können Sie auch Uhrzeit und Datum der letzten Aktualisierung anzeigen lassen.

> **Hinweis**
>
> Damit die AD-Authentifizierung auf der BI-Plattform funktioniert, müssen Sie die zeitgesteuerte Verarbeitung von Aktualisierungen für Ihre AD-Gruppen und -Aliase konfigurieren.

Bei der zeitgesteuerten Verarbeitung einer Aktualisierung stehen Ihnen die Wiederholungsmuster in der folgenden Tabelle zur Verfügung:

Wiederholungsmuster	Beschreibung
Stündlich	Die Aktualisierung wird stündlich ausgeführt. Sie legen die Startzeit sowie Anfangs- und Enddatum für das Objekt fest.
Täglich	Die Aktualisierung wird täglich oder alle n angegebenen Tage ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum für das Objekt festlegen.
Wöchentlich	Die Aktualisierung wird wöchentlich ausgeführt. Es kann einmal die Woche oder mehrmals wöchentlich ausgeführt werden. Sie können festlegen, an welchen Tagen und zu welcher Uhrzeit das Objekt ausgeführt wird, und das Anfangs- und Enddatum der Ausführung bestimmen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wiederholungsmuster	Beschreibung
Monatlich	Die Aktualisierung wird einmal monatlich oder alle n Monate ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum für das Objekt festlegen.
Am n-ten Tag des Monats	Die Aktualisierung wird an einem bestimmten Tag des Monats ausgeführt. Sie können festlegen, an welchem Tag des Monats und zu welcher Uhrzeit die Aktualisierung ausgeführt wird, sowie Anfangs- und Enddatum der Ausführung bestimmen.
Am ersten Montag des Monats	Die Aktualisierung wird jeden Monat am ersten Montag ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am letzten Tag des Monats	Die Aktualisierung wird am letzten Tag jedes Monats ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am x-ten Tag der n-ten Woche des Monats	Die Aktualisierung wird an einem bestimmten Tag einer bestimmten Woche im Monat ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Kalender	Die Aktualisierung wird zu den Terminen ausgeführt, die in einem zuvor erstellten Kalender festgelegt wurden.

Zeitgesteuerte Verarbeitung von AD-Gruppenaktualisierungen

Die BI-Plattform ruft Benutzer- und Gruppeninformationen aus AD ab. Um die Menge der an AD gesendeten Abfragen zu minimieren, werden die Informationen über Gruppen, ihre Beziehung zueinander sowie deren Benutzermitgliedschaft vom AD-Plugin zwischengespeichert. Die Aktualisierung wird nicht ausgeführt, wenn kein bestimmter Zeitplan definiert wurde.

Über die CMC müssen Sie ein Wiederholungsintervall für die Regenerierung der Gruppenaktualisierung konfigurieren. Dies sollte zeitgesteuert verarbeitet werden, um die Häufigkeit der Änderungen der Gruppenzugehörigkeitsinformationen widerzuspiegeln.

Zeitgesteuerte Verarbeitung der Aktualisierung von AD-Benutzeraliasen

Benutzerobjekte können mit einem Alias für ein AD-Konto versehen werden, damit sich Benutzern mit ihren AD-Anmeldedaten an der BI-Plattform anmelden können. Aktualisierungen von AD-Konten werden über das AD-Plugin an die BI-Plattform propagiert. In AD erstellte, gelöschte oder deaktivierte Konten werden entsprechend in der BI-Plattform erstellt, gelöscht oder deaktiviert.

Wenn Sie keine Aktualisierungen von AD-Aliasen planen, werden Aktualisierungen nur in folgenden Fällen ausgeführt:

- Sobald sich ein Benutzer anmeldet, wird der AD-Alias aktualisiert.
- Der Administrator wählt die Option **AD-Gruppen und -Aliase jetzt aktualisieren** im Bereich **AD-Aktualisierung auf Abruf** der CMC aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Im Benutzeralias werden keine AD-Kennwörter gespeichert.

9.4.4 Konfigurieren des BI-Plattform-Diensts zur Ausführung des SIA

9.4.4.1 Ausführen des SIA unter dem Dienstkonto der BI-Plattform

Zur Unterstützung der AD-Kerberos-Authentifizierung für die BI-Plattform muss dem Dienstkonto das Recht gewährt werden, als Teil des Betriebssystems zu fungieren. Dies ist auf jedem Rechner erforderlich, auf dem ein Server Intelligence Agent (SIA) mit dem Central Management Server (CMS) ausgeführt wird.

Um dem Dienstkonto die Ausführung/das Starten des SIA zu ermöglichen, müssen bestimmte Betriebssystemeinstellungen konfiguriert werden, die in diesem Abschnitt beschrieben werden.

> **Hinweis**
>
> Wenn für die Datenbank die Einzelanmeldung erforderlich ist, muss der SIA folgende Server einschließen:
>
> - Crystal Reports Processing Server
> - Report Application Server
> - Web Intelligence Processing Server

9.4.4.2 Konfigurieren des SIA zur Ausführung unter dem Dienstkonto

Vor Konfiguration des SIA-Kontos zur Ausführung unter dem Dienstkonto der BI-Plattform müssen folgende Voraussetzungen erfüllt sein:

- Ein Dienstkonto wurde auf dem Domänencontroller für die BI-Plattform erstellt.
- Sie haben sich vergewissert, dass die erforderlichen Dienstprinzipalnamen (Service Principal Names, SPNs) dem Dienstkonto hinzugefügt wurden.
- AD-Benutzergruppen wurden der BI-Plattform erfolgreich zugeordnet.

Führen Sie folgende Schritte für jeden Server Intelligence Agent (SIA) aus, der Dienste ausführt, die vom Dienstkonto verwendet werden.

1. Um den CCM zu starten, wählen Sie **Programme** > **SAP BusinessObjects Business Intelligence 4** > **SAP BusinessObjects Business Intelligence** > **Central Configuration Manager** aus.
   Die CCM-Startseite wird geöffnet.
2. Klicken Sie im CCM mit der rechten Maustaste auf den Server Intelligence Agent (SIA), und wählen Sie **Stop**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Beim Stoppen des SIA werden auch alle vom SIA verwalteten Dienste gestoppt.

3. Klicken Sie mit der rechten Maustaste auf den SIA, und wählen Sie **Eigenschaften**.
4. Deaktivieren Sie das Kontrollkästchen **Systemkonto**.
5. Geben Sie die Dienstkonto-Anmeldedaten (`<DOMÄNENNAME>\<Dienstname>`) ein, und klicken Sie auf **OK**.

   Dem Dienstkonto müssen folgende Rechte auf dem Rechner, der den SIA ausführt, gewährt werden:

   - Dem Konto muss insbesondere das Recht "Einsetzen als Teil des Betriebssystems" zugewiesen sein.
   - Dem Konto muss insbesondere das Recht "Anmelden als Dienst" zugewiesen sein.
   - Volle Kontrollrechte für den Ordner, in dem die BI-Plattform installiert ist.
   - Volle Kontrollrechte für " HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects" in der Systemregistrierung.
6. Klicken Sie auf **Start > Systemsteuerung > Verwaltung > Lokale Sicherheitsrichtlinie**.
7. Erweitern Sie **Lokale Richtlinien**, und klicken Sie auf **Zuweisen von Benutzerrechten**.
8. Doppelklicken Sie auf **Als Teil des Betriebssystems handeln**.
9. Klicken Sie auf **Hinzufügen**, geben Sie den Namen des erstellten Dienstkontos ein, und klicken Sie auf **OK**.
10. Wiederholen Sie die oben aufgeführten Schritte auf jedem Rechner, auf dem ein BI-Plattform-Server ausgeführt wird.

> **Hinweis**
>
> Es ist wichtig, dass das effektive Recht zum Schluss aktiviert ist, nachdem die Option **Als Teil des Betriebssystems handeln** ausgewählt wurde. Normalerweise muss der Server zu diesem Zweck neu gestartet werden. Falls diese Option nach dem Neustart des Servers immer noch nicht aktiviert ist, werden Ihre Einstellungen der lokalen Richtlinie mit den Einstellungen der Domänenrichtlinie überschrieben.

11. Starten Sie den SIA neu.
12. Wiederholen Sie gegebenenfalls die Schritte 1 bis 5 für jeden SIA, auf dem ein zu konfigurierender Dienst ausgeführt wird.

Sie müssten nun in der Lage sein, sich am CCM mithilfe der AD-Anmeldedaten anzumelden.

9.4.4.3 Testen von AD-Anmeldedaten im CCM

Damit Sie diese Aufgabe ausführen können, muss der BI-Plattform eine AD-Benutzergruppe erfolgreich zugeordnet worden sein.

1. Öffnen Sie den CCM, und klicken Sie auf das Symbol **Server verwalten**.
2. Stellen Sie sicher, dass die im Feld *"System"* angezeigten Informationen richtig sind.
3. Wählen Sie aus der Liste "Authentifizierungsoptionen" die Option **Windows AD** aus.
   Ein Anmeldungsdialogfeld wird geöffnet.
4. Melden Sie sich mit einem vorhandenen AD-Konto aus der AD-Gruppe an, die Sie der BI-Plattform zugeordnet haben.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Wenn Sie ein AD-Konto verwenden, das sich nicht in der Standarddomäne befindet, melden Sie sich als `Domäne\Benutzername` an.

Sie dürften keine Fehlermeldungen erhalten. Die Anmeldung über den CCM mithilfe eines zugeordneten AD-Kontos muss möglich sein, bevor Sie mit dem nächsten Abschnitt weitermachen.

> **Tipp**
>
> Wenn Sie eine Fehlermeldung erhalten, navigieren Sie zu **CMC** > **Authentifizierung** > **Windows AD**. Ändern Sie unter *Authentifizierungsoptionen* **Kerberos-Authentifizierung verwenden** in **NTLM-Authentifizierung verwenden** und klicken auf **Aktualisieren**. Wiederholen Sie die Schritte 1 bis 4 oben. Falls dies funktioniert, gibt es ein Problem mit Ihrer Kerberos-Konfiguration.

9.4.5 Konfigurieren des Webanwendungsservers für die AD-Authentifizierung

9.4.5.1 Vorbereiten des Anwendungsservers für die Windows AD-Authentifizierung (Kerberos)

Der Prozess zur Konfiguration von Kerberos für einen Webanwendungsserver unterscheidet sich minimal für die einzelnen Anwendungsserver. Im Allgemeinen umfasst die Konfiguration von Kerberos jedoch folgende Schritte:

- Erstellen der Kerberos-Konfigurationsdatei (`krb5.ini`)
- Erstellen der Konfigurationsdatei `bscLogin.conf` für die JAAS-Anmeldung

> **Hinweis**
>
> Dieser Schritt ist für den SAP-NetWeaver-7.3-Java-Anwendungsserver nicht erforderlich. Sie müssen jedoch das Login-Modul dem SAP-NetWeaver-Server hinfügen.

- Ändern der Java-Optionen für den Anwendungsserver
- Überschreiben der Eigenschaften der Datei `BOE.war` für die Windows-AD-Authentifizierung.
- Neustarten des Java-Anwendungsservers

Dieser Abschnitt enthält die Einzelheiten zum Konfigurieren von Kerberos für die Verwendung mit folgenden Anwendungsservern:

- Tomcat
- WebSphere
- WebLogic
- Oracle Application Server
- SAP NetWeaver 7.3

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.4.5.1.1 Erstellen von Kerberos-Konfigurationsdateien

9.4.5.1.1.1 Erstellen von Kerberos-Konfigurationsdateien

Bevor Sie fortfahren, stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Ein Dienstkonto wurde auf dem Domänencontroller für die BI-Plattform erstellt.
- Sie haben sich vergewissert, dass die Dienstprinzipalnamen (Service Principal Names, SPNs) dem Dienstkonto hinzugefügt wurden.
- AD-Benutzergruppen wurden der BI-Plattform erfolgreich zugeordnet.
- Sie haben die AD-Anmeldedaten im CCM getestet.

Führen Sie folgende Schritte aus, um die Kerberos-Konfigurationsdatei zu erstellen, wenn Sie SAP NetWeaver 7.3, Tomcat, Oracle Application Server, WebSphere oder WebLogic als Webanwendungsserver für Ihre BI-Plattform-Implementierung verwenden.

1. Erstellen Sie die Datei `krb5.ini`, falls diese noch nicht vorhanden ist, und speichern Sie sie für Windows unter `C:\Windows`.

   Hinweis

   Wenn der Anwendungsserver unter UNIX installiert ist, verwenden Sie die folgenden Verzeichnisse:

   Solaris: `/etc/krb5/krb5.conf`

   Linux: `/etc/krb5.conf`

   Hinweis

   Sie können diese Datei auch an einem anderen Speicherort speichern; dieser Speicherort muss dann jedoch in den Java-Optionen angegeben werden. Weitere Informationen zu `krb5.ini` finden Sie unter *http://docs.sun.com/app/docs/doc/816-0219/6m6njqb94?a=view* .

2. Fügen Sie der Kerberos-Konfigurationsdatei die folgenden erforderlichen Informationen hinzu:

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
DOMAIN.COM =
}
```

Hinweis

Die Schlüsselparameter werden in der Tabelle unten erläutert.

`DOMAIN.COM`	Der DNS-Name der Domäne, der in Großbuchstaben im FQDN-Format eingegeben werden muss.
`kdc`	Der Hostname des Domänencontrollers.
`[capath]`	Definiert die Vertrauensstellung zwischen Domänen, die sich in einem anderen AD-Forest befinden. Im vorangehenden Beispiel entspricht `DOMAIN2.COM` einer Domäne in einem externen Forest und verfügt über eine direkte beidseitige transitive Vertrauenswürdigkeit zu `DOMAIN.COM`.
`default_realm`	In einer Konfiguration mit mehreren Domänen kann der Wert `default_realm` unter `[libdefaults]` einer beliebigen Quell-Domäne entsprechen. Am besten verwenden Sie die Domäne mit der größten Anzahl von Benutzern, die sich mit ihrem AD-Konto authentifizieren. Wenn während der Anmeldung kein UPN-Suffix angegeben wird, wird standardmäßig der Wert `default_realm` verwendet. Dieser Wert sollte mit der Einstellung für *Standarddomäne* in der CMC übereinstimmen. Alle Domänen müssen in Großbuchstaben angegeben werden, wie im Beispiel oben gezeigt.

9.4.5.1.2 Erstellen einer Konfigurationsdatei für die JAAS-Anmeldung

9.4.5.1.2.1 Erstellen einer Tomcat- oder WebLogic JAAS-Anmeldekonfigurationsdatei

Mit der Datei `bscLogin.conf` wird das Java-Login-Modul geladen. Sie ist für die AD-Kerberos-Authentifizierung auf Java-Webanwendungsservern erforderlich.

Die Datei wird standardmäßig unter `C:\Windows` gespeichert.

1. Erstellen Sie eine Datei namens `bscLogin.conf`, falls diese noch nicht vorhanden ist, und speichern Sie sie unter `C:\Windows`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Sie können diese Datei an einem anderen Speicherort speichern. In diesem Fall muss der Speicherort jedoch in den Java-Optionen angegeben werden.

2. Fügen Sie der JAAS-Konfigurationsdatei `bscLogin.conf` folgenden Code hinzu:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. Speichern und schließen Sie die Datei.

9.4.5.1.2.2 Erstellen von Konfigurationsdateien für die Oracle-JAAS-Anmeldung

1. Suchen Sie die Datei `jazn-data.xml`.

> **Hinweis**
>
> Der Standardspeicherort für diese Datei ist `C:\OraHome_1\j2ee\home\config`. Wenn Sie Oracle Application Server an einem anderen Speicherort installiert haben, suchen Sie die Datei für Ihre jeweilige Installation.

2. Fügen Sie der Datei zwischen den `<jazn-loginconfig>`-Tags folgenden Inhalt hinzu:

```
<application>
<name>com.businessobjects.security.jgss.initiate</name>
<login-modules>
<login-module>
<class>com.sun.security.auth.module.Krb5LoginModule</class>
<control-flag>required</control-flag>
</login-module>
</login-modules>
</application>
```

3. Speichern und schließen Sie die Datei `jazn-data.xml`.

9.4.5.1.2.3 Erstellen von Konfigurationsdateien für die WebSphere JAAS-Anmeldung

1. Erstellen Sie eine Datei mit dem Namen `bscLogin.conf`, falls noch nicht vorhanden, und speichern Sie sie am Standardspeicherort `C:\Windows`.
2. Fügen Sie der Konfigurationsdatei `bscLogin.conf` folgenden Code hinzu:

```
com.businessobjects.security.jgss.initiate {
com.ibm.security.auth.module.Krb5LoginModule required;
};
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Speichern und schließen Sie die Datei.

9.4.5.1.2.4 Hinzufügen eines Login-Moduls zu SAP NetWeaver

Um Kerberos und SAP NetWeaver 7.3 zu verwenden, konfigurieren Sie das System so, als ob Sie den Tomcat-Webanwendungsserver verwenden würden. Sie brauchen die Datei `bscLogin.conf` nicht zu erstellen.

Anschließend fügen Sie ein Login-Modul hinzu und aktualisieren einige Java-Einstellungen auf SAP NetWeaver 7.3.

Um `com.businessobjects.security.jgss.initiate` das Login-Modul `com.sun.security.auth.module.Krb5LoginModule` zuzuordnen, müssen Sie NetWeaver manuell ein Login-Modul hinzufügen.

1. Öffnen Sie den NetWeaver-Administrator, indem Sie die folgende Adresse in den Webbrowser eingeben: `http://<Rechnername>:<Port>/nwa`.
2. Klicken Sie auf **Configuration Management** > **Security** > **Authentication** > **Login Modules** > **Edit** (Konfigurationsmanagement > Sicherheit >Authentifizierung >Login-Module > Bearbeiten).
3. Fügen Sie ein neues Login-Modul mit folgenden Informationen hinzu:

Anzeigename	**`Krb5LoginModule`**
Klassenname	**`com.sun.security.auth.module.Krb5LoginModule`**

4. Klicken Sie auf **Speichern**.
   NetWeaver erstellt das neue Modul.
5. Klicken Sie auf **Komponenten** > **Bearbeiten**.
6. Fügen Sie eine neue Richtlinie mit der Bezeichnung **`com.businessobjects.security.jgss.initiate`** hinzu.
7. Fügen Sie im *Authentication Stack (Login-Modul-Stack)* das in Schritt 3 erstellte Login-Modul hinzu, und setzen Sie es auf **Required (Erforderlich)**.
8. Überprüfen Sie, ob es weitere Einträge unter *Options for Selected Login Module (Optionen für ausgewähltes Login-Modul)* gibt. Falls ja, löschen Sie sie.
9. Klicken Sie auf **Speichern**.
10. Melden Sie sich vom NetWeaver-Administrator ab.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.4.5.1.3 Ändern der Java-Einstellungen des Anwendungsservers zum Laden von Konfigurationsdateien

9.4.5.1.3.1 So ändern Sie Java-Optionen für Kerberos unter Tomcat

1. Wählen Sie im Menü **Start** die Option **Programme >Tomcat > Tomcat-Konfiguration**.
2. Klicken Sie auf die Registerkarte **Java**.
3. Fügen Sie die folgenden Optionen hinzu:

```
-Djava.security.auth.login.config=C:\XXXX\bscLogin.conf
-Djava.security.krb5.conf=C:\XXXX\krb5.ini
```

   Ersetzen Sie XXXX durch den Speicherort der Datei `bscLogin.conf`.
4. Schließen Sie die Tomcat-Konfigurationsdatei.
5. Starten Sie Tomcat neu.

9.4.5.1.3.2 Ändern der Java-Optionen für SAP NetWeaver 7.3

1. Navigieren Sie zum Java-Konfigurationstool (befindet sich standardmäßig unter `C:\usr\sap\<NetWeaver-ID>\<Instanz>\j2ee\configtool\`), und doppelklicken Sie auf `configtool.bat`.
   Das Konfigurationstool wird geöffnet.
2. Klicken Sie auf **View** > **Expert Mode** (Ansicht > Expertenmodus).
3. Klappen Sie **Cluster-Data** > **Template** (Clusterdaten > Vorlage) auf.
4. Wählen Sie die Instanz aus, die dem NetWeaver-Server entspricht (zum Beispiel **Instance (Instanz) - `<System-ID><Rechername>`**).
5. Klicken Sie auf **VM Parameters** (VM-Parameter).
6. Wählen Sie **SAP** aus der Liste **Vendor** (Anbieter) und **GLOBAL** aus der Liste **Platform** (Plattform) aus.
7. Klicken Sie auf **System**, und fügen Sie folgende benutzerdefinierten Parameterinformationen hinzu:

java.security.krb5.conf	**`<Pfad zur Datei "krb5.ini" einschließlich Dateiname>`**
javax.security.auth.useSubjectCredsOnly	false

8. Klicken Sie auf **Save** (Speichern) und anschließend auf **Configuration Editor** (Konfigurationseditor).
9. Klicken Sie auf **Configurations** > **Security** > **Configurations** > **com.businessobjects.security.jgss.initiate** > **Security** > **Authentication** (Konfigurationen > Sicherheit > Konfigurationen > com.businessobjects.securtiy.jgss.initiate > Sicherheit > Authentifizierung).
10. Klicken Sie auf **Edit Mode** (Bearbeitungsmodus).
11. Klicken Sie mit der rechten Maustaste auf den Knoten **Authentication** (Authentifizierung), und wählen Sie **Create sub-node** (Unterknoten erstellen) aus.
12. Wählen Sie **Value-Entry** (Werteingabe) aus der oberen Liste aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

13. Geben Sie Folgendes ein:

Name	create_security_session
Wert	false

14. Klicken Sie auf **Create** (Erstellen), und schließen Sie anschließend das Fenster.
15. Klicken Sie auf **Config Tool** (Konfigurationstool) und dann auf **Speichern**.

Nachdem Sie die Konfiguration aktualisiert haben, müssen Sie den NetWeaver-Server neu starten.

9.4.5.1.3.3 So ändern Sie Java-Optionen für Kerberos unter WebLogic

Wenn Sie Kerberos mit WebLogic verwenden, müssen Ihre Java-Optionen geändert werden, um den Speicherort der Kerberos-Konfigurationsdatei und des Kerberos-Anmeldemoduls anzugeben.

1. Stoppen Sie die WebLogic-Domäne, in der die BI-Plattform-Anwendungen ausgeführt werden.
2. Öffnen Sie das Skript, mit dem die Domäne von WebLogic gestartet wird, auf der die BI-Plattform-Anwendungen ausgeführt werden (`startWeblogic.cmd` für Windows, `startWebLogic.sh` für Unix).
3. Fügen Sie im Abschnitt "Java_Options" der Datei die folgenden Informationen hinzu.

   ```
   set JAVA_OPTIONS=-Djava.security.auth.login.config=C:/XXXX/bscLogin.conf
   -Djava.security.krb5.conf=C:/XXX/krb5.ini
   ```

   Ersetzen Sie XXXX durch den Speicherort der Datei.
4. Starten Sie die Domäne von WebLogic erneut, in der die BI-Plattform-Anwendungen ausgeführt werden.

9.4.5.1.3.4 So ändern Sie Java-Optionen für Kerberos unter Oracle Application Server

Wenn Sie Kerberos mit Oracle Application Server verwenden, müssen die Java-Optionen geändert werden, um den Speicherort der Kerberos-Konfigurationsdatei anzugeben.

1. Melden Sie sich an der Administrationskonsole von Oracle Application Server an.
2. Klicken Sie auf den Namen der OC4J-Instanz, die die BI-Plattform-Anwendungen ausführt.
3. Wählen Sie **Server Properties**(Servereigenschaften) aus.
4. Führen Sie einen Bildlauf nach unten zum Abschnitt "Multiple VM Configuration" (Mehrere VM-Konfigurationen) aus.
5. Hängen Sie im Abschnitt "Command Line Options" (Befehlszeilenoptionen) Folgendes an das Ende des Textfelds *"Java Options"* (Java-Optionen) an: `-Djava.security.krb5.conf=C:/XXXX/krb5.ini`. Dabei wird XXXX durch den Speicherort der Datei ersetzt.
6. Starten Sie die OC4J-Instanz neu.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.4.5.1.3.5 So ändern Sie Java-Optionen für Kerberos unter WebSphere

1. Melden Sie sich bei der Verwaltungskonsole für WebSphere an.

   Geben Sie für IBM WebSphere 5.1 `http://Servername:9090/admin` ein. Geben Sie für IBM WebSphere 6.0 `http://Servername:9060/ibm/console` ein.
2. Klappen Sie "Server" auf, klicken Sie auf **Application Servers** (Anwendungsserver) und dann auf den Namen des Anwendungsservers, den Sie für die Verwendung mit der BI-Plattform erstellt haben.
3. Wechseln Sie zur *JVM*-Seite.

   Wenn Sie WebSphere 5.1 verwenden, rufen Sie die *JVM*-Seite anhand der folgenden Schritte auf.

   1. Führen Sie auf der Serverseite einen Bildlauf nach unten aus, bis **Process Definition** (Prozessdefinition) in der Spalte **Additional Properties** (Weitere Eigenschaften) angezeigt wird.
   2. Klicken Sie auf **Prozessdefinition**.
   3. Führen Sie einen Bildlauf nach unten aus, und klicken Sie auf **Java Virtual Machine**.

   Wenn Sie WebSphere 6.0 verwenden, rufen Sie die *JVM*-Seite anhand der folgenden Schritte auf.

   1. Wählen Sie auf der Serverseite **Java and Process Management (Java und Prozessmanagement)**.
   2. Wählen Sie **Process Definition**.
   3. Wählen Sie **Java Virtual Machine**.
4. Klicken Sie auf **Generic JVM arguments** (Generische JVM-Argumente), und geben Sie den Speicherort der Dateien `Krb5.ini` und `bscLogin.conf` ein.

   -Djava.security.auth.login.config=C:\XXXX\bscLogin.conf

   -Djava.security.krb5.conf=C:\XXXX\krb5.ini

   Ersetzen Sie XXXX durch den Speicherort der Datei.
5. Klicken Sie auf **Anwenden** und anschließend auf **Speichern**.
6. Stoppen und starten Sie den Server neu.

9.4.5.1.4 Verifizieren des Empfangs von Kerberos-Tickets bei Java

Bevor Sie testen können, ob Java das Kerberos-Ticket empfangen hat, müssen folgende Aktionen ausgeführt werden:

- Erstellen Sie die Datei `bscLogin.conf` für den Anwendungsserver.
- Erstellen Sie die Datei `krb5.ini`.

1. Navigieren Sie über die Befehlseingabeaufforderung zum Verzeichnis `jdk\bin` in der BI-Plattform-Installation.

   Standardmäßig befindet sich dieses unter `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\jdk\bin`.
2. Führen Sie *kinit <Benutzername>* aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Drücken Sie die *Eingabetaste*.
4. Geben Sie das Kennwort ein.
   Wenn die Datei `krb5.ini` richtig konfiguriert und das Java-Login-Modul geladen wurde, müsste eine Meldung mit ungefähr folgendem Wortlaut angezeigt werden:
   In der Cache-Datei "C:\Users\Administrator\krb5cc_Administrator" wurde ein neues Ticket gespeichert.

Fahren Sie mit der AD-Einrichtung erst dann fort, wenn ein Kerberos-Ticket erfolgreich eingegangen ist.

Wenn Sie kein Ticket erhalten, haben Sie folgende Möglichkeiten:

- Konsultieren Sie die Abschnitt "Fehlerbehebung" am Ende dieses Kapitels.
- Wenn es bei den Problemen um KDC, die Kerberos-Konfigurationsdateien und Benutzeranmeldedaten geht, die in der Kerberos-Datenbank nicht verfügbar sind, lesen Sie die Artikel KBA 1476374 und KBA 1245178 der SAP Knowledge Base durch.

9.4.5.1.5 Konfigurieren von BI-Launchpad für die manuelle AD-Anmeldung

Vor der Konfiguration Ihrer BI-Plattform-Anwendungen für die manuelle AD-Anmeldung müssen folgende Voraussetzungen erfüllt sein:

- Ein Dienstkonto wurde auf dem Domänencontroller für die BI-Plattform erstellt.
- Sie haben sich vergewissert, dass die erforderlichen HTTP-Dienstprinzipalnamen (Service Principal Names, SPNs) dem Dienstkonto hinzugefügt wurden.
- AD-Benutzergruppen wurden der BI-Plattform erfolgreich zugeordnet.
- Sie haben die AD-Anmeldedaten im CCM getestet.
- Sie haben die erforderlichen Konfigurationsdateien für den Webanwendungsserver erstellt, konfiguriert und getestet.
- Die Java-Einstellungen des Anwendungsservers wurden so geändert, dass die Konfigurationsdateien geladen werden.

Führen Sie zum Aktivieren der Windows AD-Authentifizierungsoption für BI-Launchpad folgende Schritte aus:

1. Greifen Sie auf den benutzerdefinierten Ordner der BOE-Webanwendung auf dem Rechner zu, der den Webanwendungsserver hostet:

   `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Nehmen Sie die Änderungen im Verzeichnis `config\custom` und nicht im Verzeichnis `config\default` vor. Ansonsten werden die Änderungen überschrieben, wenn Sie zukünftige Patches auf die Implementierung anwenden.

   Die geänderte BOE-Webanwendung muss zu einem späteren Zeitpunkt erneut implementiert werden.
2. Erstellen Sie eine neue Datei.

   > **Hinweis**
   >
   > Verwenden Sie Notepad oder ein anderes Textbearbeitungsprogramm.

3. Speichern Sie die Datei unter dem Namen `BIlaunchpad.properties`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Geben Sie Folgendes ein:

```
authentication.visible=true
authentication.default=secWinAD
```

5. Speichern und schließen Sie die Datei.
6. Starten Sie Ihren Webanwendungsserver neu.

Sie sollten nun in der Lage sein, sich manuell an BI-Launchpad anzumelden. Rufen Sie eine der Anwendungen auf, und wählen Sie "Windows AD" aus der Liste der Authentifizierungsoptionen aus.

> **Hinweis**
>
> Fahren Sie mit der Windows-AD-Einrichtung erst dann fort, wenn Sie sich mithilfe eines vorhandenen AD-Kontos an BI-Launchpad anmelden können.

Die neuen Eigenschaften werden erst wirksam, wenn die BOE-Webanwendung auf dem Rechner, auf dem der Webanwendungsserver ausgeführt wird, erneut implementiert wird. Verwenden Sie WDeploy zur erneuten Implementierung von BOE auf dem Webanwendungsserver. Weitere Informationen zur Verwendung von WDeploy zur Deinstallation von Webanwendungen finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.

> **Hinweis**
>
> Wenn Ihre Implementierung eine Firewall verwendet, öffnen Sie alle erforderlichen Ports, da die Webanwendungen sonst keine Verbindung mit den BI-Plattform-Servern herstellen können.

9.4.6 Einrichten der Einzelanmeldung

9.4.6.1 SSO bei der BI-Plattform mit AD-Authentifizierung

Optionen für SSO bei Verwendung von Windows AD

Zur Einrichtung der Einzelanmeldung (SSO) für die Windows-AD-Authentifizierung mit der BI-Plattform stehen zwei unterstützte Methoden zur Verfügung:

- Vintela – diese Option kann nur mit Kerberos verwendet werden.
- SiteMinder – diese Option kann nur mit Kerberos verwendet werden.

SSO bei der Datenbank

SSO bei der Datenbank ermöglicht angemeldeten Benutzern die Ausführung von Aktionen, die Datenbankzugriff erfordern. Dazu gehören vor allem das Anzeigen und Regenerieren von Berichten, ohne erneut Anmeldedaten eingeben zu müssen. Während die eingeschränkte Delegierung für die AD-Authentifizierung mit Vintela-SSO optional ist, ist sie für Implementierungsszenarios erforderlich, die eine Einzelanmeldung an der Systemdatenbank umfassen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

End-to-End-SSO

Auf der BI-Plattform wird End-to-End-SSO über Windows AD und Kerberos unterstützt. In diesem Szenario können Benutzer sowohl die Einzelanmeldung an der BI-Plattform am Frontend als auch den SSO-Zugriff auf Datenbanken am Backend nutzen. Folglich müssen Benutzer ihre Anmeldedaten nur einmal angeben, wenn sie sich beim Betriebssystem anmelden. Anschließend können sie dann auf die BI-Plattform zugreifen und Aktionen ausführen, die Datenbankzugriff erfordern, z.B. Berichte anzeigen.

Konfiguration der manuellen Authentifizierung und der SSO-AD-Authentifizierung im Vergleich

Nachdem Sie die Implementierung erfolgreich so konfiguriert haben, dass über AD-Konten eine manuelle Anmeldung an BI-Launchpad durchgeführt werden kann, müssen Sie zur Einrichtung der AD-Authentifizierung zurückkehren, um bestimmte SSO-Anforderungen zu aktivieren. Die Anforderungen richten sich jeweils nach der ausgewählten SSO-Methode.

9.4.6.2 Verwenden der Vintela-Einzelanmeldung

9.4.6.2.1 Checkliste für die Vintela-SSO-Einrichtung

Zum Einrichten der BI-Plattform für den Betrieb mit Vintela-SSO müssen Sie folgende Aufgaben ausführen:

1. Konfigurieren Sie das Dienstkonto speziell für Vintela-SSO.
2. Konfigurieren Sie die eingeschränkte Delegierung (optional).
3. Konfigurieren Sie die Windows-AD-SSO-Authentifizierungsoptionen in der CMC.
4. Konfigurieren Sie die allgemeinen Eigenschaften und die BI-Launchpad-spezifischen Eigenschaften für Vintela-SSO.
5. Wenn Sie Tomcat als Webanwendungsserver für die Implementierung verwenden, müssen Sie die maximale Größe des Headers erhöhen.
6. Konfigurieren Sie die Internetbrowser für Vintela.

9.4.6.2.2 Einrichten des Dienstkontos für Vintela-SSO

Mit dem Befehlszeilentool `Ktpass` wird der Serverprinzipalname für den Host oder Dienst in Active Directory konfiguriert und eine Kerberos-Keytab-Datei generiert, die den gemeinsamen geheimen Schlüssel des Dienstkontos enthält. Dieses Tool befindet sich meist auf Domänencontrollern oder kann von der Microsoft-Support-Website (*http://support.microsoft.com/kb/892777*) heruntergeladen werden.

Sie benötigen ein Dienstkonto, das so konfiguriert ist, dass sich Benutzer mit ihren AD-Anmeldedaten automatisch gegenüber BI-Launchpad authentifizieren können. Sie können das Dienstkonto, das für die AD-Kerberos-Authentifizierung erstellt wurde, auf dem Domänencontroller neu konfigurieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wenn ein Client versucht, sich an BI-Launchpad anzumelden, wird eine Anforderung für den Server angestoßen, der das Kerberos-Ticket generiert. Um diese Anforderung beantworten zu können, muss das für die BI-Plattform erstellte Dienstkonto über einen SPN verfügen, der mit der URL des Anwendungsservers übereinstimmt. Führen Sie die folgenden Schritte auf dem Rechner aus, der den Domänencontroller hostet.

1. Führen Sie den Kerberos-Keytab-Setup-Befehl *ktpass* aus, um eine `Keytab`-Datei zu erstellen und abzulegen.

   Geben Sie die *ktpass*-Parameter an, die in der folgenden Tabelle aufgeführt sind:

Parameter	Beschreibung
-out	Angeben des Namens der zu erzeugenden Kerberos-`Keytab`-Datei.
-princ	Gibt den Prinzipalnamen für das Dienstkonto im SPN-Format an:`< MYSIAMYSERVER>/<sbo.service.domain.com>@<DOMAIN>.COM`, wobei `<MYSIAMYSERVER>` für den Namen des im Central Configuration Manager (CCM) angegebenen Service Intelligence Agent steht. **Hinweis** Bei den Namen von Dienstkonten wird zwischen Groß-/Kleinschreibung unterschieden. Der SPN umfasst den Namen des Hostrechners, auf dem die Dienstinstanz ausgeführt wird. **Tipp** Der SPN muss im Forest, in dem er registriert ist, eindeutig sein. Um dies zu überprüfen, suchen Sie mithilfe des Windows-Supporttools `Ldp.exe` nach dem SPN.
-pass	Gibt das vom Dienstkonto verwendete Kennwort an.
-ptype	Angeben des Prinzipaltyps: `-ptype KRB5_NT_PRINCIPAL`
-crypto	Angeben des für das Dienstkonto zu verwendenden Verschlüsselungstyps: `-crypto RC4-HMAC-NT`

   Beispiel:

```
ktpass -out <keytab_filename>.keytab -princ <MYSIAMYSERVER>/
sbo.service.domain.com@DOMAIN.COM
-pass password -kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

   In der Ausgabe des Befehls *ktpass* sollten der Ziel-Domänencontroller sowie die Erstellung einer Kerberos-`Keytab`-Datei mit dem gemeinsamen geheimen Schlüssel bestätigt werden. Der Befehl ordnet außerdem den Prinzipalnamen zum (lokalen) Dienstkonto zu.

2. Klicken Sie mit der rechten Maustaste auf das Dienstkonto, und wählen Sie **Eigenschaften** > **Delegierung** aus.
3. Wählen Sie **Benutzer bei Delegierungen aller Dienste vertrauen (nur Kerberos)**.
4. Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern.

Das Dienstkonto verfügt nun über alle erforderlichen Dienstprinzipalnamen für Vintela-SSO, und Sie haben eine Keytab-Datei mit dem verschlüsselten Kennwort für das Dienstkonto generiert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.4.6.2.2.1 Konfigurieren der eingeschränkten Delegierung für Vintela-SSO

Die eingeschränkte Delegierung ist bei Einrichtung von Vintela-SSO optional. Sie ist jedoch obligatorisch bei Implementierungen, die Systemdatenbank-SSO erfordern.

1. Öffnen Sie auf dem Rechner mit dem AD-Domänencontroller das Snap-In *Active-Directory-Benutzer und -Computer*.
2. Klicken Sie mit der rechten Maustaste auf das im vorherigen Abschnitt erstellte Dienstkonto, und klicken Sie auf **Eigenschaften** > **Delegierung**.
3. Wählen Sie **Benutzer bei Delegierungen angegebener Dienste vertrauen** .
4. Wählen Sie **Nur Kerberos verwenden**.
5. Klicken Sie auf **Hinzufügen** > **Benutzer oder Computer**.
6. Geben Sie den Namen des Dienstkontos ein, und klicken Sie auf **OK**.
   Eine Liste der Dienste wird eingeblendet.
7. Wählen Sie die folgenden Dienste aus, und klicken Sie dann auf **OK**.
   - Den HTTP-Dienst
   - Den Dienst, der zur Ausführung des Service Intelligence Agent (SIA) auf dem Rechner verwendet wird, der die BI-Plattform hostet.

   Die Dienste werden der Liste der Dienste hinzugefügt, die für das Dienstkonto delegiert werden können.

Damit diese Änderung übernommen wird, müssen die Webanwendungseigenschaften bearbeitet werden.

9.4.6.2.3 Konfigurieren von SSO-Einstellungen in der CMC

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
2. Doppelklicken Sie auf **Windows AD**.
3. Stellen Sie sicher, dass das Kontrollkästchen **Windows Active Directory (AD) aktivieren** aktiviert ist.
4. Vergewissern Sie sich, dass unter *Authentifizierungsoptionen* die Option **Kerberos-Authentifizierung verwenden** ausgewählt ist.
5. Wenn für die Konfiguration SSO bei der Datenbank erforderlich ist, wählen Sie **Cachesicherheitskontext** aus.
6. Aktivieren Sie das Kontrollkästchen **Einzelanmeldung für ausgewählten Authentifizierungsmodus aktivieren**.
7. Klicken Sie auf **Aktualisieren**.

9.4.6.2.4 Aktivieren der Vintela-Einzelanmeldung für BI-Launchpad und OpenDocument

Dieses Verfahren wird für BI-Launchpad oder OpenDocument verwendet. Um SSO für die BI-Plattform-Anwendungen zu aktivieren, müssen Vintela- und SSO-spezifische Eigenschaften in der Datei `BOE.war`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

angegeben werden. Zum Zweck der SSO-Einrichtung empfiehlt es sich, dass Sie sich zunächst auf die Aktivierung von SSO für BI-Launchpad für AD-Konten konzentrieren, bevor Sie sich anderen Anwendungen zuwenden.

1. Greifen Sie auf den benutzerdefinierten Ordner der BOE-Webanwendung auf dem Rechner zu, der den Webanwendungsserver hostet:

   `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Nehmen Sie die Änderungen im Verzeichnis `config\custom` und nicht im Verzeichnis `config\default` vor. Ansonsten werden die Änderungen überschrieben, wenn Sie zukünftige Patches auf die Implementierung anwenden.

   Die geänderte BOE-Webanwendung muss zu einem späteren Zeitpunkt erneut implementiert werden.
2. Erstellen Sie eine neue Datei mit einem Texteditor.
3. Geben Sie Folgendes ein:

```
sso.enabled=true
siteminder.enabled=false
vintela.enabled=true
idm.realm=DOMAIN.COM
idm.princ=MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM
idm.allowUnsecured=true
idm.allowNTLM=false
idm.logger.name=simple
idm.keytab=C:/WIN/filename.keytab
idm.logger.props=error-log.properties
```

> **Hinweis**
>
> Für die Parameter*idm.realm* und *idm.princ* müssen gültige Werte eingegeben werden. Beim Wert von *idm.realm* sollte es sich um denselben Wert handeln, den Sie bei der Konfiguration von `default_realm` in der Datei `krb5.ini` festgelegt haben. Der Wert muss in Großbuchstaben eingegeben werden. Der Parameter *idm.princ* ist der SPN, der für das für die Vintela-Einzelanmeldung erstellte Dienstkonto verwendet wird.

> **Hinweis**
>
> Bei Angabe des Speicherorts der Keytab-Datei müssen Schrägstriche verwendet werden.

   Überspringen Sie den folgenden Schritt, wenn Sie die eingeschränkte Delegation für die Windows-AD-Authentifizierung und die Vintela-Einzelanmeldung nicht verwenden möchten.
4. Um die eingeschränkte Delegation zu verwenden, fügen Sie den folgenden Wert hinzu:

```
idm.allowS4U=true
```

5. Schließen Sie die Datei, und speichern Sie sie unter dem Namen `global.properties`.

> **Hinweis**
>
> Stellen Sie sicher, dass der Dateiname nicht mit einer Dateierweiterung wie `.txt` gespeichert wird.

6. Erstellen Sie eine weitere Datei im selben Verzeichnis. Speichern Sie die Datei je nach Ihren Anforderungen unter `OpenDocument.properties` oder `BIlaunchpad.properties`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7. Geben Sie Folgendes ein:

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

Beispiel:

```
authentication.default=secWinAD
cms.default=mycms:6400
```

8. Speichern und schließen Sie die Datei.
9. Starten Sie Ihren Webanwendungsserver neu.

Die neuen Eigenschaften werden erst wirksam, wenn die BOE-Webanwendung auf dem Rechner, auf dem der Webanwendungsserver ausgeführt wird, erneut implementiert wird. Verwenden Sie WDeploy zur erneuten Implementierung von BOE auf dem Webanwendungsserver. Weitere Informationen zur Verwendung von WDeploy zur Deinstallation von Webanwendungen finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.

> **Hinweis**
>
> Wenn Ihre Implementierung eine Firewall enthält, öffnen Sie alle erforderlichen Ports, da die Webanwendungen sonst keine Verbindung mit den BI-Servern herstellen können.

9.4.6.2.5 Aktivieren der Vintela-Einzelanmeldung für Webdienste

Für einige Clienttools ist die Authentifizierung über Webdienste erforderlich. Führen Sie diese Schritte aus, um die Einzelanmeldung (SSO) für Webdienste zu aktivieren.

1. Sichern Sie diese Datei: `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\web.xml`, und öffnen Sie sie anschließend zur Bearbeitung.
2. Entfernen Sie den Kommentar der Abschnitte für den Kerberos-Proxy-Filter und den Kerberos-Filter, um die Kerberos-Einzelanmeldung für die Authentifizierung von Windows Active Directory (secWinAD) zu aktivieren.

   Folgende Optionen müssen festgelegt werden (die restlichen sind optional):

   - `idm.realm` (identisch mit default_realm wie in Datei Krb5.ini angegeben).
   - `idm.princ` (identisch mit idm.princ in der Datei global.properties, die sich im Verzeichnis `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` befindet).
   - `idm.keytab` (identisch mit idm.keytab in der Datei global.properties, die sich im Verzeichnis `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` befindet).

     > **Hinweis**
     >
     > Wenn Sie das in den Tomcat-Java-Optionen festgelegte festkodierte Kennwort verwenden, nehmen Sie keine Änderungen an den Keytab-Zeilen in der Datei `web.xml` vor.

3. Wenn SSL nicht mit dem Java-Anwendungsserver verwendet wird, setzen Sie den Parameter idm.allowUnsecured auf **`Wahr`**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen zu Tomcat-SSL finden Sie im Knowledge-Base-Artikel mit der ID 1484802.

4. Sichern Sie diese Datei: `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\classes\dsws.properties`, und öffnen Sie sich anschließend zur Bearbeitung.
5. Legen Sie kerberos.sso auf `Wahr` fest, und sichern Sie die Datei.
6. Implementieren Sie die WAR-Datei mit WDeploy erneut auf dem Webanwendungsserver.

   Informationen zum Umgang mit WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen*.
7. Starten Sie Tomcat neu.
8. Starten Sie Query-As-a-Web-Service-Designer auf dem Clientcomputer mit den installierten Clienttools, um Ihre Einstellungen zu testen.
9. Fügen Sie einen neuen verwalteten Host ein.
10. Geben Sie den Anwendungsservernamen ein.
11. Geben Sie die Webdienst-URL in diesem Format ein: `http://<WebAnwServer>:<Portnummer>/dswsbobje/services/Session`.

    Beispiel: `http://BI4:8080/dswsbobje/services/Session`.
12. Geben Sie den CMS-Hostnamen ein.
13. Ändern Sie den Authentifizierungstyp in **Windows AD**.
14. Wählen Sie **Windows-Active-Directory-Einzelanmeldung aktivieren**.
15. Lassen Sie in der Anmeldeaufforderung die Felder **Benutzer** und **Kennwort** leer, und klicken Sie auf **OK**.

9.4.6.2.6 Erhöhen des Grenzwerts für die Headergröße für Tomcat

Active Directory erstellt ein Kerberos-Token, das bei der Authentifizierung verwendet wird. Dieses Token wird im HTTP-Header gespeichert. Der Java-Anwendungsserver verfügt über eine standardmäßige HTTP-Headergröße. Um Fehler zu vermeiden, sollten Sie sicherstellen, dass eine standardmäßige Mindestgröße von 16384 Byte angegeben ist. (Einige Implementierungen erfordern u.U. eine umfangreichere Größe. Weitere Informationen finden Sie in den Microsoft-Richtlinien zu Größenanforderungen auf der Support-Website (http://support.microsoft.com/kb/327825).)

1. Öffnen Sie auf dem Server, auf dem Tomcat installiert ist, die Datei `server.xml`.

   Unter Windows befindet sich die Datei unter `<TomcatINSTALLVERZ>/conf`.

   - Wenn Sie die mit der BI-Plattform unter Windows installierte Tomcat-Version verwenden, und Sie den Standardinstallationspfad nicht geändert haben,

     ersetzen Sie `<TomcatINSTALLVERZ>` durch `C:\Programme (x86)\SAP BusinessObjects\Tomcat\`.
   - Wenn Sie einen anderen unterstützten Webanwendungsserver verwenden, schlagen Sie den richtigen Pfad in der Begleitdokumentation Ihres Webanwendungsservers nach.
2. Suchen Sie das `<Connector …>`-Tag für die konfigurierte Portnummer.

   Wenn Sie den Standardport 8080 verwenden, suchen Sie das `<Connector …>`-Tag mit port="8080".

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Beispiel:

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
minSpareThreads="25" port="8080" redirectPort="8443"
/>
```

3. Fügen Sie folgenden Wert innerhalb des `<Connector …>`-Tags ein:

   `maxHttpHeaderSize="16384"`

   Beispiel:

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
maxHttpHeaderSize="16384" minSpareThreads="25" port="8080" redirectPort="8443" />
```

4. Speichern und schließen Sie die Datei `server.xml`.
5. Starten Sie Tomcat neu.

> **Hinweis**
>
> Wenn Sie einen anderen Java-Anwendungsserver verwenden, sollten Sie sich in der Dokumentation des betreffenden Java-Anwendungsservers informieren.

9.4.6.2.7 Konfigurieren von Internet-Browsern

Damit Vintela-SSO für die AD-Kerberos-Authentifizierung unterstützt wird, müssen die BI-Plattform-Clients konfiguriert werden. Dazu gehört die Konfiguration des Webbrowsers auf den Clientcomputern.

9.4.6.2.7.1 Konfigurieren des Internet Explorers auf Clientrechnern

1. Öffnen Sie auf dem Clientrechner einen Internet-Explorer-Browser.
2. Aktivieren Sie die integrierte Windows-Authentifizierung.
   a) Klicken Sie im Menü **Extras** auf **Internetoptionen**.
   b) Klicken Sie auf die Registerkarte **Erweitert**.
   c) Führen Sie einen Bildlauf zu **Sicherheit** aus, wählen Sie **Integrierte Windows-Authentifizierung aktivieren**, und klicken Sie auf **Übernehmen**.
3. Fügen Sie den Java-Anwendungsrechner oder die URL zu den vertrauenswürdigen Sites hinzu. Sie können den vollständigen Domänennamen der Site eingeben.
   a) Klicken Sie im Menü **Extras** auf **Internetoptionen**.
   b) Klicken Sie auf die Registerkarte **Sicherheit**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

c) Klicken Sie auf **Sites** und dann auf **Erweitert**.
d) Wählen Sie die Site aus, oder geben Sie sie ein, und klicken Sie anschließend auf **Hinzufügen.**
e) Klicken Sie so lange auf **OK**, bis das Dialogfeld "Internetoptionen" geschlossen wird.

4. Schließen und öffnen Sie das Internet Explorer-Browserfenster erneut, damit diese Änderungen wirksam werden.
5. Wiederholen Sie alle diese Schritte auf jedem BI-Plattform-Clientrechner.

9.4.6.2.7.2 So konfigurieren Sie Firefox auf Clientrechnern

1. **Ändern Sie "network.negotiate-auth.delegation-uris"**
   a) Öffnen Sie auf dem Clientrechner das Firefox-Browserfenster.
   b) Geben Sie `about:config` in das URL-Adressfeld ein.
   Eine Liste der konfigurierbaren Eigenschaften wird angezeigt.
   c) Doppelklicken Sie auf **network.negotiate-auth.delegation-uris**, um die Eigenschaft zu bearbeiten.
   d) Geben Sie die URL ein, über die Sie auf BI-Launchpad zugreifen.

   Beispiel: Lautet die BI-Launchpad-URL `http://<Rechner.Domäne.com>:8080/BOE/BI`, müssen Sie `http://<Rechner.Domäne.com>` eingeben.

   > **Hinweis**
   > Wenn Sie mehrere URLs hinzufügen, trennen Sie sie durch ein Komma. Beispiel: `http://<Rechner.Domäne.com>,<Rechner2.Domäne.com>` .

   e) Klicken Sie auf **OK**.
2. **Ändern Sie "network.negotiate-auth.trusted-uris"**
   a) Öffnen Sie auf dem Clientrechner das Firefox-Browserfenster.
   b) Geben Sie `about:config` in das URL-Adressfeld ein.
   Eine Liste der konfigurierbaren Eigenschaften wird angezeigt.
   c) Doppelklicken Sie auf **network.negotiate-auth.trusted-uris**, um die Eigenschaft zu ändern.
   d) Geben Sie die URL ein, über die Sie auf BI-Launchpad zugreifen.
   Wenn die BI-Launchpad-URL beispielsweise `http://<Rechner.Domäne.com>:8080/BOE/BI` lautet, müssen Sie `http://<Rechner.Domäne.com>` eingeben.

   > **Hinweis**
   > Wenn Sie mehrere URLs hinzufügen, trennen Sie sie durch ein Komma. Beispiel: `http://<Rechner.Domäne.com>,<Rechner2.Domäne.com>` .

   e) Klicken Sie auf **OK**.
3. Schließen und öffnen Sie das Firefox-Browserfenster erneut, damit diese Änderungen wirksam werden.
4. Wiederholen Sie alle diese Schritte auf jedem BI-Plattform-Clientrechner.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.4.6.2.8 Testen von Vintela-SSO für die AD-Kerberos-Authentifizierung

Sie sollten die SSO-Einrichtung über eine Clientarbeitsstation testen. Stellen Sie sicher, dass sich der Client in derselben Domäne wie die BI-Plattform-Implementierung befindet, und dass Sie als zugeordneter AD-Benutzer an der Arbeitsstation angemeldet sind. Sie müssen über dieses Benutzerkonto in der Lage sein, sich manuell an BI-Launchpad anzumelden.

Öffnen Sie zum Testen von SSO einen Browser, und geben Sie die URL für BI-Launchpad ein. Wenn SSO korrekt konfiguriert ist, dürften Ihre Anmeldedaten nicht angefordert werden.

➔ Tipp

Es empfiehlt sich, verschiedene AD-Benutzerszenarios in der Implementierung zu testen. Wenn die Umgebung beispielsweise Benutzer aus mehreren Betriebssystemen umfasst, sollten Sie die SSO-Einrichtung für Benutzer aus jedem Betriebssystem testen. Des Weiteren ist es ratsam, die SSO-Einrichtung mit allen Browsern zu testen, die in der Organisation unterstützt werden. Wenn die Umgebung Benutzer aus mehreren Gesamtstrukturen oder Domänen umfasst, sollten Sie die SSO-Einrichtung für ein Benutzerkonto aus jeder Domäne oder Gesamtstruktur testen.

9.4.6.2.9 Konfigurieren von Kerberos und Datenbank-Einzelanmeldung für Anwendungsserver

Die Einzelanmeldung bei Datenbanken wird für Implementierungen unterstützt, die alle folgenden Voraussetzungen erfüllen:

- Die Implementierung der BI-Plattform befindet sich auf einem Webanwendungsserver.
- Der Webanwendungsserver wurde für Vintela-SSO für die AD-Authentifizierung konfiguriert.
- Bei der Datenbank, für die SSO erforderlich ist, handelt es sich um eine unterstützte Version von SQL Server oder Oracle.
- Den Benutzergruppen, die Zugriff auf die Datenbank benötigen, müssen Berechtigungen innerhalb von SQL Server oder Oracle gewährt werden.

Der letzte Schritt besteht darin, die Datei `krb5.ini` zu ändern, damit Datenbank-SSO für Webanwendungen unterstützt wird.

9.4.6.2.9.1 So aktivieren Sie die Einzelanmeldung bei Datenbanken für Java-Anwendungsserver

1. Öffnen Sie die Datei `krb5.ini`, die für die Implementierung der BI-Plattform verwendet wird.

   Der Standardspeicherort für diese Datei ist das Verzeichnis WIN auf Ihrem Webanwendungsserver.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Wenn die Datei nicht im Verzeichnis WIN enthalten ist, überprüfen Sie das folgende Java-Argument auf den Speicherort der Datei:
>
> ```
> -Djava.security.auth.login.config
> ```
>
> Diese Variable wird angegeben, wenn AD mit Kerberos auf dem Webanwendungsserver konfiguriert wird.

2. Wechseln Sie zum Abschnitt `[libdefaults]` der Datei.
3. Geben Sie die folgende Zeichenfolge vor dem Abschnitt `[realms]` der Datei ein:

   ```
   forwardable=true
   ```

4. Speichern und schließen Sie die Datei.
5. Starten Sie Ihren Webanwendungsserver neu.

Die Einzelanmeldung an der Datenbank wird erst aktiviert, wenn Sie das Feld **Cachesicherheitskontext (für SSO bei Datenbank erforderlich)** auf der Windows AD-Authentifizierungsseite in der CMC aktivieren.

9.4.6.3 Verwenden von SiteMinder

9.4.6.3.1 Verwenden von Windows AD mit SiteMinder

In diesem Abschnitt wird erläutert, wie Sie AD und SiteMinder verwenden. SiteMinder ist ein von einem Fremdhersteller entwickeltes Benutzerzugriffs- und Authentifizierungstool, das mit dem AD-Sicherheits-Plugin verwendet werden kann, um die Einzelanmeldung bei der BI-Plattform einzurichten. Sie können SiteMinder mit Kerberos verwenden.

Stellen Sie sicher, dass die SiteMinder-Identitätsverwaltungsressourcen installiert und konfiguriert sind, bevor Sie die Windows AD-Authentifizierung für SiteMinder konfigurieren. Weitere Informationen zu SiteMinder sowie Installationshinweise finden Sie in der SiteMinder-Dokumentation.

Zur Aktivierung der AD-Einzelanmeldung mit SiteMinder müssen zwei Schritte ausgeführt werden:

- Konfigurieren des AD-Plugins für die Einzelanmeldung mit SiteMinder
- Konfigurieren der SiteMinder-Eigenschaften für die BOE-Webanwendung

> **Hinweis**
>
> Stellen Sie sicher, dass der SiteMinder-Administrator die Unterstützung für 4.x-Agenten aktiviert hat. Dies muss unabhängig von der unterstützten SiteMinder-Version geschehen, die Sie verwenden. Weitere Informationen zur SiteMinder-Konfiguration erhalten Sie in der SiteMinder-Dokumentation.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.4.6.3.1.1 Aktivieren von SiteMinder-Eigenschaften für BI-Launchpad

Außer den SiteMinder-Einstellungen, die für das Windows AD-Sicherheitsplugin vorgenommen werden müssen, sind SiteMinder-Einstellungen für die BOE war-Eigenschaften festzulegen.

1. Suchen Sie das Verzeichnis `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` in Ihrer BI-Plattform-Installation.
2. Erstellen Sie mit Editor oder einem anderen Textbearbeitungsprogramm eine neue Datei in dem Verzeichnis.
3. Geben Sie folgende Werte in die neue Datei ein:

```
sso.enabled=true
siteminder.authentication=secWinAD
siteminder.enabled=true
```

4. Speichern Sie die Datei unter dem Namen `global.properties`.

> **Hinweis**
>
> Stellen Sie sicher, dass der Dateiname nicht mit einer Dateierweiterung, z.B. `.txt`, gespeichert wird.

5. Erstellen Sie eine weitere Datei im selben Verzeichnis.
6. Geben Sie folgende Werte in die neue Datei ein:

```
authentication.default=secWinAD
cms.default=[cms name]:[CMS port number]
```

   Beispiel:

```
authentication.default=LDAP
cms.default=mycms:6400
```

7. Speichern Sie die Datei unter dem Namen `BIlaunchpad.properties`, und schließen Sie sie.

Die neuen Eigenschaften werden erst wirksam, wenn die Datei BOE.war auf dem Computer, auf dem der Webanwendungsserver ausgeführt wird, erneut implementiert wird. Implementieren Sie die WAR-Datei mit WDeploy erneut auf dem Webanwendungsserver. Weitere Informationen zur Verwendung von WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.

9.4.6.3.1.2 Konfigurieren von SiteMinder-Einstellungen in der CMC

Vor Konfiguration der CMC für SiteMinder müssen folgende Voraussetzungen erfüllt sein:

- AD-Benutzergruppen wurden der BI-Plattform erfolgreich zugeordnet.
- Sie haben die AD-Anmeldedaten im CCM getestet.

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
2. Doppelklicken Sie auf **Windows AD**.
3. Aktivieren Sie das Kontrollkästchen **Windows Active Directory (AD) aktivieren**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Wählen Sie unter "Authentifizierungsoptionen" die Option **NTLM-Authentifizierung verwenden** oder **Kerberos-Authentifizierung verwenden** aus.

   Um die BI-Plattform für die Kerberos- und AD-Authentifizierung mit Kerberos konfigurieren zu können, benötigen Sie ein Dienstkonto. Sie können entweder ein neues Domänenkonto erstellen oder ein vorhandenes verwenden. Das Dienstkonto wird zur Ausführung der BI-Plattform-Server verwendet.

   > **Tipp**
   >
   > Bei der manuellen Anmeldung an BI-Launchpad müssen Benutzer anderer Domänen den Domänennamen in Großbuchstaben an ihren Benutzernamen anhängen. Beispiel: Bei `user@CHILD.PARENTDOMAIN.COM` ist “CHILD.PARENTDOMAIN.COM” die Domäne.

5. Wenn Sie **Kerberos-Authentifizierung verwenden** ausgewählt haben:
   a) Wenn Sie die Einzelanmeldung an einer Datenbank konfigurieren möchten, wählen Sie **Cachesicherheitskontext** aus.
   b) Löschen Sie alle Informationen aus dem Feld **Dienstprinzipalname**.
6. Wenn Sie die Einzelanmeldung konfigurieren möchten, aktivieren Sie **Einzelanmeldung für ausgewählten Authentifizierungsmodus aktivieren**.

   Außerdem müssen die allgemeinen BOE-Webanwendungseigenschaften und die BI-Launchpad-Eigenschaften zur Aktivierung der Einzelanmeldung konfiguriert werden.
7. Wählen Sie im Bereich *Synchronisierung der Anmeldedaten* eine Option aus, um die Datenquellenanmeldedaten des AD-Benutzers zum Zeitpunkt der Anmeldung zu aktivieren und zu aktualisieren.

   Durch diese Option wird die Datenquelle mit den aktuellen Anmeldedaten des Benutzers synchronisiert.
8. Konfigurieren Sie im Bereich *SiteMinder-Optionen* SiteMinder als Einzelanmeldungsoption für die AD-Authentifizierung mit Kerberos:
   a) Klicken Sie auf **Deaktiviert**.

      Die Seite *Windows Active Directory* wird angezeigt.

      Falls Sie das Windows-AD-Plugin noch nicht konfiguriert haben, wird eine Warnmeldung mit der Frage angezeigt, ob Sie den Vorgang fortsetzen möchten. Klicken Sie auf **OK**.
   b) Klicken Sie auf **SiteMinder-Einzelanmeldung verwenden**.
   c) Geben Sie im Feld **Richtlinienserver-Host** die Namen der einzelnen Richtlinienserver ein, und klicken Sie auf **Hinzufügen**.
   d) Geben Sie für jeden Richtlinienserver-Host eine Portnummer in die Felder **Accounting**, **Authentifizierung** und **Autorisierung** ein.
   e) Geben Sie in das Feld **Agentname** den Agentnamen ein.
   f) Geben Sie in die Felder von **Gemeinsamer geheimer Schlüssel** den gemeinsamen geheimen Schlüssel ein.

      Stellen Sie sicher, dass der SiteMinder-Administrator die Unterstützung für 4.x-Agenten aktiviert hat, ungeachtet dessen, welche unterstützte Version von SiteMinder Sie verwenden. Informationen sowie Installationshinweise zu SiteMinder finden Sie in der SiteMinder-Dokumentation.
   g) Klicken Sie auf **Aktualisieren**, um die Daten zu speichern und zur Hauptseite der AD-Authentifizierung zurückzukehren.
9. Geben Sie im Bereich *Optionen für AD-Aliase* an, wie neue Aliase der BI-Plattform hinzugefügt und auf dieser aktualisiert werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

a) Wählen Sie im Bereich *Optionen für neuen Alias* eine Option für die Zuordnung neuer Aliase zu Enterprise-Konten aus:

- **Jeden neuen AD-Alias einem vorhandenen Benutzerkonto mit demselben Namen zuweisen**

  Wählen Sie diese Option aus, wenn Sie wissen, dass einige Benutzer über ein bereits vorhandenes Enterprise-Konto mit demselben Namen verfügen, d.h. vorhandenen Benutzern werden AD-Aliase zugewiesen (die automatische Generierung von Aliasen ist aktiviert). Benutzer ohne Enterprise-Konto oder mit unterschiedlichen Namen für das Enterprise- und das AD-Konto werden als neue Benutzer hinzugefügt.
- **Neues Benutzerkonto für jeden neuen AD-Alias erstellen**

  Verwenden Sie diese Option, wenn Sie für jeden Benutzer ein neues Konto erstellen möchten.

b) Wählen Sie im Bereich *Aktualisierungsoptionen für Aliase* eine Option für die Verwaltung von Aliasaktualisierungen für Enterprise-Konten aus:

- **Neue Aliase bei der Aliasaktualisierung erstellen**

  Wählen Sie diese Option aus, um für jeden AD-Benutzer, der der BI-Plattform zugeordnet wurde, automatisch einen neuen Alias zu erstellen. Neue AD-Konten werden für Benutzer ohne BI-Plattform-Konten bzw. für alle Benutzer hinzugefügt, wenn Sie die Option **Neues Benutzerkonto für jeden neuen AD-Alias erstellen** ausgewählt und auf **Aktualisieren** geklickt haben.
- **Neue Aliase nur bei der Benutzeranmeldung erstellen**

  Wählen Sie diese Option, wenn das zuzuordnende AD-Verzeichnis viele Benutzer umfasst, von denen jedoch nur wenige die BI-Plattform werden. Die Plattform erstellt nicht automatisch Aliase und Enterprise-Konten für alle Benutzer. Vielmehr werden Aliase (und ggf. Konten) nur für die Benutzer erstellt, die sich an der BI-Plattform anmelden.

c) Wählen Sie im Bereich *Optionen für neue Benutzer* eine Option zum Erstellen neuer Benutzer aus:

- **Neue Benutzer werden als vordefinierte Benutzer erstellt**

  Neue Benutzerkonten werden für die Verwendung von Namenslizenzen konfiguriert. Namenslizenzen sind mit bestimmten Benutzern verbunden und ermöglichen den Zugriff auf das System auf der Grundlage von Benutzername und Kennwort. Dieser Lizenztyp ermöglicht Namenslizenzbenutzern den Zugriff auf das System, unabhängig von der Anzahl der derzeit verbundenen Benutzer. Für jedes mit dieser Option erstellte Benutzerkonto muss eine Namenslizenz verfügbar sein.
- **Neue Benutzer werden als gleichzeitige Benutzer erstellt**

  Neue Benutzerkonten werden für die Verwendung von Zugriffslizenzen konfiguriert. Zugriffslizenzen geben die Anzahl der Personen an, die gleichzeitig mit der BI-Plattform verbunden sein können. Dieser Lizenztyp ist sehr flexibel, da mit einer geringen Anzahl von Zugriffslizenzen viele Benutzer unterstützt werden können. Je nach Häufigkeit und Dauer des Zugriffs auf das System können 100 Zugriffslizenzen beispielsweise 250, 500 oder auch 700 Benutzer unterstützen.

10. Klicken Sie auf **Zeitgesteuert verarbeiten**, um zu konfigurieren, wie AD-Aliasaktualisierungen zeitgesteuert verarbeitet werden.

    a) Wählen Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* ein Wiederholungsintervall aus der Liste **Objekt ausführen** aus.

    b) Legen Sie andere Optionen und Parameter der zeitgesteuerten Verarbeitung nach Bedarf fest.

    c) Klicken Sie auf **Zeitgesteuert verarbeiten**.
    Bei der Aliasaktualisierung werden auch die Gruppeninformationen aktualisiert.

11. Legen Sie im Bereich *Optionen für die Attributbindung* die Attributbindungspriorität für das AD-Plugin fest:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

a) Aktivieren Sie das Kontrollkästchen **Vollständigen Namen, E-Mail-Adresse und andere Attribute importieren**.
Die in AD-Konten verwendeten vollständigen Namen und Beschreibungen werden importiert und mit Benutzerobjekten in der BI-Plattform gespeichert.

b) Geben Sie eine Option für **Priorität der AD-Attributbindung im Verhältnis zu anderen Attributbindungen festlegen** an.

Wenn die Option auf 1 festgelegt ist, haben AD-Attribute immer dann Vorrang, wenn AD-Plugins und andere Plugins (LDAP und SAP) aktiviert sind. Wenn die Option auf 3 festgelegt ist, haben Attribute von anderen aktivierten Plugins Priorität. Die Bindungen müssen auf unterschiedliche Werte festgelegt sein. Mehrere Authentifizierungs-Plugins auf denselben Bindungswert festzulegen kann zu unerwarteten Ergebnissen führen.

12. Konfigurieren Sie im Bereich *AD-Gruppenoptionen* AD-Gruppenaktualisierungen:

a) Klicken Sie auf **Zeitgesteuert verarbeiten**.
Das Dialogfeld *Zeitgesteuerte Verarbeitung* wird angezeigt.

b) Wählen Sie ein Wiederholungsintervall aus der Liste **Objekt ausführen** aus.

c) Legen Sie andere Optionen und Parameter der zeitgesteuerten Verarbeitung nach Bedarf fest.

d) Klicken Sie auf **Zeitgesteuert verarbeiten**.

Das System führt die zeitgesteuerte Verarbeitung der Aktualisierung gemäß den von Ihnen angegebenen Zeitsteuerungsinformationen aus. Die nächste zeitgesteuerte Aktualisierung für die AD-Gruppenkonten wird unter *AD-Gruppenoptionen* angezeigt.

13. Wählen Sie im Bereich *AD-Aktualisierung auf Abruf* eine Option aus, um anzugeben, ob beim Klicken auf **Aktualisieren** AD-Gruppen oder -Benutzer (oder keine davon) aktualisiert werden:

- **AD-Gruppen jetzt aktualisieren**

  Wählen Sie diese Option aus, wenn beim Klicken auf **Aktualisieren** mit der Aktualisierung aller zeitgesteuerter AD-Gruppen begonnen werden soll. Die nächste zeitgesteuerte AD-Gruppenaktualisierung ist unter *AD-Gruppenoptionen* aufgeführt.

- **AD-Gruppen und -Aliase jetzt aktualisieren**

  Wählen Sie diese Option aus, wenn beim Klicken auf **Aktualisieren** mit der Aktualisierung aller zeitgesteuerter AD-Gruppen und -Benutzeraliase begonnen werden soll. Die nächsten zeitgesteuerten Aktualisierungen sind unter *AD-Gruppenoptionen* und *Optionen für AD-Aliase* aufgeführt.

- **AD-Gruppen und -Aliase jetzt nicht aktualisieren**

  Beim Klicken auf **Aktualisieren** werden keine AD-Gruppen oder -Benutzeraliase aktualisiert.

14. Klicken Sie auf **Aktualisieren** und dann auf **OK**.

9.4.6.3.1.3 Deaktivieren von SiteMinder

Wenn Sie die Konfiguration von SiteMinder verhindern oder SiteMinder nach der Konfiguration in der CMC deaktivieren möchten, ändern Sie die Webkonfigurationsdatei für BI-Launchpad.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.4.6.3.1.3.1 Deaktivieren von SiteMinder für Java-Clients

Neben der Deaktivierung der SiteMinder-Einstellungen für das Windows AD-Sicherheits-Plugin müssen die SiteMinder-Einstellungen auch für die BOE-WAR-Datei auf dem Webanwendungsserver deaktiviert werden.

1. Wechseln Sie zu folgendem Verzeichnis in der BI-Plattform-Installation:

   `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`

2. Öffnen Sie die Datei `global.properties`.
3. Ändern Sie *siteminder.enabled* in "false".

   ```
   siteminder.enabled=false
   ```

4. Speichern Sie Ihre Änderungen, und schließen Sie die Datei.

Die Änderung tritt erst in Kraft, wenn `BOE.war` auf dem Rechner mit dem Webanwendungsserver erneut implementiert wurde. Implementieren Sie die WAR-Datei mit WDeploy erneut auf dem Webanwendungsserver. Weitere Informationen zur Verwendung von WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.

9.4.7 Fehlerbehebung Windows AD-Authentifizierung

9.4.7.1 Fehlerbehebung der Konfiguration

Die folgenden Schritte können hilfreich sein, falls bei der Konfiguration von Kerberos Probleme auftreten:

- Protokollierung aktivieren
- Java SDK-Kerberos-Konfiguration testen

9.4.7.1.1 So aktivieren Sie die Protokollierung

1. Wählen Sie im Menü **Start** die Option **Programme >Tomcat > Tomcat-Konfiguration**.
2. Klicken Sie auf die Registerkarte **Java**.
3. Fügen Sie die folgenden Optionen hinzu:

   ```
   -Dcrystal.enterprise.trace.configuration=verbose
   -sun.security.krb5.debug=true
   ```

   Hierdurch wird eine Protokolldatei in folgendem Speicherort erstellt:

   ```
   C:\Documents and Settings\<user name>\.businessobjects\jce_verbose.log
   ```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.4.7.1.2 So testen Sie die Kerberos-Konfiguration

Führen Sie zum Testen der Kerberos-Konfiguration den folgenden Befehl aus, wobei `servant` für das Dienstkonto und die Domäne steht, unter der der CMS ausgeführt wird, und `password` für das Kennwort, das dem Dienstkonto zugeordnet ist.

```
<Installverz>\SAP BusinessObjects Enterprise XI 4.0\win64_64\jdk\bin
\servact@TESTM03.COM Password
```

Beispiel:

```
C:\Program Files\SAP BusinessObjects\
 SAP BusinessObjects Enterprise XI 4.0\win64_64\jdk\bin\
 servact@TESTM03.COM Password
```

Der Domänen- und Dienstprinzipalname muss genau mit dem Domänen- und Dienstprinzipalnamen von Active Directory übereinstimmen. Wenn das Problem weiterhin auftritt, prüfen Sie, ob Sie den gleichen Namen eingegeben haben. Beachten Sie, dass beim Namen die Groß- und Kleinschreibung berücksichtigt wird.

9.4.7.1.3 Anmeldefehler aufgrund unterschiedlicher AD UPN- und SAM-Namen

Die Active-Directory-ID eines Benutzers wurde der BI-Plattform erfolgreich zugeordnet. Trotzdem ist der Benutzer nicht in der Lage, mit der Windows AD-Authentifizierung und Kerberos in folgendem Format eine Anmeldung bei der CMC oder bei BI-Launchpad auszuführen: `DOMÄNE\ABC123`

Dieses Problem kann auftreten, wenn der Benutzer in Active Directory mit einem UPN und SAM-Namen eingerichtet wurde, die nicht identisch sind. Die folgenden Beispiele können ein Problem verursachen:

- Der UPN lautet "abc123@firma.com" und der SAM-Name "DOMAIN\ABC123".
- Der UPN lautet "jschmidt@firma" und der SAM-Name "DOMAIN\janschmidt"

Dieses Problem kann auf zwei Weisen behoben werden:

- Benutzer melden sich unter Verwendung des UPN-Namens und nicht mit dem SAM-Namen an.
- Stellen Sie sicher, dass der SAM-Kontoname und der UPN-Name identisch sind.

9.4.7.1.4 Fehler vor der Authentifizierung

Ein Benutzer, der sich zuvor anmelden konnte, kann sich nicht mehr anmelden. Der Benutzer erhält folgende Fehlermeldung: "Kontoinformationen nicht erkannt." In Tomcat-Fehlerprotokollen finden Sie folgenden Fehler: `"Pre-authentication information was invalid (24)"` (Vorbestätigungsinformationen waren ungültig).

Dieser Fehler kann darin begründet liegen, dass eine Änderung, die in AD am UPN vorgenommen wurde, nicht an die Kerberos-Benutzerdatenbank weitergeleitet wurde. Es ist also möglich, dass die Kerberos-Benutzerdatenbank und die AD-Informationen nicht synchronisiert sind.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Um dieses Problem zu beheben, setzen Sie das Benutzerkennwort in AD zurück. Dadurch wird sichergestellt, dass die Änderungen ordnungsgemäß weitergeleitet werden.

> **Hinweis**
>
> Dieses Problem tritt bei J2SE 5.0 nicht auf.

9.5 SAP-Authentifizierung

9.5.1 Konfigurieren der SAP-Authentifizierung

In diesem Abschnitt wird erläutert, wie Sie die BI-Plattform-Authentifizierung für Ihre SAP-Umgebung konfigurieren.

Die SAP-Authentifizierung ermöglicht es SAP-Benutzern, sich mit ihrem SAP-Benutzernamen und -Kennwort bei der BI-Plattform anzumelden, ohne dass das Kennwort in der BI-Plattform gespeichert wird. Außerdem bietet Ihnen die SAP-Authentifizierung die Möglichkeit, Informationen über Benutzerrollen in SAP beizubehalten und diese Rolleninformationen in der Plattform zu verwenden, um Rechte für Administrationsaufgaben oder den Zugriff auf Inhalte zuzuweisen.

Zugreifen auf die SAP-Authentifizierungsanwendung

Sie müssen der BI-Plattform Informationen über das SAP-System bereitstellen. Auf eine dedizierte Webanwendung können Sie über das Hauptadministrationstool der BI-Plattform, die Central Management Console (CMC), zugreifen. Um von der Homepage der CMC darauf zuzugreifen, wählen Sie **Authentifizierung**.

Authentifizieren von SAP-Benutzern

Mithilfe von Sicherheits-Plugins können Sie Vorgehensweisen der BI-Plattform bei der Authentifizierung von Benutzern erweitern und anpassen. Die SAP-Authentifizierung enthält ein SAP-Sicherheits-Plugin (`secSAPR3.dll`) für den Central Management Server der BI-Plattform. Dieses SAP-Sicherheits-Plugin bietet mehrere wichtige Vorteile:

- Es übernimmt die Funktion eines Authentifizierungs-Providers, der die Anwender-Anmeldedaten für den CMS beim SAP-System verifiziert. Wenn Benutzer sich direkt bei der BI-Plattform anmelden, können sie die SAP-Authentifizierung wählen und ihren üblichen SAP-Benutzernamen und das zugehörige Kennwort angeben. Die BI-Plattform ermöglicht zudem die Anmeldung bei SAP-Systemen unter Verwendung von Enterprise-Portal-Anmeldetickets.
- Es erleichtert das Erstellen neuer Benutzerkonten, da Rollen von SAP den BI-Plattform-Benutzergruppen zugeordnet werden können, und vereinfacht die Benutzerkontenverwaltung, da Sie den Benutzern und Gruppen in der BI-Plattform Rechte in einheitlicher Weise zuweisen können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Es verwaltet die SAP-Rollenauflistungen dynamisch. Wenn Sie der Plattform eine SAP-Rolle zuweisen, können sich alle Benutzer, die dieser Rolle angehören, beim System anmelden. Werden anschließend die Eigenschaften der SAP-Rolle geändert, müssen Sie die Liste in der BI-Plattform nicht aktualisieren oder regenerieren.
- Die SAP-Authentifizierung umfasst eine Webanwendung zur Konfiguration des Plugins. Auf diese Anwendung können Sie über den Bereich *Authentifizierung* in der Central Management Console (CMC) zugreifen.

9.5.2 Erstellen von Benutzerkonten für die BI-Plattform

Das BI-Plattform-System erfordert ein SAP-Benutzerkonto, das dazu berechtigt, auf die SAP-Listen für die Rollenzugehörigkeit zuzugreifen und SAP-Benutzer zu authentifizieren. Sie benötigen die Kontoanmeldedaten, um die BI-Plattform bei Ihrem SAP-System anzumelden. Eine allgemeine Anleitung zum Erstellen von SAP-Benutzerkonten und Zuweisen von Autorisierungen mithilfe von Rollen finden Sie in der SAP BW-Dokumentation.

Mit der Transaktion `SU01` können Sie neues SAP-Benutzerkonto mit dem Namen `CRYSTAL` erstellen. Mit der Transaktion `PFCG` können Sie eine neue Rolle mit dem Namen `CRYSTAL_ENTITLEMENT` erstellen. (Bei den Namen handelt es sich lediglich um eine Empfehlung.) Ändern Sie die Berechtigung der neuen Rolle, indem Sie Werte für die folgenden Berechtigungsobjekte festlegen:

Berechtigungsobjekt	Feld	Wert
Berechtigung für den Datenzugriff (S_DATASET)	Aktivität (ACTVT)	Lese-, Schreibzugriff (33, 34)
	Physischer Dateiname (FILENAME)	* (steht für Alle)
	Name des ABAP-Programms (PROGRAM)	*
Berechtigungsprüfung für RFC-Zugriff (S_RFC)	Aktivität (ACTVT)	16
	Name des zu schützenden RFC (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY
	Typ des zu schützenden RFC-Objektes (RFC_TYPE)	Funktionsgruppe (FUGR)
Anwenderstammpflege: Anwendergruppen (S_USER_GRP)	Aktivität (ACTVT)	Erstellen/Generieren und Anzeigen (03)
	Anwendergruppe in Anwenderstammpflege (CLASS)	* **Hinweis** Um mehr Sicherheit zu gewährleisten, können Sie die Benutzergruppen, deren Mitglieder Zugriff

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Berechtigungsobjekt	Feld	Wert
		auf die BI-Plattform benötigen, auch ausdrücklich aufführen.

Fügen Sie abschließend den Benutzer `CRYSTAL` der Rolle `CRYSTAL_ENTITLEMENT` hinzu.

> **Tipp**
>
> Falls Ihre Systemrichtlinien vorsehen, dass Benutzer ihr Kennwort bei der ersten Anmeldung beim System ändern, melden Sie sich jetzt mit dem Benutzerkonto `CRYSTAL` an, und geben Sie ein neues Kennwort ein.

9.5.3 Verbinden mit SAP-Berechtigungssystemen

Bevor Sie Rollen importieren oder BW-Inhalt in der BI-Plattform veröffentlichen können, müssen Sie Informationen über die SAP-Berechtigungssysteme bereitstellen, in die Sie integrieren möchten. Die BI-Plattform verwendet diese Informationen zum Verbinden mit dem SAP-Zielsystem beim Ermitteln der Rollenzugehörigkeiten und Authentifizieren von SAP-Benutzern.

9.5.3.1 Hinzufügen eines SAP-Berechtigungssystems

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
2. Doppelklicken Sie auf die Verknüpfung **SAP**.

   Die Einstellungen für das Berechtigungssystem werden angezeigt.

   > **Tipp**
   >
   > Wird in der Liste **Name des logischen Systems** bereits ein Berechtigungssystem angezeigt, klicken Sie auf die Schaltfläche **Neu**.

3. Geben Sie in das Feld **System** die dreistellige System-ID (SID) Ihres SAP-Systems ein.
4. Geben Sie im Feld **Client** die Clientnummer ein, die die BI-Plattform zur Anmeldung bei Ihrem SAP-System verwenden muss.
   Die BI-Plattform kombiniert Ihre System- und Clientdaten und fügt der Liste **Name des logischen Systems** einen Eintrag hinzu.
5. Stellen Sie sicher, dass das Kontrollkästchen **Deaktiviert** deaktiviert ist.

   > **Hinweis**
   >
   > Das Kontrollkästchen **Deaktiviert** signalisiert der BI-Plattform, dass ein bestimmtes SAP-System vorübergehend nicht verfügbar ist.

6. Füllen Sie die Felder **Message-Server** und **Anmeldegruppe** entsprechend aus, wenn Sie den Lastausgleich so eingerichtet haben, dass die Anmeldung der BI-Plattform über einen Message-Server erfolgen muss.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Sie müssen die entsprechenden Eingaben in der Datei `Dienste` auf Ihrem BI-Plattform-Rechner vornehmen, um den Lastausgleich zu aktivieren. Dies ist besonders dann wichtig, wenn die Implementierung sich auf mehrere Computer verteilt. Insbesondere zu berücksichtigen sind die Computer, die als Host für den CMS dienen, der Webanwendungsserver sowie alle Computer, die Ihre Authentifizierungskonten und -einstellungen verwalten.

7. Wenn Sie keinen Lastausgleich eingerichtet haben (oder wenn die BI-Plattform eine direkte Anmeldung beim SAP-System vornehmen soll), füllen Sie die Felder **Anwendungsserver** und **Systemnummer** entsprechend aus.
8. Geben Sie in die Felder **Benutzername**, **Kennwort** und **Sprache** den Benutzernamen, das Kennwort und den Sprachcode für das SAP-Konto ein, das die BI-Plattform für die Anmeldung bei SAP benutzen soll.

> **Hinweis**
>
> Diese Anmeldedaten müssen denen des Benutzerkontos entsprechen, das Sie für die BI-Plattform erstellt haben.

9. Klicken Sie auf **Aktualisieren**.

Wenn Sie mehrere Berechtigungssysteme hinzufügen, klicken Sie auf die Registerkarte **Optionen**, um das System festzulegen, das von der BI-Plattform standardmäßig verwendet wird (also das System, das zur Authentifizierung von Benutzern aufgerufen wird, die sich mit SAP-Anmeldedaten anzumelden versuchen, ohne jedoch ein bestimmtes SAP-System anzugeben).

Weitere Informationen

Erstellen von Benutzerkonten für die BI-Plattform [Seite 300]

9.5.3.2 Überprüfenk, ob das Berechtigungssystem ordnungsgemäß hinzugefügt wurde

1. Klicken Sie auf die Registerkarte **Rollenimport**.
2. Wählen Sie den Namen des Berechtigungssystems aus der Liste **Name des logischen Systems**.

   Wenn das Berechtigungssystem korrekt hinzugefügt wurde, enthält die Liste **Verfügbare Rollen** eine Liste mit Rollen, die für den Import ausgewählt werden können.

> **Tipp**
>
> Wenn in der Liste **Name des logischen Systems** keine Rollen sichtbar sind, suchen Sie auf der Seite nach einer entsprechenden Fehlermeldung. Dort erhalten Sie möglicherweise Hinweise darauf, wie das Problem behoben werden kann.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.5.3.3 Vorübergehendes Deaktivieren einer Verbindung mit einem SAP-Berechtigungssystem

In der CMC können Sie eine Verbindung zwischen der BI-Plattform und einem SAP-Berechtigungssystem vorübergehend deaktivieren. Diese Möglichkeit gewährleistet die Reaktionsfähigkeit der BI-Plattform auch in Situationen wie einer geplanten Ausfallzeit eines SAP-Berechtigungssystems.

1. Wechseln Sie in der CMC zum Verwaltungsbereich **Authentifizierung**.
2. Doppelklicken Sie auf die Verknüpfung **SAP**.
3. Wählen Sie in der Liste **Name des logischen Systems** das System aus, das Sie deaktivieren möchten.
4. Aktivieren Sie das Kontrollkästchen **Deaktiviert**.
5. Klicken Sie auf **Aktualisieren**.

9.5.4 Einstellen von SAP-Authentifizierungsoptionen

Die SAP-Authentifizierung umfasst eine Reihe von Optionen, die Sie bei der Integration der BI-Plattform in Ihr SAP-System angeben können. Zu diesen Optionen zählen:

- Aktivieren oder Deaktivieren der SAP-Authentifizierung
- Festlegen der Verbindungseinstellungen
- Verknüpfen von importierten Benutzern mit BI-Plattform-Lizenzmodellen.
- Konfigurieren der Einzelanmeldung beim SAP-System

9.5.4.1 So richten Sie die SAP-Authentifizierungsoptionen ein

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
2. Doppelklicken Sie auf die Verknüpfung **SAP**, und klicken Sie auf die Registerkarte **Optionen**.
3. Überprüfen und ändern Sie die folgenden Einstellungen nach Bedarf:

Einstellung	Beschreibung
SAP-Authentifizierung aktivieren	Heben Sie die Auswahl dieses Kontrollkästchens auf, um die SAP-Authentifizierung zu deaktivieren. **Hinweis** Zur Deaktivierung der SAP-Authentifizierung für ein bestimmtes SAP-System aktivieren Sie das betreffende Kontrollkästchen **Deaktiviert** auf der Registerkarte **Berechtigungssysteme**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Einstellung	Beschreibung
Stamm des Inhaltsordners	Legen Sie fest, an welcher Stelle die BI-Plattform mit der Replikation der BW-Ordnerstruktur in der CMC und im BI-Launchpad beginnen soll. Die Standardvorgabe ist `/SAP/2.0`, allerdings können Sie auch einen anderen Ordner angeben. Wenn Sie den Wert ändern möchten, muss dies sowohl in der CMC als auch in der Content Administration Workbench erfolgen.
Standardsystem	Wählen Sie ein SAP-Berechtigungssystem aus, das die BI-Plattform kontaktiert, um Benutzer zu authentifizieren, die sich mit SAP-Anmeldedaten anmelden, jedoch kein bestimmtes SAP-System angeben. **Hinweis** Wenn Sie ein Standardsystem auswählen, müssen Benutzer dieses Systems keine System-ID und keinen Client eingeben, wenn sie aus Clienttools wie Live Office oder Universe Designer mithilfe der SAP-Authentifizierung eine Verbindung herstellen. Wenn beispielsweise "SYS~100" als Standardsystem festgelegt wird, kann sich "SYS~100/user1" bei Auswahl der SAP-Authentifizierung als Benutzer1 anmelden.
Maximale Anzahl fehlgeschlagener Versuche des Zugriffs auf das Berechtigungssystem	Geben Sie an, wie viele Versuche die BI-Plattform unternehmen soll, um eine Verbindung zu einem SAP-System für Authentifizierungsanfragen herzustellen. Wenn Sie als Wert -1 festlegen, kann die BI-Plattform beliebig oft versuchen, eine Verbindung zum Berechtigungssystem herzustellen. Bei Angabe des Werts 0 kann die BI-Plattform nur einmal versuchen, eine Verbindung zum Berechtigungssystem herzustellen. **Hinweis** Verwenden Sie diese Einstellung zusammen mit **Berechtigungssystem für [Sekunden] deaktiviert lassen**, um festzulegen, wie die BI-Plattform mit vorübergehend nicht verfügbaren SAP-Berechtigungssystemen umgehen soll. Das System ermittelt über diese zwei Optionen, wann die Kommunikation mit einem nicht verfügbaren SAP-System abgebrochen wird und wann die Kommunikation mit diesem System wieder aufgenommen wird.
Berechtigungssystem für [Sekunden] deaktiviert lassen	Geben Sie an, wie viele Sekunden die BI-Plattform vor einem Neuversuch zur Authentifizierung der Benutzer bei einem SAP-System warten soll.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Einstellung	Beschreibung
	Wenn Sie z.B. 3 für **Max. erfolglose Zugriffe auf das Berechtigungssystem** festlegen, lässt die BI-Plattform maximal drei erfolglose Versuche zur Authentifizierung von Benutzern für ein beliebiges SAP-System zu. Bei einem vierten fehlgeschlagenen Versuch wird das System für die angegebene Zeit daran gehindert, zu versuchen, die Benutzer für dieses System zu authentifizieren.
Max. gleichzeitige Verbindungen pro System	Geben Sie an, wie viele Verbindungen zum SAP-System gleichzeitig geöffnet sein sollen. Wenn Sie beispielsweise 2 eingeben, werden von der BI-Plattform zwei Verbindungen zu SAP offen gehalten.
Anzahl der Verwendungen pro System	Geben Sie an, wie viele Anmeldungen beim SAP-System pro Verbindung zulässig sind. Wenn **Max. gleichzeitige Verbindungen pro System** beispielsweise auf 2 festgelegt ist und **Anzahl der Verwendungen pro Verbindung** auf 3 festgelegt ist, wird diese Verbindung von der BI-Plattform geschlossen und neu gestartet, sobald drei Anmeldungen für eine Verbindung erfolgt sind.
Zugriffslizenzbenutzer und **Namenslizenzbenutzer**	Geben Sie an, ob für neue Benutzerkonten Zugriffslizenzbenutzer-Lizenzen oder Namenslizenzen verwendet werden. Zugriffslizenzen geben die Anzahl der Personen an, die gleichzeitig mit der BI-Plattform verbunden sein können. Dieser Lizenztyp ist sehr flexibel, da mit einer geringen Anzahl von Zugriffslizenzen viele Benutzer unterstützt werden können. Je nach Häufigkeit und Dauer des Zugriffs auf das System können 100 Zugriffslizenzen beispielsweise 250, 500 oder auch 700 Benutzer unterstützen. Namenslizenzen sind mit bestimmten Benutzern verbunden und ermöglichen den Zugriff auf das System auf der Grundlage von Benutzername und Kennwort. Dieser Lizenztyp ermöglicht Benutzern den Zugriff auf das System unabhängig von der Anzahl der derzeit verbundenen Benutzer. **Hinweis** Die ausgewählte Option bewirkt keine Änderung der Anzahl oder des Typs der in der BI-Plattform installierten Benutzerlizenzen. Die entsprechenden Lizenzen müssen im System verfügbar sein.
Vollständigen Namen, E-Mail-Adresse und andere Attribute importieren	Legen Sie eine Prioritätsstufe für das SAP-Authentifizierungsplugin fest.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Einstellung	Beschreibung
	Die in den SAP-Konten verwendeten vollständigen Namen und Beschreibungen werden importiert und mit Benutzerobjekten in der BI-Plattform gespeichert.
Priorität der SAP-Attributbindung im Verhältnis zu anderen Attributbindungen festlegen	Gibt eine Priorität für die Bindung von SAP-Benutzerattributen (vollständiger Name und E-Mail-Adresse) an. Wenn die Option auf 1 festgelegt ist, haben SAP-Attribute immer dann Vorrang, wenn SAP-Plugins und andere Plugins (Windows AD und LDAP) aktiviert sind. Wenn die Option auf 3 festgelegt ist, haben Attribute von anderen aktivierten Plugins Priorität. Die Bindungen müssen auf unterschiedliche Werte festgelegt sein. Mehrere Authentifizierungs-Plugins auf denselben Bindungswert festzulegen kann zu unerwarteten Ergebnissen führen.

Legen Sie die folgenden Optionen fest, um den SAP-Einzelanmeldungsdienst zu konfigurieren:

Einstellung	Beschreibung
System-ID	Die System-ID, die von der BI-Plattform an das SAP-System übergeben wird, wenn der SAP-Einzelanmeldungsdienst durchgeführt wird.
Durchsuchen	Klicken, um die `Keystore`-Datei hochzuladen, die zur Aktivierung der SAP-Einzelanmeldung generiert wurde. Sie können den vollständigen Pfad zur Datei auch manuell eingeben.
Kennwort für den Schlüsselspeicher	Geben Sie das für den Zugriff auf die `Keystore`-Datei erforderliche Kennwort ein.
Kennwort für den privaten Schlüssel	Geben Sie das für den Zugriff auf das der `Keystore`-Datei entsprechende Zertifikat erforderliche Kennwort ein. Das Zertifikat ist im SAP-System gespeichert.
Alias des privaten Schlüssels	Geben Sie den für den Zugriff auf die `Keystore`-Datei erforderlichen Alias ein.

4. Klicken Sie auf **Aktualisieren**.

Weitere Informationen

Konfigurieren der SAP-Authentifizierung [Seite 299]

9.5.4.2 Ändern des Stamms im Inhaltsordner

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Doppelklicken Sie auf die Verknüpfung **SAP**.
3. Klicken Sie auf **Optionen**, und geben Sie den Namen des Ordners in das Feld **Stamm des Inhaltsordners** ein.

   Der hier eingegebene Ordnername entspricht dem Ordner, von dem aus die BI-Plattform mit der Replikation der BW-Ordnerstruktur beginnen soll.
4. Klicken Sie auf **Aktualisieren**.
5. Erweitern Sie in der BW-Workbench zur Content-Verwaltung **Enterprise-System**.
6. Klappen Sie **Verfügbare Systeme** auf, und doppelklicken Sie auf das System, mit dem die BI-Plattform verbunden wird.
7. Klicken Sie auf die Registerkarte **Layout**, und geben Sie unter **Inhaltsbasisordner** den Ordner ein, der in der BI-Plattform als SAP-Stammordner verwendet werden soll (z.B. `/SAP/2.0/`).

9.5.5 Importieren von SAP-Rollen

Durch den Import von SAP-Rollen in die BI-Plattform können Rollenmitglieder sich mit ihren üblichen SAP-Anmeldeinformationen am System anmelden. Außerdem ist die Einzelanmeldung aktiviert, so dass SAP-Benutzer automatisch bei der BI-Plattform angemeldet werden, sobald sie von innerhalb des SAP GUI oder eines SAP Enterprise Portals auf Berichte zugreifen.

> **Hinweis**
>
> Oft gibt es viele Anforderungen für die Aktivierung der Einzelanmeldung. In einigen Fällen ist es erforderlich, einen SSO-fähigen Treiber oder eine SSO-fähige Anwendung zu verwenden und sicherzustellen, dass der Server und der Webserver sich in derselben Domäne befinden

Für jede importierte Rolle erstellt die BI-Plattform eine Gruppe. Die Namen für die einzelnen Gruppen werden unter Berücksichtigung der folgenden Konventionen gebildet: **`<System-ID~Clientnumner@Rollenname>`**. Die neuen Gruppen können Sie im Verwaltungsbereich *Benutzer und Gruppen* der CMC anzeigen. Anhand dieser Gruppen kann auch die Objektsicherheit innerhalb der BI-Plattform definiert werden.

Ziehen Sie bei der Konfiguration der BI-Plattform für die Veröffentlichung und beim Importieren von Rollen in das System drei Hauptkategorien von Benutzern in Betracht:

- BI-Plattform-Administratoren

  Enterprise-Administratoren konfigurieren das System für die Veröffentlichung von Inhalten aus SAP. Sie importieren die entsprechenden Rollen, erstellen die benötigten Ordner und weisen diesen Rollen und Ordnern in der BI-Plattform Rechte zu.
- Content Publisher

  Content Publisher sind diejenigen Benutzer, welche die Rechte zum Veröffentlichen von Inhalten für Rollen besitzen. Der Sinn dieser Benutzerkategorie besteht darin, normale Rollenmitglieder von denjenigen Benutzern zu unterscheiden, die über Rechte zum Veröffentlichen von Berichten verfügen.
- Rollenmitglieder

  Rollenmitglieder sind Benutzer, die Rollen angehören, welche “Inhalte umfassen”. Das bedeutet, dass diese Benutzer zu Rollen gehören, für welche Berichte veröffentlicht werden. Sie besitzen Rechte zum *Anzeigen*, zum *Anzeigen auf Abruf* und zum *zeitgesteuerten Verarbeiten* für alle Berichte, die für diejenigen Rollen veröffentlicht wurden, denen sie angehören. Normale Rollenmitglieder können jedoch weder neue Inhalte noch aktualisierte Versionen von Inhalten veröffentlichen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Vor der ersten Veröffentlichung müssen Sie zunächst alle Rollen, die Inhalte veröffentlichen, und alle Rollen, die Inhalte umfassen, in die BI-Plattform importieren.

> **Hinweis**
>
> Es wird dringend empfohlen, die Aktivitäten der einzelnen Rollen getrennt zu halten. Beispielsweise ist es zwar möglich, von einer Administratorrolle aus zu veröffentlichen, es sollte jedoch nur von Content Publisher-Rollen aus veröffentlicht werden. Die Funktion von Rollen, die Inhalte veröffentlichen, besteht außerdem nur darin zu definieren, welche Benutzer Inhalte veröffentlichen können. Diese Rollen sollten daher keine Inhalte enthalten; Content Publisher sollten in Rollen veröffentlichen, die Inhalte umfassen und normalen Rollenmitgliedern zugänglich sind.

Weitere Informationen

Funktionsweise von Rechten in der BI-Plattform [Seite 124]
Verwalten von Sicherheitseinstellungen für Objekte in der CMC [Seite 133]

9.5.5.1 Importieren von SAP-Rollen

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
2. Doppelklicken Sie auf die Verknüpfung **SAP**.
3. Wählen Sie auf der Registerkarte **Optionen** je nach Lizenzvereinbarung entweder **Zugriffslizenzbenutzer** oder **Namenslizenzbenutzer** aus.

   Diese Option bewirkt keine Änderung der Anzahl oder des Typs der in der BI-Plattform installierten Benutzerlizenzen. Die entsprechenden Lizenzen müssen im System verfügbar sein.
4. Klicken Sie auf **Aktualisieren**.
5. Wählen Sie auf der Registerkarte **Rollenimport** aus der Liste **Name des logischen Systems** das gewünschte Berechtigungssystem aus.
6. Wählen Sie im Bereich *Verfügbare Rollen* die zu importierenden Rollen aus, und klicken Sie auf **Hinzufügen**.
7. Klicken Sie auf **Aktualisieren**.

9.5.5.2 Überprüfen, ob Rollen und Benutzer ordnungsgemäß importiert wurden

Bevor Sie mit dieser Aufgabe beginnen, notieren Sie sich den Benutzernamen und das Kennwort eines SAP-Benutzers, der zu einer der Rollen gehört, die Sie der BI-Plattform zugeordnet haben.

1. Für Java-BI-Launchpad rufen Sie `http://<webserver>:<portnumber>/BOE/BI` auf.

   Ersetzen Sie `<Webserver>` durch den Namen des Webservers und `<Portnummer>` durch die Portnummer für die BI-Plattform. Möglicherweise benötigen Sie von Ihrem Administrator den Namen des Webservers, die Portnummer oder die URL.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Wählen Sie aus der Liste **Authentifizierungstyp** die Option **SAP**.

> **Hinweis**
>
> Die Liste **Authentifizierungstyp** ist im BI-Launchpad standardmäßig ausgeblendet. Falls die Liste nicht angezeigt wird, bitten Sie Ihren Systemadminstrator, die Liste **Authentifizierungstyp** in der Datei `BIlaunchpad.properties` zu aktivieren, und starten Sie den Anwendungsserver anschließend neu.

3. Geben Sie das SAP-System und den Systemclient an, bei dem Sie sich anmelden möchten.
4. Geben Sie den Benutzernamen und das Kennwort eines zugeordneten Benutzers ein.
5. Klicken Sie auf **Anmelden**.

   Sie werden bei BI-Launchpad als der ausgewählte Benutzer angemeldet.

9.5.5.3 Aktualisieren von SAP-Rollen und -Benutzern

Nach der Aktivierung der SAP-Authentifizierung müssen regelmäßige Aktualisierungen von zugeordneten Rollen, die in die BI-Plattform importiert wurden, zeitgesteuert verarbeitet und ausgeführt werden. Dadurch ist gewährleistet, dass aktualisierte SAP-Rolleninformationen in BI-Plattform genau widergespiegelt werden.

Für die Ausführung und zeitgesteuerte Verarbeitung von Aktualisierungen für SAP- Rollen stehen zwei Optionen zur Verfügung:

- Nur Rollen aktualisieren: Bei Verwendung dieser Option werden nur die Verknüpfungen zwischen den aktuell zugeordneten Rollen aktualisiert, die in die BI-Plattform importiert wurden. Es wird empfohlen, diese Option nur dann zu verwenden, wenn Sie häufig Aktualisierungen ausführen müssen und Bedenken hinsichtlich der Systemressourcennutzung haben. Wenn Sie nur SAP-Rollen aktualisieren, werden keine neuen Benutzerkonten erstellt.
- Rollen und Aliase aktualisieren: Bei Verwendung dieser Option werden nicht nur Verknüpfungen zwischen Rollen aktualisiert, sondern auch neue Benutzerkonten in der BI-Plattform für Benutzeraliase erstellt, die zu Rollen im SAP-System hinzugefügt wurden.

> **Hinweis**
>
> Wenn Sie bei der Aktivierung der SAP-Authentifizierung nicht angegeben haben, dass Benutzeraliase automatisch für Aktualisierungen erstellt werden sollen, werden keine Konten für neue Aliase erstellt.

9.5.5.3.1 Zeitgesteuertes Verarbeiten von Aktualisierungen für SAP-Rollen

Nachdem Sie Rollen in der BI-Plattform zugeordnet haben, müssen Sie angeben, wie das System diese Rollen aktualisiert.

1. Klicken Sie auf die Registerkarte **Benutzeraktualisierung**.
2. Klicken Sie in der Sektion **Nur Rollen aktualisieren** oder im Bereich *Rollen und Aliase aktualisieren* auf *Zeitgesteuert verarbeiten*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Tipp**
>
> Um sofort eine Aktualisierung durchzuführen, klicken Sie auf **Jetzt aktualisieren**.

> **Tipp**
>
> Verwenden Sie die Option **Nur Rollen aktualisieren**, wenn Sie häufig aktualisieren möchten und Bedenken bezüglich der Systemressourcen haben. Das System benötigt mehr Zeit, um sowohl Rollen als auch Aliase zu aktualisieren.

Das Dialogfeld *Wiederholung* wird angezeigt.

3. Wählen Sie in der Liste **Objekt ausführen** eine Option aus, und geben Sie alle angeforderten Informationen zur zeitgesteuerten Verarbeitung in die vorgesehenen Felder ein.

   Bei der zeitgesteuerten Verarbeitung einer Aktualisierung stehen Ihnen die Wiederholungsmuster in der folgenden Tabelle zur Verfügung:

Wiederholungsmuster	Beschreibung
Stündlich	Die Aktualisierung wird stündlich ausgeführt. Sie legen die Startzeit sowie das Start- und Enddatum fest.
Täglich	Die Aktualisierung wird täglich oder alle `<n>` Tage ausgeführt (wobei `<n>` der von Ihnen festgelegten Anzahl an Tagen entspricht). Sie können die Startzeit sowie das Start- und Enddatum festlegen.
Wöchentlich	Die Aktualisierung wird einmal oder mehrmals pro Woche ausgeführt. Sie können die Tage der Ausführung, die Startzeit sowie das Start- und Enddatum festlegen.
Monatlich	Die Aktualisierung wird einmal monatlich oder alle n Monate ausgeführt. Sie können die Startzeit sowie das Start- und Enddatum festlegen.
Am n-ten Tag des Monats	Die Aktualisierung wird an einem bestimmten Tag des Monats ausgeführt. Sie können festlegen, an welchem Tag des Monats und zu welcher Uhrzeit die Aktualisierung ausgeführt wird, sowie Anfangs- und Enddatum der Ausführung bestimmen.
Am ersten Montag des Monats	Die Aktualisierung wird jeden Monat am ersten Montag ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am letzten Tag des Monats	Die Aktualisierung wird am letzten Tag jedes Monats ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Tag x der n-ten Woche des Monats	Die Aktualisierung wird an einem bestimmten Tag einer bestimmten Woche im Monat ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Kalender	Die Aktualisierung wird zu den Terminen ausgeführt, die in einem zuvor erstellten Kalender festgelegt wurden.

4. Klicken Sie auf **Zeitgesteuert verarbeiten**.
   Auf der Registerkarte **Benutzeraktualisierung** wird das Datum der nächsten zeitgesteuert verarbeiteten Rollenaktualisierung angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

➔ Tipp

Um die nächste zeitgesteuert verarbeitete Aktualisierung abzubrechen, klicken Sie im Bereich **Nur Rollen aktualisieren** oder *Rollen und Aliase aktualisieren* auf *Geplante Aktualisierungen abbrechen*.

9.5.6 Konfigurieren der Secure Network Communication (SNC)

In diesem Abschnitt wird die Konfiguration von SNC im Rahmen des Einrichtens der SAP-Authentifizierung für die BI-Plattform beschrieben.

Vor dem Einrichten der Vertrauenswürdigkeit zwischen den SAP- und BI-Plattform-Systemen müssen Sie sicherstellen, dass der SIA so konfiguriert wurde, dass er unter einem für SNC eingerichteten Konto gestartet und ausgeführt wird. Außerdem müssen Sie Ihr SAP-System so konfigurieren, dass es der BI-Plattform vertraut.

Weitere Informationen

SAP: Serverseitiges Vertrauen – Übersicht [Seite 311]

9.5.6.1 SAP: Serverseitiges Vertrauen – Übersicht

Dieser Abschnitt beschreibt die Vorgehensweise bei der Konfiguration des serverseitigen Vertrauens zwischen SAP Web Application Servern (Version 6.20 und höher) und SAP BusinessObjects Business Intelligence. Sie müssen ein serverseitiges Vertrauen einrichten, wenn Sie Berichtsbursting in mehreren Arbeitsgängen verwenden (für Veröffentlichungen, bei denen die Berichts-Query vom Kontext des Anwenders abhängt).

Zum serverseitigen Vertrauen gehört auch eine Identitätsmaskierung ohne Kennworteingabe. Um die Identität eines SAP-Anwenders ohne Angabe eines Kennworts anzunehmen, muss ein Anwender von SAP mithilfe einer sichereren Methode als der üblichen Anwendername- und Kennworteingabe identifiziert werden. (Ein SAP-Anwender mit dem Autorisierungsprofil `SAP_ALL` kann nicht die Identität eines anderen SAP-Anwenders annehmen, ohne dessen Kennwort zu kennen.)

Einrichten des serverseitigen Vertrauens mithilfe der SAP Cryptographic Library

Um ein serverseitiges Vertrauen für die BI-Plattform mithilfe der SAP Cryptographic Library zu ermöglichen, müssen Sie die relevanten Server unter Verwendung von Anmeldedaten ausführen, die durch einen registrierten SNC-Provider (Secure Network Communication) authentifiziert werden. Diese Anmeldedaten werden von SAP so konfiguriert, dass eine Identitätsmaskierung ohne Kennwort möglich ist. Für die BI-Plattform müssen Sie die

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Server, die in das Berichtsbursting involviert sind, unter Verwendung dieser SNC-Anmeldedaten ausführen, z.B. den Adaptive Job Server.

Sie benötigen 32-Bit-SNC-Binärdateien für 32-Bit-Prozesse bzw. 64-Bit-Binärdateien für 64-Bit-Prozesse. Die SAP Cryptographic Library wird zusammen mit der BI-Plattform installiert. Die SAP Cryptographic Library kann nur zum Einrichten des serverseitigen Vertrauens verwendet werden. Die Cryptographic Library ist für Windows und UNIX verfügbar.

Weitere Informationen über die Cryptographic Library finden Sie auf der SAP-Website in den SAP-Hinweisen 711093, 597059 und 397175.

Dem SAP-Server und der BI-Plattform müssen Zertifikate zugewiesen sein, die zum gegenseitigen Nachweis der Identität dienen. Jeder Server verfügt über ein eigenes Zertifikat und eine Liste von Zertifikaten für vertrauenswürdige Parteien. Um das serverseitige Vertrauen zwischen SAP und der BI-Plattform zu konfigurieren, müssen Sie eine kennwortgeschützte Gruppe von Zertifikaten erstellen. Eine solche Gruppe wird als "Persönliche Sicherheitsumgebung" (Personal Security Environment, PSE) bezeichnet. In diesem Abschnitt wird beschrieben, wie Sie solche PSEs erstellen und verwalten und wie Sie sie auf sichere Weise den BI-Plattform-Verarbeitungsservern zuweisen.

Client- und Server-SNC

Beim Client-SNC wird einem oder mehreren SAP-Anwendernamen in SU01 eine SNC-Namens-ID zugewiesen. Wird eine Anmeldeanforderung gesendet, wird der SNC-Name zusammen mit dem SAP-Namen an das SAP-System weitergeleitet, es wird jedoch kein Kennwort gesendet. Wenn der SNC-Name zum angegebenen SAP-Namen passt, wird die Anmeldung zugelassen. Im Folgenden wird ein clientseitiger Anmelde-String für eine direkte Anmeldung beim Anwendungshost gezeigt.

```
ASHOST =myserver.mydomain SYSNR=37 CLIENT=066 LANG=EN USER=USER123
SNC_MODE=1 SNC_QOP=9 SNC_LIB="/usr/local/lib/libsapcrypto.so"
SNC_PARTNERNAME="p:CN=TheServer, OU=Dept., O=TheCompany, C=FR"
SNC_MYNAME="p:CN=TheUser, O=TheCompany, C=US"
```

Damit dieser Anmeldeversuch erfolgreich ist, muss der SAP-Anwender USER123 `p:CN=TheUser`, `O=TheCompany`, `C=US in SU01` zugeordnet werden. Beim serverseitigen SNC ist es dagegen nicht erforderlich, die SNC-Namens-ID und den SAP-Anwendernamen einander ausdrücklich zuzuordnen. Der SNC-Name wird stattdessen in der Transaktion `SNC0` konfiguriert, damit eine Impersonation-ähnliche Anmeldung für “beliebige” Benutzer möglich wird, ohne dass das Kennwort des jeweiligen Benutzers benötigt wird. Beispiel:

```
ASHOST =myserver.mydomain SYSNR=37 CLIENT=066 LANG=EN SNC_MODE=1
SNC_QOP=9 SNC_LIB="/usr/local/lib/libsapcrypto.so"
SNC_PARTNERNAME="p:CN=TheServer, OU=Dept., O=TheCompany, C=FR"
SNC_MYNAME="p:CN=TheUser, O=TheCompany, C=US" EXTIDTYPE=UN EXTIDDATA=USER123
```

Die serverseitige SNC-Anmeldung mit Impersonation (oder Anmeldung über externe ID) ist wesentlich leistungsstärker als die clientseitige. Dieser Anmeldungstyp ermöglicht den Zugriff auf jedes beliebige SAP-Anwenderkonto im System. Andere Optionen für die Anmeldung mit externer ID sind Logon-Tickets und X.509-Client-Zertifikate.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

SAP-BusinessObjects-BI-Serververantwortlichkeiten

Bestimmte BI-Plattform-Server sind für die SAP-Integration in Bezug auf die Einzelanmeldung (SSO) von Bedeutung. Die folgende Tabelle zeigt diese Server und den SNC-Typ, den diese für bestimmte Aufgabenbereiche benötigen.

Server	SNC-Typ	Aufgabenbereich
Webanwendungsserver	Client	Rollenliste für SAP-Authentifizierung
BW Publisher-Dienst	Server	Auswahllisten und Personalisierung für dynamische Parameter in Crystal Reports
CMS	Client	Kennwort, Ticket, Überprüfen der Zugehörigkeit zur Rolle, Anwenderlisten
Page Server	Server	Crystal-Reports-Anzeige auf Abruf
Job Server	Server	Zeitgesteuerte Verarbeitung von Crystal Reports
Web Intelligence Processing Server	Server	Anzeige und zeitgesteuerte Verarbeitung von Web-Intelligence-Berichten und Eingabeaufforderungen mit Wertelisten (LOV)
Multi-Dimensional Analysis Service	Server	Stufe Detail

Hinweis

Für den Webanwendungsserver und den CMS wird Client-SNC verwendet. Sie benötigen daher eine explizite Zuordnung des SNC-Namens zum SAP-Benutzernamen. Diese wird in einer der Transaktionen `SU01` oder `SM30` für die Tabelle `USRACL` festgelegt.

9.5.6.2 Konfigurieren von SAP für serverseitiges Vertrauen

Die serverseitige Vertrauensstellung gilt nur für Crystal-Reports- und Web-Intelligence-Berichte, die auf Universen (`.unv`) basieren. Sie müssen SNC zur Verwendung mit der BI-Plattform einrichten. Weitere Informationen oder hilfreiche Hinweise zur Fehlerbehebung finden Sie in der SAP-Dokumentation, die mit dem SAP-Server bereitgestellt wurde.

9.5.6.2.1 Konfigurieren von SAP für serverseitiges Vertrauen

1. Stellen Sie sicher, dass Sie über Administrator-Anmeldedaten für SAP und für den Rechner, auf dem SAP ausgeführt wird, verfügen sowie über Administrator-Anmeldedaten für die BI-Plattform und den Rechner (bzw. die Rechner), auf dem es ausgeführt wird.
2. Stellen Sie sicher, dass sich die SAP Cryptographic Library und das SAPGENPSE-Tool auf dem SAP-Rechner im Verzeichnis (unter Windows): `<LAUFWERK>:\usr\sap\<SID>\SYS\exe\run\` befindet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Erstellen Sie eine Umgebungsvariable mit dem Namen `<SECUDIR>`, die auf das Verzeichnis verweist, in dem sich das Ticket befindet.

> **Hinweis**
>
> Diese Variable muss für den Anwender verfügbar sein, unter dem der *disp+work*-Prozess von SAP ausgeführt wird.

4. Wechseln Sie in der SAP GUI zur Transaktion RZ10, und ändern Sie das Instanzprofil in den Modus **Extended maintenance** (Erweiterte Verwaltung).
5. Verweisen Sie SAP-Profilvariablen im Profilbearbeitungsmodus auf die Cryptographic Library, und geben Sie dem SAP-System einen definierten Namen. Diese Variablen sollten auf der LDAP-Namenskonvention beruhen:

Tag	Bedeutung	Beschreibung
`CN`	Common Name (Üblicher Name)	Der alltägliche Name des Zertifikatsbesitzers.
`OU`	Organizational Unit (Organisationseinheit)	Z. B. "PG" für "Produktgruppe".
`O`	Unternehmen	Der Name des Unternehmens, für das das Zertifikat ausgegeben wurde.
`C`	Land	Das Land, in dem sich das Unternehmen befindet.

Z. B. für R21: `p:CN=R21, OU=PG, O=BOBJ, C=CA`

> **Hinweis**
>
> Das Präfix `p:` steht für die SAP Cryptographic Library. Es ist erforderlich, wenn innerhalb von SAP auf den definierten Namen (DN) verwiesen wird, ist jedoch beim Überprüfen von Zertifikaten in STRUST oder mithilfe von SAPGENPSE nicht sichtbar.

6. Geben Sie die folgenden Profilwerte ein, und ersetzen Sie sie ggf. mit den Werten für Ihr SAP-System:

Profilvariable	Wert
`ssf/name`	`SAPSECULIB`
`ssf/ssfapi_lib`	Vollständiger Pfad zur SAP Cryptographic Library
`sec/libsapsecu`	Vollständiger Pfad zur SAP Cryptographic Library
`snc/gssapi_lib`	Vollständiger Pfad zur SAP Cryptographic Library
`snc/identity/as`	Definierter Name (DN) des SAP-Sytems

7. Starten Sie die SAP-Instanz neu.
8. Wenn das System wieder ausgeführt wird, melden Sie sich an, und wechseln Sie zur Transaktion STRUST, die nun über zusätzliche Einträge für SNC und SSL verfügen sollte.
9. Klicken Sie mit der rechten Maustaste auf den SNC-Knoten, und klicken Sie dann auf **Erstellen**.
   Die in RZ10 angegebene Identität sollte nun angezeigt werden.
10. Klicken Sie auf **OK**.
11. Klicken Sie auf das Sperrsymbol, um für die SNC-PSE ein Kennwort festzulegen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Bewahren Sie dieses Kennwort sicher auf. Sie werden bei jedem Anzeigen oder Bearbeiten der SNC-PSE von STRUST nach diesem Kennwort gefragt.

12. Speichern Sie die Änderungen.

> **Hinweis**
>
> Wenn Sie Ihre Änderungen nicht speichern, wird der Anwendungsserver beim Aktivieren von SNC nicht wieder gestartet.

13. Kehren Sie zur Tansaktion RZ10 zurück, und geben Sie die übrigen SNC-Profilparameter ein:

Profilvariable	Parameter
`snc/accept_insecure_rfc`	`1`
`snc/accept_insecure_r3int_rfc`	`1`
`snc/accept_insecure_gui`	`1`
`snc/accept_insecure_cpic`	`1`
`snc/permit_insecure_start`	`1`
`snc/data_protection/min`	`1`
`snc/data_protection/max`	`3`
`snc/enable`	`1`

Das niedrigste Schutzniveau umfasst nur eine Authentifizierung (1), das höchste Niveau (3) steht für Datenschutz (3). Der Wert `snc/data_protection/use` gibt an, dass in diesem Fall nur Authentifizierung verwendet wird. Er kann jedoch auch auf (2) für Integrität, auf (3) für Datenschutz und auf (9) für maximal verfügbaren Schutz gesetzt werden. Die Werte `snc/accept_insecure_rfc`, `snc/accept_insecure_r3int_rfc`, `snc/accept_insecure_gui` und `snc/accept_insecure_cpic` sind auf (1) gesetzt und stellen sicher, dass vorherige (und möglicherweise nicht sichere) Kommunikationmethoden nach wie vor zulässig sind.

14. Starten Sie das SAP-System neu.

Sie müssen nun die BI-Plattform für serverseitiges Vertrauen konfigurieren.

9.5.6.3 Konfigurieren der BI-Plattform für serverseitiges Vertrauen

Führen Sie die folgenden Schritte aus, um die BI-Plattform für serverseitiges Vertrauen zu konfigurieren. Beachten Sie, dass diese Schritte auf Windows basieren. Da jedoch das SAP-Tool ein Befehlszeilentool ist, sind die unter Unix auszuführenden Schritte nahezu identisch.

1. Richten Sie die Umgebung ein.
2. Generieren Sie eine persönliche Sicherheitsumgebung (Personal Security Environment, PSE).
3. Konfigurieren Sie die BI-Plattform-Server

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Konfigurieren Sie den PSE-Zugriff.
5. Konfigurieren Sie die SNC-Einstellungen für die SAP-Authentifizierung.
6. Richten Sie dedizierte SAP-Servergruppen ein.

Weitere Informationen

So richten Sie die Umgebung ein [Seite 316]
Erstellen einer PSE [Seite 317]
Konfigurieren der BI-Servern [Seite 318]
Konfigurieren des PSE-Zugriffs [Seite 318]
Konfigurieren der SNC-Einstellungen für die SAP-Authentifizierung [Seite 319]
Verwenden von Servergruppen [Seite 320]

9.5.6.3.1 So richten Sie die Umgebung ein

Die BI-Plattform enthält eine Standard-SAP-Cryptographic-Library. Wenn Sie die Standardbibliothek verwenden, müssen Sie nur die letzten beiden Schritte durchführen: einen Unterordner erstellen und eine Umgebungsvariable hinzufügen. Um eine benutzerdefinierte Kopie der SAP Cryptographic Library zu konfigurieren, führen Sie alle Schritte aus.

Die Standard-SAP-Cryptographic-Library befindet sich im folgenden Verzeichnis:

- Windows: `<INSTALLVERZ>\sap\sapcrypto.dll`
- Unix: `<INSTALLVERZ>/sap/libsapcrypto.so`

Stellen Sie zunächst Folgendes sicher:

- Die SAP Cryptographic Library wurde auf dem Host erweitert, auf dem die BI-Plattform-Verarbeitungsserver ausgeführt werden.
- Die erforderlichen SAP-Systeme wurden so konfiguriert, dass die SAP Cryptographic Library als SNC-Provider verwendet wird.

Bevor Sie mit der PSE-Verwaltung beginnen können, müssen Sie die Bibliothek, das Tool und die Umgebung, in der die PSEs gespeichert werden, einrichten

1. Kopieren Sie die SAP Cryptographic Library (einschließlich des PSE-Verwaltungstools) in einen Ordner auf dem Rechner, auf dem die BI-Plattform ausgeführt wird.

   Beispiel: `C:\Programme\SAP\Crypto`
2. Fügen Sie diesen Ordner der Umgebungsvariable `<PATH>` hinzu.
3. Fügen Sie die systemweite Umgebungsvariable `<SNC_LIB>` hinzu, die auf die Cryptographic Library verweist.

   Beispiel: `C:\Programme\SAP\Crypto\sapcrypto.dll`

> **Hinweis**
>
> Der Pfad darf maximal 100 Zeichen umfassen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Erstellen Sie einen Unterordner mit dem Namen **sec**.

   Beispiel: `C:\Programme\SAP\Crypto\sec`
5. Fügen Sie die systemweite Umgebungsvariable **<SECUDIR>** hinzu, die auf den Ordner **sec** verweist.

Weitere Informationen

Konfigurieren von SAP für serverseitiges Vertrauen [Seite 313]

9.5.6.3.2 Erstellen einer PSE

SAP akzeptiert BI-Server als vertrauenswürdige Einheiten, wenn die entsprechenden BI-Server über eine PSE verfügen und die PSE mit SAP verknüpft ist. Dieses "Vertrauen" zwischen den SAP- und BI-Plattform-Komponenten wird durch Freigabe der öffentlichen Versionen der Zertifikate beider Einheiten erreicht. Zunächst muss eine PSE für die BI-Plattform erstellt werden, die automatisch ein eigenes Zertifikat erstellt.

1. Öffnen Sie eine Eingabeaufforderung, und führen Sie den Befehl **sapgenpse.exe gen_pse -v -p BOE.pse** im Cryptographic Library-Ordner aus.
2. Legen Sie eine PIN und den definierten Namen (DN) für Ihr BI-Plattform-System fest.

   Beispiel: **CN=MyBOE01, OU=PG, O=BOBJ, C=CA**.

   Sie haben eine standardmäßige PSE und deren eigenes Zertifikat erstellt.
3. Exportieren Sie das Zertifikat der PSE mithilfe des folgenden Befehls:

   ```
   sapgenpse.exe export_own_cert -v -p BOE.pse -o <MyBOECert.crt>
   ```
4. Wechseln Sie in der SAP GUI zur Transaktion STRUST, und öffnen Sie die mit Ihrem SAP-System verbundene System-PSE.

   Sie werden u.U. aufgefordert, das zuvor dieser System-PSE zugewiesene Kennwort einzugeben.
5. Importieren Sie die zuvor erstellte Datei **<MyBOECert.crt>**, indem Sie links unten im STRUST-Transaktionsbild auf die Schaltfläche "Zertifikat importieren" klicken.

   Die Zertifikate von SAPGENPSE sind Base64-kodiert. Stellen Sie sicher, dass Sie beim Importieren der Zertifikate die Base64-Kodierung auswählen.
6. Um das BI-Plattform-Zertifikat der PSE-Zertifikatsliste des SAP-Servers hinzuzufügen, klicken Sie auf die Schaltfläche **Add to certificate list** (Der Zertifikatsliste hinzufügen).
7. Speichern Sie Ihre Änderungen in STRUST.
8. Klicken Sie auf die Schaltfläche **Export** (Exportieren), und geben Sie dem Zertifikat einen Dateinamen.

   Beispiel: **MySAPCert.crt**.

   > **Hinweis**
   >
   > Behalten Sie Base64 als Format bei.
9. Wechseln Sie zur Transaktion SNC0
10. Fügen Sie einen neuen Eintrag hinzu. Beachten Sie hierbei Folgendes:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Sie können eine beliebige System-ID wählen, sie muss jedoch Ihr BI-Plattform-System repräsentieren.
- Der SNC-Name ist der definierte Name (DN) (mit Präfix `p:`), den Sie beim Erstellen der PSE für die BI-Plattform festgelegt haben (in Schritt 2).
- Die beiden Kontrollkästchen **Entry for RFC activated** (Eintrag für RFC aktiviert) und **Entry for ext. ID activated** (Eintrag für ext. ID aktiviert) sind ausgewählt:

11. Um das exportierte Zertifikat der BI-Plattform-PSE hinzufügen, führen Sie in der Eingabeaufforderung den folgenden Befehl aus:

```
sapgenpse.exe maintain_pk -v -a <MySAPCert.crt> -p BOE.pse
```

Die SAP Cryptographic Library wurde auf dem BI-Plattform-Rechner installiert. Sie haben eine PSE erstellt, die von BI-Servern verwendet wird, um sich bei den SAP-Servern zu identifizieren. SAP und die BI-Plattform-PSE haben Zertifikate ausgetauscht. SAP ermöglicht Einheiten mit Zugriff auf die BI-Plattform-PSE die Durchführung von RFC-Anrufen und die Identitätsmaskierung ohne Kennwort.

Weitere Informationen

Konfigurieren der BI-Servern [Seite 318]

9.5.6.3.3 Konfigurieren der BI-Servern

Nach dem Erstellen einer PSE für die BI-Plattform müssen Sie eine geeignete Serverstruktur für die SAP-Verarbeitung konfigurieren. Im Folgenden wird beschrieben, wie Sie einen Knoten für SAP-Verarbeitungsserver erstellen, um auf Knotenebene Anmeldedaten für das Betriebssystem festzulegen.

> **Hinweis**
>
> In dieser Version der BI-Plattform werden Server nicht mehr im Central Configuration Manager (CCM) konfiguriert. Stattdessen muss ein neuer Server Intelligence Agent (SIA) erstellt werden.

1. Erstellen Sie im CCM einen neuen Knoten für die SAP-Verarbeitungsserver

   Geben Sie dem Knoten einen geeigneten Namen, z.B. `SAPProcessor`.
2. Fügen Sie dem neuen Knoten im CMC die benötigten Verarbeitungsserver hinzu, und starten Sie dann die neuen Server.

9.5.6.3.4 Konfigurieren des PSE-Zugriffs

Nachdem Sie den BI-Plattform-Knoten und die Server konfiguriert haben, müssen Sie den PSE-Zugriff mithilfe des SAPGENPSE-Tools konfigurieren.

1. Führen Sie in der Eingabeaufforderung folgenden Befehl aus:

```
sapgenpse.exe seclogin -p SBOE.pse
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Sie werden aufgefordert, die PSE-PIN einzugeben. Wenn Sie das Tool unter Verwendung derselben Anmeldedaten ausführen, die auch von den SAP-Verarbeitungsservern der BI-Plattform verwendet werden, müssen Sie keinen Benutzernamen angeben.

2. Um zu überprüfen, ob die SSO-Verknüpfung erstellt wurde, zeigen Sie den PSE-Inhalt mithilfe des folgenden Befehls an:

   sapgenpse.exe maintain_pk -l

   Das Ergebnis sollte etwa so aussehen:

```
C:\Documents and Settings\username\Desktop\sapcrypto.x86\ntintel>sapgenpse.exe
maintain_pk -l
 maintain_pk for PSE "C:\Documents and Settings\username\My Documents\snc\sec
\bobjsapproc.pse"
*** Object <PKList> is of the type <PKList_OID> ***

1. ------------------------------------------------------------
            Version:                  0 (X.509v1-1988)
            SubjectName:              CN=R21Again, OU=PG, O=BOBJ, C=CA
            IssuerName:               CN=R21Again, OU=PG, O=BOBJ, C=CA
            SerialNumber:             00
            Validity  -  NotBefore:   Wed Nov 28 16:23:53 2007 (071129002353Z)
                                                                 NotAfter:    Thu
Dec 31 16:00:01 2037 (380101000001Z)
            Public Key Fingerprint:   851C 225D 1789 8974 21DB 9E9B 2AE8 9E9E
            SubjectKey:               Algorithm RSA (OID 1.2.840.113549.1.1.1),
NULL


C:\Documents and Settings\username\Desktop\sapcrypto.x86\ntintel>
```

   Nach erfolgreicher Ausführung des Befehls **seclogin** sollten Sie nicht erneut zur Eingabe der PSE-PIN aufgefordert werden.

> **Hinweis**
>
> Wenn Probleme im Zusammenhang mit dem PSE-Zugriff auftreten, verwenden Sie das Argument *-O*, um den Zugriff einzurichten. Wenn Sie beispielsweise den PSE-Zugriff auf einen bestimmten Benutzer in einer bestimmten Domäne ermöglichen möchten, geben Sie unter Windows den folgenden Befehl ein:
>
> ```
> sapgenpse seclogin -p SBOE.pse -O SYSTEM
> ```

9.5.6.3.5 Konfigurieren der SNC-Einstellungen für die SAP-Authentifizierung

Im Anschluss an die Konfiguration des PSE-Zugriffs müssen Sie die SAP-Authentifizierungseinstellungen in der CMC konfigurieren.

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
2. Doppelklicken Sie auf die Verknüpfung **SAP**.

   Die Einstellungen für das Berechtigungssystem werden angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Klicken Sie auf der Seite **SAP-Authentifizierung** auf die Registerkarte *SNC-Einstellungen*.
4. Wählen Sie aus der Liste **Name des logischen Systems** das Berechtigungssystem.
5. Wählen Sie unter "**Grundlegende Einstellungen**" *Secure Network Communication (SNC) aktivieren* aus.
6. Wählen Sie die Option **Standard verwenden** aus, um den Standardpfad für die Bibliothek zu übernehmen, oder wählen Sie die Option **Benutzerdefinierten Pfad definieren** aus, um den Speicherort zu ändern.
7. Wählen Sie unter "*Qualität der Sicherung*" die gewünschte Sicherungsebene aus,

   beispielsweise **Authentifizierung**.

   > **Hinweis**
   >
   > Achten Sie darauf, dass Sie nicht die für das SAP-System konfigurierte Schutzebene überschreiten. Die Sicherungsebene kann angepasst werden und wird durch die Anforderungen Ihres Unternehmens und die Fähigkeiten der SNC-Bibliothek bestimmt.

8. Geben Sie unter *Einstellungen zur gegenseitigen Authentifizierung* den SNC-Namen des SAP-Systems ein.

   Das SNC-Namensformat hängt von der SNC-Bibliothek ab. Bei Verwendung der SAP-Kryptografiebibliothek wird der Distinguished Name entsprechend LDAP-Konventionen empfohlen. Dem Namen muss das Präfix `p:` vorangestellt sein.
9. Stellen Sie sicher, dass der SNC-Name der Anmeldedaten, unter denen die BI-Plattform-Server ausgeführt werden, im Feld **SNC-Name des Enterprise-Systems** angezeigt wird.

   Wenn mehrere SNC-Namen konfiguriert sind, sollte dieses Feld leer gelassen werden.
10. Geben Sie die definierten Namen (DNs) des SAP-Systems und der BI-Plattform-PSE an.

9.5.6.3.6 Verwenden von Servergruppen

Wenn die Verarbeitungsserver (Crystal Reports oder Web Intelligence) nicht unter Anmeldedaten laufen, die Zugriff auf das PSE haben, müssen Sie eine separate Servergruppe erstellen, die nur diese Server und die benötigten Unterstützungsserver enthält. Weitere Informationen sowie Beschreibungen der verschiedenen BI-Plattform-Server finden Sie im Kapitel “"Architektur"”.

Bei der Konfiguration der Verarbeitungsserver für SAP-Inhalte stehen drei Optionen zur Auswahl:

1. Verwenden eines einzigen SIA für alle BI-Plattform-Server, die alle Anmeldedaten mit Zugriff auf die PSE benutzen. Das ist die einfachste Option. Es müssen keine Servergruppen erstellt werden. Diese Methode ist die unsicherste, da eine unnötige Anzahl von Servern Zugriff auf das PSE hat.
2. Erstellen Sie einen zweiten SIA mit Zugriff auf das PSE und fügen Sie ihn zu den Crystal-Reports- oder Web-Intelligence-Verarbeitungsservern hinzu. Löschen Sie alle doppelt vorhandenen Server aus dem ursprünglichen SIA. Es müssen keine Servergruppen erstellt werden, aber es haben weniger Server Zugriff auf das PSE.
3. Erstellen Sie einen SIA, der ausschließlich von SAP verwendet wird, und Zugriff auf das PSE hat. Fügen Sie diesem die Verarbeitungsserver für Crystal Reports oder Web Intelligence hinzu. Bei dieser Option sollten nur SAP-Inhalte auf diesen Servern verarbeitet werden und, wichtiger, SAP-Inhalte sollten nur auf diesen Servern ausgeführt werden. Da in diesem Szenario Inhalte zu bestimmten Servern geleitet werden müssen, müssen Sie Servergruppen für den SIA erstellen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Richtlinien für die Verwendung von Servergruppen

Die Servergruppe muss auf den SIA verweisen, der ausschließlich für SAP-Inhalte verwendet wird. Außerdem muss die Servergruppe auf die folgenden Server verweisen:

- Adaptive Server
- Adaptive Job Server

Alle SAP-Inhalte, Web-Intelligence-Dokumente und Crystal-Reports-Berichte müssen über die strengste Zuordnung mit der Servergruppe verknüpft werden, d.h., sie müssen auf Servern in der Gruppe ausgeführt werden. Wenn diese Zuordnung auf Objektebene geschieht, sollte die Servergruppeneinstellung auch für die Einstellungen sowohl für zeitgesteuerte Verarbeitung als auch Publikationen übernommen werden.

Um zu verhindern, dass andere Inhalte (nicht SAP) auf den speziellen SAP-Verarbeitungsservern verarbeitet werden, sollten Sie eine weitere Servergruppe erstellen, die alle Server unter dem ursprünglichen SIA enthält. Es wird empfohlen, dass Sie eine strenge Zuordnung zwischen diesen Inhalten und der Nicht-SAP-Servergruppe einrichten.

9.5.6.4 Konfigurieren von Veröffentlichungen mit mehreren Arbeitsgängen

Fehlerbehebung für Veröffentlichungen mit mehreren Arbeitsgängen

Wenn im Zusammenhang mit Veröffentlichungen mit mehreren Arbeitsgängen Probleme auftreten, aktivieren Sie die Ablaufverfolgung für die CR- oder MDA-Treiber (Crystal Reports/Multidimensional Data Access) für SAP und überprüfen die Anmeldezeichenfolge, die für jeden Job oder Empfänger verwendet wurde. Diese Anmeldezeichenfolgen sollten dem folgenden Beispiel entsprechen:

```
 SAP: Successfully logged on to SAP server.
Logon handle: 1. Logon string: CLIENT=800 LANG=en
ASHOST="vanrdw2k107.sap.crystald.net" SYSNR=00 SNC_MODE=1 SNC_QOP=1
SNC_LIB="C:\WINDOWS\System32\sapcrypto.dll"
SNC_PARTNERNAME="p:CN=R21Again, OU=PG, O=BOBJ, C=CA" EXTIDDATA=HENRIKRPT3
EXTIDTYPE=UN
```

Die Anmeldezeichenfolge muss über den richtigen **EXTIDTYPE=UN** (für Anwendername) verfügen, und **EXTIDDATA** sollte der SAP-Anwendername des Empfängers sein. In diesem Beispiel war der Anmeldeversuch erfolgreich.

9.5.6.5 Workflow für die Integration in Secure Network Communication

Die BI-Plattform unterstützt Umgebungen, die Secure Network Communication (SNC) für die Authentifizierung und Datenverschlüsselung verschiedener SAP-Komponenten integrieren. Wenn Sie die SAP Cryptographic Library (oder ein anderes externes Sicherheitsprodukt, das die SNC-Schnittstelle verwendet) implementiert

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

haben, müssen Sie weitere Werte einstellen, um die BI-Plattform erfolgreich in Ihre gesicherte Umgebung zu integrieren.

Um die BI-Plattform für die Verwendung von Secure Network Communication (SNC) zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Konfigurieren Sie die BI-Plattform-Server, damit sie unter einem geeigneten Benutzerkonto gestartet und ausgeführt werden.
2. Konfigurieren Sie das SAP-System so, dass Ihr BI-Plattform-System als vertrauenswürdig erkannt wird.
3. Konfigurieren Sie die SNC-Einstellungen in der Verknüpfung "SNC" der Central Management Console .
4. Importieren Sie SAP-Rollen und -Benutzer in die BI-Plattform.

Weitere Informationen

Importieren von SAP-Rollen [Seite 307]
Konfigurieren von SAP für serverseitiges Vertrauen [Seite 313]
Konfigurieren der BI-Plattform für serverseitiges Vertrauen [Seite 315]

9.5.6.6 Konfigurieren der SNC-Einstellungen in der Central Management Console

Bevor Sie SNC-Einstellungen konfigurieren können, müssen Sie der BI-Plattform ein neues Berechtigungssystem hinzufügen, dafür sorgen, dass sich die SNC-Bibliotheksdatei in einem bekannten Verzeichnis befindet, und eine Umgebungsvariable namens **`<RFC_LIB>`** erstellen, die auf die Datei zeigt.

1. Klicken Sie auf der Seite **SAP-Authentifizierung** auf die Registerkarte *SNC-Einstellungen*.
2. Wählen Sie aus der Liste **Name des logischen Systems** das Berechtigungssystem.
3. Wählen Sie unter "**Grundlegende Einstellungen**" *Secure Network Communication (SNC) aktivieren* aus.
4. Wenn Sie die SAP-Authentifizierung für die Nutzung von `.unx`-Universen oder OLAP-BICS-Verbindungen konfigurieren und beabsichtigen, STS zu verwenden, aktivieren Sie das Kontrollkästchen **Kommunikation über unsichere eingehende RFC-Verbindungen unterbinden**.
5. Wählen Sie die Option **Standard verwenden** aus, um den Standardpfad für die Bibliothek zu übernehmen, oder wählen Sie die Option **Benutzerdefinierten Pfad definieren** aus, um den Speicherort zu ändern.

   Der Anwendungsserver und der CMS müssen auf demselben Betriebssystemtyp mit demselben Pfad zur Kryptografiebibliothek ausgeführt werden.
6. Wählen Sie unter "*Qualität der Sicherung*" die gewünschte Sicherungsebene aus,

   beispielsweise **Authentifizierung**.

   > **Hinweis**
   >
   > Die Sicherungsebene kann angepasst werden und wird durch die Anforderungen Ihres Unternehmens und die Fähigkeiten der SNC-Bibliothek bestimmt.
7. Geben Sie unter *Einstellungen zur gegenseitigen Authentifizierung* den SNC-Namen des SAP-Systems ein.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Das SNC-Namensformat hängt von der SNC-Bibliothek ab. Bei Verwendung der SAP-Kryptografiebibliothek wird der Distinguished Name entsprechend LDAP-Konventionen empfohlen. Dem Namen muss das Präfix `p:` vorangestellt sein.

8. Stellen Sie sicher, dass der SNC-Name der Anmeldedaten, unter denen die BI-Plattform-Server ausgeführt werden, im Feld **SNC-Name des Enterprise-Systems** angezeigt wird.

   Wenn mehrere SNC-Namen konfiguriert sind, lassen Sie dieses Feld leer.
9. Klicken Sie auf **Speichern**.
10. Klicken Sie auf der *SAP-Authentifizierungsseite* auf die Registerkarte **Berechtigungssysteme**.
    Die Option **SNC-Name** wird unter der Option **Sprache** angezeigt.
11. Geben Sie im Feld **SNC-Name** den SNC-Namen ein, den Sie auf dem SAP-BW-Server konfiguriert haben.

    Der Name sollte identisch sein mit dem, der verwendet wurde, um die BI-Plattform gegenüber dem SAP-System als vertrauenswürdig zu konfigurieren.

    Wenn Sie das Insight-to-Action-Framework zur Aktivierung der Bericht-zu-Bericht-Schnittstelle verwenden, kann es bis zu 10 Minuten dauern, bis der SNC aktiviert ist oder die Änderungen an den SNC-Einstellungen wirksam werden. Um ein sofortiges Update auszulösen, führen Sie einen Neustart des Adaptive Processing Servers durch, auf dem der Dienst "Insight to Action" ausgeführt wird.

Weitere Informationen

Verbinden mit SAP-Berechtigungssystemen [Seite 301]

9.5.6.7 So verbinden Sie einen berechtigten Benutzer mit einem SNC-Namen

1. Melden Sie sich bei Ihrem SAP BW-System an, und führen Sie die Transaktion `SU01` aus.

   Der Anfangsbildschirm "User Maintenance" (Benutzerverwaltung) wird geöffnet.
2. Geben Sie im Feld **User (Benutzer)** den Namen des SAP-Kontos ein, das als berechtigter Benutzer konfiguriert ist, und klicken Sie dann in der Symbolleiste auf die Schaltfläche **Change (Ändern)**.

   Das Dialogfeld "Maintain User" (Benutzer verwalten) wird geöffnet.
3. Klicken Sie auf die Registerkarte "SNC".
4. Geben Sie im Feld **SNC name** (SNC-Name) das `SNC-BENUTZERKONTO` ein, das Sie oben in Schritt 2 eingegeben haben.
5. Klicken Sie auf **Speichern**.

9.5.6.8 So fügen Sie der SNC-Zugriffskontrollliste eine System-ID hinzu

1. Melden Sie sich bei Ihrem SAP BW-System an, und führen Sie die Transaktion `SNC0` aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Das Dialogfeld "SNC: Access Control List (ACL) for Systems: Overview" (SNC: Zugriffskontrolllisten für Systeme: Überblick) wird geöffnet.

2. Klicken Sie in der Symbolleiste auf **New Entries** (Neue Einträge).

   Das Dialogfeld "New Entries: Details of Added Entries" (Neue Einträge: Details hinzugefügter Einträge) wird geöffnet.

3. Geben Sie den Namen Ihres BI-Plattform-Computers im Feld **System ID** ein.
4. Geben Sie `p:<SNC-BENUTZERNAME>` im Feld **SNC user name** (SNC-Benutzername) ein, wobei `SNC-BENUTZERNAME` für das Konto steht, das Sie beim Konfigurieren der BI-Plattform-Server verwendet haben.

   > **Hinweis**
   >
   > Wenn Ihr SNC-Provider gssapi32.dll ist, verwenden Sie bei Eingabe des SNC-BENUTZERNAMENS Großbuchstaben. Sie müssen den Domänennamen einschließen, wenn Sie das Benutzerkonto angeben. Beispiel: Domäne\Benutzername.

5. Wählen Sie **Entry for RFC activated** (Eintrag für RFC aktiviert) und **Entry for ext. ID activated** (Eintrag für ext. ID aktiviert) aus.
6. Deaktivieren Sie alle anderen Optionen, und klicken Sie auf **Save** (Speichern).

9.5.7 Einrichten der Einzelanmeldung beim SAP-System

Verschiedene BI-Plattform-Client- und Backend-Dienste interagieren mit NetWeaver-ABAP-Backendsystemen in einer integrierten Umgebung. Es ist sinnvoll, die Einzelanmeldung von der BI-Plattform zu diesen Backend-Systemen (normalerweise BW) einzurichten. Nach der Konfiguration des ABAP-Systems als externes Authentifizierungssystem wird mithilfe von SAP-Token ein Mechanismus bereitgestellt, der die Einzelanmeldung für alle BI-Plattform-Clients und -Dienste unterstützt, die eine Verbindung mit NetWeaver-ABAP-Systemen herstellen.

Zum Aktivieren der Einzelanmeldung am SAP-System erstellen Sie eine `Keystore`-Datei und ein entsprechendes Zertifikat. Verwenden Sie das `keytool`-Befehlszeilenprogramm zum Erzeugen der Datei und des Zertifikats. Das Programm keytool ist standardmäßig im Verzeichnis `sdk/bin` für die einzelnen Plattformen installiert.

Das Zertifikat muss mit der CMC zum SAP-ABAP-BW-System und zur BI-Plattform hinzugefügt werden.

> **Hinweis**
>
> Das SAP-Authentifizierungs-Plugin muss konfiguriert werden, bevor Sie die Einzelanmeldung an der von SAP BW verwendeten Datenbank einrichten können.

9.5.7.1 Erzeugen einer keystore-Datei

Mit dem Programm PKCS12Tool werden keystore-Dateien und Zertifikate erzeugt, die für die Einrichtung der Einzelanmeldung bei der SAP-Datenbank benötigt werden. Die folgende Tabelle enthält die Standardspeicherorte der Datei `PKCS12Tool.jar` für die einzelnen unterstützten Plattformen:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Plattform	Standardspeicherort
Windows	`<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\java\lib`
Unix	`sap_bobj/enterprise_xi40/java/lib`

1. Starten Sie eine Befehlseingabeaufforderung, und navigieren Sie zu dem Verzeichnis, in dem sich das Programm PKCS12Tool befindet
2. Führen Sie den folgenden Befehl aus, um eine keystore-Datei mit Standardeinstellungen zu generieren:

```
java -jar PKCS12Tool.jar
```

Die Dateien `cert.der` und `keystore.p12` werden im selben Verzeichnis generiert. Die Dateien enthalten die folgenden Standardwerte:

Parameter	Standard
-keystore	keystore.p12
-alias	myalias
-storepass	123456
-dname	CN=CA
-validity	365
-cert	cert.der

Tipp

Um die Standardwerte außer Kraft zu setzen, führen Sie das Tool gemeinsam mit dem Parameter `-?` aus. Die folgende Meldung wird angezeigt:

```
Usage: PKCS12Tool <options>
       -keystore <filename(keystore.p12)>
       -alias <key entry alias(myalias)>
       -storepass <keystore password(123456)>
       -dname <certificate subject DN(CN=CA)>
       -validity <number of days(365)>
       -cert <filename (cert.der)>
        (No certificate is generated when importing a keystore)
       -disablefips
       -importkeystore <filename>
```

Sie können anhand der Parameter die Standardwerte außer Kraft setzen.

9.5.7.2 Exportieren des Zertifikats für den öffentlichen Schlüssel

Sie müssen ein Zertifikat für die Schlüsseldatei erstellen und exportieren.

1. Starten Sie eine Eingabeaufforderung, und navigieren Sie zu dem Verzeichnis, in dem das Keytool-Programm gespeichert ist

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Exportieren Sie ein Schlüsselzertifikat für die Schlüsselspeicherdatei mit folgendem Befehl.

```
keytool -exportcert -keystore <keystore> -storetype pkcs12 -file <filename>
-alias <alias>
```

Ersetzen Sie <Schlüsselspeicher> durch den Namen der Schlüsselspeicherdatei.
Ersetzen Sie <Dateiname> durch den Namen des Zertifikats.
Ersetzen Sie <Alias> durch den zum Erstellen der Schlüsselspeicherdatei verwendeten Alias.

3. Geben Sie bei Eingabeaufforderung das Kennwort ein, das Sie für die Schlüsselspeicherdatei angegeben haben.

Es befinden sich nun eine Schlüsselspeicherdatei und ein Zertifikat in dem Verzeichnis mit dem keytool-Programm.

9.5.7.3 Importieren der Zertifikatsdatei in das ABAP-Zielsystem

Sie benötigen eine Schlüsselspeicherdatei und ein zugehöriges Zertifikat für Ihre BI-Plattform-Implementierung, um die folgende Aufgabe auszuführen.

> **Hinweis**
>
> Die Aktion kann nur auf einem ABAP-basierten SAP-System ausgeführt werden.

1. Stellen Sie über die SAP GUI eine Verbindung zu Ihrem SAP ABAP-BW-System her.

   > **Hinweis**
   >
   > Sie sollten sich als Benutzer mit Administratorrechten anmelden.

2. Führen Sie STRUSTSSO2 in der SAP GUI aus.
   Das System wird auf den Import der Zertifikatdatei vorbereitet.
3. Wechseln Sie zur Registerkarte **Certificate** (Zertifikat).
4. Stellen Sie sicher, dass das Kontrollkästchen **Use Binary option** (Binäroption verwenden) aktiviert ist.
5. Klicken Sie auf die Schaltfläche für den Dateiverzeichnispfad, um auf den Speicherort der Zertifikatsdatei zu zeigen.
6. Klicken Sie auf das grüne Häkchen.
   Die Zertifikatdatei wird hochgeladen.
7. Klicken Sie auf **Add to Certificate List** (Zur Zertifikatsliste hinzufügen).
   Das Zertifikat wird in der Zertifikatliste angezeigt.
8. Klicken Sie auf **Add to ACL**(Zu ACL hinzufügen), und geben Sie eine System-ID und einen Client an.

   Die System-ID muss mit der ID zur Identifikation des BI-Plattform-Systems für SAP BW übereinstimmen.

   Das Zertifikat wird zu der Zugriffskontrollliste hinzugefügt. Der Client sollte als “000” angegeben werden.
9. Speichern Sie Ihre Einstellung und beenden Sie.
   Die Änderungen werden im SAP-System gespeichert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.5.7.4 Konfigurieren der Einzelanmeldung bei der SAP-Datenbank in der CMC

Zum Ausführen der folgenden Schritte müssen Sie mit einem Administratorkonto auf das SAP-Sicherheitsplugin zugreifen.

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
2. Doppelklicken Sie auf die Verknüpfung **SAP** und anschließend auf die Registerkarte **Optionen**.
   Falls kein Zertfikat importiert wurde wird folgende Meldung im Bereich *SAP SSO-Dienst* angezeigt:
   Es wurde keine Schlüsselspeicherdatei hochgeladen
3. Geben Sie die System-ID für Ihr BI-Plattform-System in das entsprechende Feld ein.

   Dieser Wert sollte identisch mit dem beim Import des Zertifikats in das SAP-ABAP-Zielsystem verwendeten Werts sein.
4. Klicken Sie auf die Schaltfläche **Durchsuchen**, um auf die Schlüsselspeicherdatei zu zeigen.
5. Geben Sie die folgenden erforderlichen Informationen ein:

Feld	Erforderliche Information
Kennwort für den Schlüsselspeicher	Geben Sie das für den Zugriff auf die Schlüsselspeicherdatei erforderliche Kennwort ein. Dieses Kennwort wurde beim Erstellen der Schlüsselspeicherdatei angegeben.
Kennwort für den privaten Schlüssel	Geben Sie das für den Zugriff auf das der Schlüsselspeicherdatei entsprechende Zertfikat erforderliche Kennwort ein. Dieses Kennwort wurde beim Erstellen des Zertifikats der Schlüsselspeicherdatei angegeben.
Alias des privaten Schlüssels	Geben Sie den für den Zugriff auf die Schlüsselspeicherdatei erforderlichen Alias ein. Dieser Alias wurde beim Erstellen der Schlüsselspeicherdatei angegeben.

6. Klicken Sie auf **Aktualisieren**, um die Einstellungen zu speichern.
   Nachdem die Einstellungen erfolgreich übertragen wurden, wird folgende Meldung unterhalb des Felds "System-ID" angezeigt:
   Eine Schlüsselspeicherdatei wurde hochgeladen

9.5.7.5 Hinzufügen des Sicherheitstokendiensts zum Adaptive Processing Server

In einer geclusterten Umgebung werden Sicherheitstokendienste separat zu den einzelnen Adaptive Processing Servern hinzugefügt.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf **Kerndienste**.
   Unter *Kerndienste* wird die Serverliste angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Adaptive Processing Server, und wählen Sie **Server stoppen**.

   Setzen Sie den Vorgang erst fort, wenn der Serverstatus "Gestoppt" ist.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Klicken Sie auf den Adaptive Processing Server und wählen **Dienste auswählen**.
   Das Dialogfeld *Dienste auswählen* wird angezeigt.
5. Verschieben Sie den Sicherheitstokendienst mithilfe der Schaltfläche **Hinzufügen** aus der Liste **Verfügbare Dienste** in die Liste **Dienste**.
6. Klicken Sie auf **OK**.
7. Starten Sie den Adaptive Processing Server neu.

9.5.8 Konfigurieren der Einzelanmeldung für SAP Crystal Reports und SAP Netweaver

Die BI-Plattform ist standardmäßig so konfiguriert, dass Benutzer von SAP Crystal Reports mit der Einzelanmeldung auf SAP-Daten zugreifen können.

9.5.8.1 Deaktivieren der Einzelanmeldung für SAP Netweaver und SAP Crystal Reports

1. Klicken Sie in der Central Management Console (CMC) auf **Anwendungen**.
2. Doppelklicken Sie auf **Crystal-Reports-Konfiguration**.
3. Klicken Sie auf **Einzelanmeldungsoptionen**.
4. Wählen Sie einen der folgenden Treiber aus:

Treiber	Anzeigename
ODS-Treiber (Operational Data Store)	**crdb_ods**
Open SQL-Treiber	**crdb_opensql**
InfoSet-Treiber	**crdb_infoset**
BW MDX Query-Treiber	**crdb_bwmdx**

5. Klicken Sie auf **Entfernen**.
6. Klicken Sie auf **Speichern und schließen**.
7. Starten Sie SAP Crystal Reports erneut.

9.5.8.2 Erneutes Aktivieren der Einzelanmeldung für SAP Netweaver und SAP Crystal Reports

Führen Sie die folgenden Schritte aus, um die Einzelanmeldung für SAP Netweaver (ABAP) und SAP Crystal Reports erneut zu aktivieren.

1. Klicken Sie in der Central Management Console (CMC) auf **Anwendungen**.
2. Doppelklicken Sie auf **Crystal-Reports-Konfiguration**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Klicken Sie auf **Einzelanmeldungsoptionen**.
4. Geben Sie unter *SSO-Kontext für Datenbankanmeldung verwenden* Folgendes ein:

`crdb_ods`	Zum Aktivieren des ODS-Treibers
`crdb_opensql`	Zum Aktivieren des Open SQL-Treibers
`crdb_bwmdx`	Zum Aktivieren des SAP BW MDX Query-Treibers
`crdb_infoset`	Zum Aktivieren des InfoSet-Treibers

5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Speichern und schließen**.
7. Starten Sie SAP Crystal Reports erneut.

9.6 PeopleSoft-Authentifizierung

9.6.1 Übersicht

Um die PeopleSoft Enterprise-Daten mit der BI-Plattform zu verwenden, müssen Sie dem Programm Informationen über die Implementierung bereitstellen. Mithilfe dieser Informationen können Benutzer der BI-Plattform authentifiziert werden, damit sie sich mit ihren PeopleSoft-Anmeldedaten beim Programm anmelden können.

9.6.2 Aktivieren der PeopleSoft Enterprise-Authentifizierung

Damit PeopleSoft Enterprise-Informationen von der BI-Plattform verwendet werden können, benötigt die BI-Plattform Informationen zur Authentifizierung im PeopleSoft Enterprise-System.

9.6.2.1 Aktivieren der PeopleSoft-Enterprise-Authentifizierung in der BI-Plattform

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie im Verwaltungsbereich auf **Authentifizierung**.
3. Doppelklicken Sie auf **PeopleSoft Enterprise**.
   Die Seite *PeopleSoft Enterprise* wird angezeigt. Sie verfügt über vier Registerkarten: **Optionen**, **Domänen**, **Rollen** und **Benutzeraktualisierung**.
4. Aktivieren Sie auf der Registerkarte **Optionen** das Kontrollkästchen **PeopleSoft Enterprise-Authentifizierung aktivieren**.
5. Nehmen Sie unter **Neuer Alias**, **Aktualisierungsoptionen** und **Optionen für neue Benutzer** die Änderungen vor, die je nach Ihrer BI-Plattform-Implementierung erforderlich sind.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern, bevor Sie mit der Registerkarte **Domänen** fortfahren.

6. Klicken Sie auf die Registerkarte **Domänen**.
7. Geben Sie im Bereich *PeopleSoft Enterprise-Systembenutzer* einen Datenbank-Benutzernamen und ein Kennwort ein, die die BI-Plattform für die Anmeldung bei der PeopleSoft Enterprise-Datenbank verwenden soll.
8. Geben Sie im Bereich *PeopleSoft-Enterprise-Domänen* den Domänennamen und die QAS-Adresse ein, die zur Verbindungsherstellung mit der PeopleSoft-Enterprise-Umgebung verwendet werden, und klicken Sie auf **Hinzufügen**.

   Hinweis

   Wenn Sie über mehrere PeopleSoft-Domänen verfügen, wiederholen Sie diesen Schritt für jede zusätzliche Domäne, auf die Sie zugreifen möchten. Die Domäne, die Sie als erstes eingeben, wird die Standarddomäne.

9. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

9.6.3 Zuordnen von PeopleSoft-Rollen zur BI-Plattform

Die BI-Plattform erstellt für jede zugeordnete PeopleSoft-Rolle automatisch eine Gruppe. Darüber hinaus erstellt das Programm Aliase, die die Mitglieder der zugeordneten PeopleSoft-Rollen darstellen.

Sie können für jeden erstellten Alias ein Benutzerkonto erstellen.

Wenn Sie jedoch mehrere Systeme ausführen und Ihre Benutzer in mehreren Systemen über Konten verfügen, können Sie jeden Benutzer einem Alias mit demselben Namen zuordnen, bevor Sie die Konten in der BI-Plattform erstellen.

Auf diese Weise reduziert sich die Anzahl der Konten, die für ein und denselben Benutzer in der BI-Plattform erstellt werden müssen.

Wenn Sie beispielsweise PeopleSoft HR 8.3 und PeopleSoft Financials 8.4 ausführen, und 30 Benutzer Zugriff auf beide Systeme haben, müssen für diese Benutzer nur 30 Konten eingerichtet werden. Wenn Sie die Benutzer nicht jeweils einem Alias mit demselben Namen zuweisen, werden für die 30 Benutzer in der BI-Plattform 60 Konten eingerichtet.

Falls Sie jedoch mehrere Systeme ausführen und identische Benutzernamen vorhanden sind, muss für jeden erstellten Alias ein neues Mitgliedskonto erstellt werden.

Wenn Sie beispielsweise PeopleSoft HR 8.3 mit einem Benutzerkonto für Ronald Schneider (Benutzername "rschneider") und PeopleSoft Financials 8.4 mit einem Benutzerkonto für Regina Schneider (Benutzername "rschneider") ausführen, müssen Sie ein separates Konto für den Alias des jeweiligen Benutzers erstellen. Andernfalls werden die beiden Benutzer demselben BI-Plattform-Konto hinzugefügt, können sich mit ihren eigenen PeopleSoft-Anmeldedaten bei der BI-Plattform anmelden und haben Zugriff auf Daten aus beiden PeopleSoft-Systemen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.6.3.1 Zuordnen von PeopleSoft-Rollen zur BI-Plattform

Falls die BI-Plattform-JVM (Java Virtual Machine) kein Zertfikat für den PeopleSoft-Server hat, führen Sie vor dem Durchführen der Hauptschritte unten die folgenden zusätzlichen Schritte aus:

1. Rufen Sie die .cer-Datei vom PeopleSoft-Server ab.
2. Kopieren Sie die .cer-Datei nach `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.
3. Führen Sie den folgenden Befehl vom Sicherheitsverzeichnis aus: `"<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool.exe" -import -file <PeopleSoftServer>.cer -keystore cacerts -alias <PeopleSoftServer>`.
4. Starten Sie den Webanwendungsserver neu.

Die wichtigsten Schritte:

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie auf **Authentifizierung**.
3. Doppelklicken Sie auf **PeopleSoft Enterprise**.
4. Wählen Sie im Bereich "PeopleSoft Enterprise-Domänen" auf der Registerkarte **Rollen** die Domäne aus, die mit der Rolle verknüpft ist, die Sie der BI-Plattform zuordnen möchten.
5. Wählen Sie mithilfe einer der folgenden Optionen die Rollen aus, die Sie zuordnen möchten:
   - Geben Sie im Bereich *PeopleSoft Enterprise-Rollen* im Feld "Suchen" die Rolle ein, die Sie suchen und der BI-Plattform zuordnen möchten, und klicken Sie dann auf **>**.
   - Wählen Sie aus der Liste *Verfügbare Rollen* die Rolle aus, die Sie der BI-Plattform zuordnen möchten, und klicken Sie auf **>**.

   > **Hinweis**
   >
   > Bei der Suche nach einem bestimmten Benutzer oder einer bestimmten Rolle können Sie das Platzhalterzeichen % verwenden. Um beispielsweise alle Rollen zu suchen, die mit "A" beginnen, geben Sie **A%** ein. Außerdem wird die Groß-/Kleinschreibung bei der Suche berücksichtigt.

   > **Hinweis**
   >
   > Wenn Sie eine Rolle von einer anderen Domäne zuordnen möchten, wählen Sie die neue Domäne aus der Liste verfügbarer Domänen aus, um eine Rolle von einer anderen Domäne zuzuordnen.
6. Öffnen Sie die Registerkarte **Benutzeraktualisierung**, und klicken Sie entweder auf die Schaltfläche **Aktualisieren**, oder planen Sie die zeitgesteuerte Verarbeitung der Aktualisierungen.
7. Wechseln Sie auf der Registerkarte **Optionen** in den Bereich *Optionen für neue Benutzer* eine der folgenden Optionen aus:
   - **Jeden hinzugefügten Alias einem Konto mit demselben Namen zuweisen**

     Aktivieren Sie diese Option bei Verwendung mehrerer PeopleSoft Enterprise-Systeme mit Benutzern, die über Konten auf mehr als einem System verfügen (dabei dürfen zwei Benutzer jedoch nicht denselben Benutzernamen auf unterschiedlichen Systemen besitzen).
   - **Neues Konto für jeden hinzugefügten Alias erstellen**

     Aktivieren Sie diese Option, wenn Sie nur ein PeopleSoft Enterprise-System ausführen, die Mehrheit Ihrer Benutzer nur über ein Konto auf einem der Systeme verfügt, oder falls für unterschiedliche Benutzer auf mindestens zwei Systemen identische Benutzernamen vorhanden sind.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8. Wählen Sie im Bereich *Aktualisierungsoptionen für Aliase* eine der folgenden Optionen aus:
   - **Neue Aliase bei der Aliasaktualisierung erstellen**

     Wählen Sie diese Option, um einen neuen Alias für jeden Benutzer zu erstellen, den Sie der BI-Plattform zuordnen. Bei Benutzern ohne BI-Plattform-Konto oder bei Aktivierung der Option "Neues Konto für jeden hinzugefügten Alias erstellen" werden neue Konten für die Benutzer hinzugefügt.
   - **Neue Aliase nur bei der Benutzeranmeldung erstellen**

     Aktivieren Sie diese Option, wenn die zuzuordnende Rolle viele Benutzer umfasst, die BI-Plattform jedoch nur von einigen wenigen Benutzern genutzt wird. Aliase und Konten für die Benutzer werden von der Plattform nicht automatisch erstellt. Vielmehr werden Aliase (und gegebenenfalls Konten) für die Benutzer erst dann erstellt, wenn sie sich zum ersten Mal bei der BI-Plattform anmelden. Dies ist die Standardoption.
9. Geben Sie unter *Optionen für neue Benutzer* an, wie neue Benutzer erstellt werden.

   Wählen Sie eine der folgenden Optionen:
   - **Neue Benutzer werden als Namenslizenzbenutzer erstellt**

     Neue Benutzerkonten werden für die Verwendung von Namenslizenzen konfiguriert. Namenslizenzen sind mit bestimmten Benutzern verbunden und ermöglichen den Zugriff auf das System auf der Grundlage von Benutzername und Kennwort. Dieser Lizenztyp ermöglicht Benutzern den Zugriff auf das System unabhängig von der Anzahl der derzeit verbundenen Benutzer. Für jedes mit dieser Option erstellte Benutzerkonto muss eine Namenslizenz verfügbar sein.
   - **Neue Benutzer werden als Zugriffslizenzbenutzer erstellt**

     Neue Benutzerkonten werden für die Verwendung von Zugriffslizenzen konfiguriert. Zugriffslizenzen geben die Anzahl der Personen an, die gleichzeitig mit der BI-Plattform verbunden sein können. Dieser Lizenztyp ist sehr flexibel, da mit einer geringen Anzahl von Zugriffslizenzen viele Benutzer unterstützt werden können. Je nach Häufigkeit und Dauer des Zugriffs auf die BI-Plattform können 100 Zugriffslizenzen beispielsweise 250, 500 oder auch 700 Benutzer unterstützen.

   Die ausgewählten Rollen werden jetzt als Gruppen in der BI-Plattform angezeigt.

9.6.3.2 Hinweise zum erneuten Zuordnen

Wenn Sie Benutzer einer Rolle hinzufügen, die der BI-Plattform bereits zugeordnet wurde, müssen Sie die Rolle erneut zuordnen, damit die Benutzer zur BI-Plattform hinzugefügt werden. Beim erneuten Zuordnen der Rolle hat die Option zum Zuordnen der Benutzer als Namenslizenz- oder Zugriffslizenzbenutzer nur Einfluss auf die neuen, der Rolle hinzugefügten Benutzer.

Beispiel: Zuerst ordnen Sie der BI-Plattform eine Rolle mit aktivierter Option "Neue Benutzer werden als *Namenslizenzbenutzer* erstellt" zu. Später fügen Sie derselben Rolle Benutzer hinzu und ordnen die Rolle dann erneut zu, während die Option "Neue Benutzer werden als *Zugriffslizenzbenutzer* erstellt" aktiviert ist.

In diesem Fall werden nur die neuen Benutzer in der Rolle der BI-Plattform als Zugriffslizenzbenutzer zugeordnet. Benutzer, die bereits zugeordnet waren, bleiben Namenslizenzbenutzer. Dasselbe gilt, wenn Sie Benutzer erst als Zugriffslizenzbenutzer zuordnen und später die Einstellungen ändern, um neue Benutzer als Namenslizenzbenutzer neu zuzuordnen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.6.3.3 Aufheben der Zuordnung einer Rolle

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie auf **Authentifizierung**.
3. Klicken Sie auf **PeopleSoft Enterprise**.
4. Klicken Sie auf **Rollen**.
5. Wählen Sie die Rolle aus, die Sie entfernen möchten, und klicken Sie auf **<**.
6. Klicken Sie auf **Aktualisieren**.

   Mitglieder der Rolle sind nicht mehr in der Lage, auf die BI-Plattform zuzugreifen, es sei denn, sie verfügen noch über andere Konten oder Aliase.

   > **Hinweis**
   >
   > Sie können auch einzelne Konten löschen oder Benutzer aus Rollen entfernen, bevor Sie die Rollen der BI-Plattform zuordnen, um zu verhindern, dass sich bestimmte Benutzer anmelden können.

9.6.4 Zeitgesteuertes Verarbeiten von Benutzeraktualisierungen

Um sicherzustellen, dass Änderungen Ihrer Benutzerdaten für das ERP-System in Ihren BI-Plattform-Benutzerdaten widergespiegelt werden, können Sie regelmäßige Benutzeraktualisierungen planen. Diese Aktualisierungen synchronisieren automatisch die ERP- und BI-Plattform-Benutzer in Übereinstimmung mit den Zuordnungseinstellungen, die Sie in der Central Management Console (CMC) konfiguriert haben.

Für die Ausführung und zeitgesteuerte Verarbeitung von Aktualisierungen für importierte Rollen stehen zwei Optionen zur Verfügung:

- Nur Rollen aktualisieren: Bei Verwendung dieser Option werden nur die Verknüpfungen zwischen den aktuell zugeordneten Rollen aktualisiert, die in die BI-Plattform importiert wurden. Verwenden Sie diese Option, wenn Sie voraussichtlich häufig Aktualisierungen ausführen müssen und Bedenken hinsichtlich der Systemressourcennutzung haben. Wenn Sie nur Rollen aktualisieren, werden keine neuen Benutzerkonten erstellt.
- Rollen und Aliase aktualisieren: Bei Verwendung dieser Option werden nicht nur Verknüpfungen zwischen Rollen aktualisiert, sondern auch neue Benutzerkonten in der BI-Plattform für neue Benutzeraliase erstellt, die zum ERP-System hinzugefügt wurden.

> **Hinweis**
>
> Wenn Sie bei der Aktivierung der Authentifizierung nicht angegeben haben, dass Benutzeraliase automatisch für Aktualisierungen erstellt werden sollen, werden keine Konten für neue Aliase erstellt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.6.4.1 Zeitgesteuertes Verarbeiten von Benutzeraktualisierungen

Nachdem Sie Rollen in der BI-Plattform zugeordnet haben, müssen Sie angeben, wie das System diese Rollen aktualisiert.

1. Klicken Sie auf die Registerkarte **Benutzeraktualisierung**.
2. Klicken Sie im Abschnitt *Nur Rollen aktualisieren* oder *Rollen und Aliase aktualisieren* auf **Zeitgesteuert verarbeiten**.

   ➔ Tipp

   Wenn Sie die Aktualisierung sofort ausführen möchten, klicken Sie auf **Jetzt aktualisieren**.

   ➔ Tipp

   Verwenden Sie die Option *Nur Rollen aktualisieren*, wenn Sie häufig aktualisieren möchten und Bedenken bezüglich der Systemressourcen haben. Das System benötigt mehr Zeit, um sowohl Rollen als auch Aliase zu aktualisieren.

   Das Dialogfeld *Wiederholung* wird angezeigt.
3. Wählen Sie in der Liste *Objekt ausführen* eine Option aus, und geben Sie alle angeforderten Informationen zur zeitgesteuerten Verarbeitung ein.

   Bei der zeitgesteuerten Verarbeitung einer Aktualisierung stehen Ihnen die Wiederholungsmuster in der folgenden Tabelle zur Verfügung:

Wiederholungsmuster	Beschreibung
Stündlich	Die Aktualisierung wird stündlich ausgeführt. Sie legen die Startzeit sowie Anfangs- und Enddatum für das Objekt fest.
Täglich	Die Aktualisierung wird täglich oder alle n angegebenen Tage ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum für das Objekt festlegen.
Wöchentlich	Die Aktualisierung wird wöchentlich ausgeführt. Es kann einmal die Woche oder mehrmals wöchentlich ausgeführt werden. Sie können festlegen, an welchen Tagen und zu welcher Uhrzeit das Objekt ausgeführt wird, und das Anfangs- und Enddatum der Ausführung bestimmen.
Monatlich	Die Aktualisierung wird einmal monatlich oder alle n Monate ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am n-ten Tag des Monats	Die Aktualisierung wird an einem bestimmten Tag des Monats ausgeführt. Sie können festlegen, an welchem Tag des Monats und zu welcher Uhrzeit die Aktualisierung ausgeführt wird, sowie Anfangs- und Enddatum der Ausführung bestimmen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wiederholungsmuster	Beschreibung
Am ersten Montag des Monats	Die Aktualisierung wird jeden Monat am ersten Montag ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am letzten Tag des Monats	Die Aktualisierung wird am letzten Tag jedes Monats ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am x-ten Tag der n-ten Woche des Monats	Die Aktualisierung wird an einem bestimmten Tag einer bestimmten Woche im Monat ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Kalender	Die Aktualisierung wird zu den Terminen ausgeführt, die in einem zuvor erstellten Kalender festgelegt wurden.

4. Klicken Sie auf **Zeitgesteuert verarbeiten**, nachdem Sie die Informationen für die zeitgesteuerte Verarbeitung angegeben haben.
   In der Registerkarte **Benutzeraktualisierung** wird das Datum der nächsten zeitgesteuert verarbeiteten Rollenaktualisierung angezeigt.

> **Hinweis**
>
> Sie können die nächste zeitgesteuert verarbeitete Aktualisierung jederzeit abbrechen, indem Sie im Abschnitt *Nur Rollen aktivieren* oder *Rollen und Aliase aktivieren* auf **Geplante Aktualisierungen abbrechen** klicken.

9.6.5 Verwenden der PeopleSoft-Sicherheitsbrücke

Mit der Funktion "Sicherheitsbrücke" der BI-Plattform können Sie die Sicherheitseinstellungen von PeopleSoft EPM-in die BI-Plattform importieren.

Die Sicherheitsbrücke hat zwei verschiedene Modi:

- **Konfigurationsmodus**

  Im Konfigurationsmodus ist die Sicherheitsbrücke eine Art Schnittstelle, mit der Sie eine Antwortdatei erstellen können. Diese Antwortdatei steuert das Verhalten der Sicherheitsbrücke während des Ausführungsmodus.
- **Ausführungsmodus**

  Auf Basis der von Ihnen in der Antwortdatei festgelegten Parameter importiert die Sicherheitsbrücke die Sicherheitseinstellungen der Dimensionstabellen in PeopleSoft EPM in die Universen in der BI-Plattform.

9.6.5.1 Importieren von Sicherheitseinstellungen

Führen Sie zum Importieren der Sicherheitseinstellungen folgende Aufgaben der Reihe nach aus:

- Definieren Sie die Objekte, die von der Sicherheitsbrücke verwaltet werden sollen.
- Erstellen Sie eine Antwortdatei.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Führen Sie das Sicherheitsbrückenprogramm aus.

Weitere Informationen über die Sicherheitsverwaltung nach dem Importieren der Einstellungen finden Sie unter *Verwalten von Sicherheitseinstellungen* [Seite 339].

9.6.5.1.1 Definieren verwalteter Objekte

Vor Ausführung der Sicherheitsbrücke ist es wichtig, dass die Objekte festgelegt werden, die von der Anwendung verwaltet werden sollen. Die Sicherheitsbrücke kann eine oder mehrere PeopleSoft-Rollen, eine BI-Plattform-Gruppe und ein oder mehrere Universen verwalten.

- Verwaltete PeopleSoft-Rollen

  Dies sind die Rollen in Ihrem PeopleSoft-System. Die Mitglieder dieser Rollen verarbeiten PeopleSoft-Daten über PeopleSoft EPM. Wählen Sie die Rollen mit den Mitgliedern aus, für die Sie die Zugriffsberechtigungen zu in der BI-Plattform verwalteten Universen einrichten oder aktualisieren möchten.
  Die für die Mitglieder dieser Rollen definierten Zugriffsberechtigungen basieren auf den eingestellten Berechtigungen in PeopleSoft EPM. Die Sicherheitsbrücke importiert diese Sicherheitseinstellungen in die BI-Plattform.
- Verwaltete BI-Plattform-Gruppe

  Beim Ausführen der Sicherheitsbrücke erstellt das Programm in der BI-Plattform für jedes Mitglied einer verwalteten PeopleSoft-Rolle einen Benutzer.
  Die Gruppe, in der die Benutzer erstellt werden, ist die verwaltete BI-Plattform-Gruppe. Mitglieder dieser Gruppe sind die Benutzer, deren Zugriffsberechtigungen für die verwalteten Universen von der Sicherheitsbrücke verwaltet werden. Da die Benutzer in einer Gruppe erstellt werden, können Sie die Sicherheitsbrücke so konfigurieren, dass die Sicherheitseinstellungen für bestimmte Benutzer einfach durch das Entfernen von Benutzern aus der verwalteten BI-Plattform-Gruppe nicht aktualisiert werden.
  Wählen Sie vor Ausführung der Sicherheitsbrücke eine Gruppe in der BI-Plattform als Speicherort zum Erstellen der Benutzer aus. Wenn Sie eine nicht vorhandene Gruppe angeben, erstellt die Sicherheitsbrücke diese Gruppe in der BI-Plattform.
- Verwaltete Universen

  Verwaltete Universen sind jene Universen, in die die Sicherheitsbrücke die Sicherheitseinstellungen aus PeopleSoft EPM importiert. Wählen Sie aus den in Ihrem BI-Plattform-System gespeicherten Universen die Universen aus, die von der Sicherheitsbrücke verwaltet werden sollen. Mitglieder der verwalteten PeopleSoft-Rollen, die auch Mitglieder der verwalteten BI-Plattform-Gruppe sind, können durch diese Universen nicht auf Daten zugreifen, auf die sie auch in PeopleSoft EPM keinen Zugriff haben.

9.6.5.1.2 Erstellen von Antwortdateien

1. Wechseln Sie zu dem Ordner, den Sie bei der Installation der Sicherheitsbrücke angegeben haben, und führen Sie die Datei `crpsepmsecuritybridge.bat` (unter Windows) und `crpsepmsecuritybridge.sh` (unter Unix) aus.

   Hinweis

   Unter Windows befindet sich der Ordner standardmäßig unter `C:\Programme\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\epm`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Das Dialogfeld "Sicherheitsbrücke für PeopleSoft EPM" wird angezeigt.

2. Wählen Sie **Neu** aus, um eine Antwortdatei zu erstellen, oder wählen Sie **Öffnen** aus, und klicken Sie auf **Durchsuchen**, um nach der zu ändernden Antwortdatei zu suchen. Wählen Sie die gewünschte Sprache für die Datei aus.
3. Klicken Sie auf **Weiter**.
4. Geben Sie die Verzeichnisse des **PeopleSoft EPM SDK** und des **BI-Plattform-SDK** an.

> **Hinweis**
>
> Normalerweise befindet sich das PeopleSoft EPM SDK auf dem PeopleSoft-Server unter `<PS_HOME>/class/com.peoplesoft.epm.pf.jar`.

> **Hinweis**
>
> Das BI-Plattform-SDK ist normalerweise unter `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib` zu finden.

5. Klicken Sie auf **Weiter**.

   Das Dialogfeld fordert Sie zur Eingabe von Verbindungs- und Treiberinformationen für die PeopleSoft-Datenbank auf.
6. Wählen Sie aus der Datenbankliste den entsprechenden Datenbanktyp aus, und geben Sie die Informationen in die entsprechenden Felder ein.

Feld	Beschreibung
Datenbank	Name der PeopleSoft-Datenbank
Host	Name des Servers, der Host der Datenbank ist
Portnummer	Portnummer für Zugriff zum Server
Klassenspeicherort	Speicherort der Klassendateien für den Datenbank-treiber
Benutzername	Ihr Benutzername
Kennwort	Ihr Kennwort

7. Klicken Sie auf **Weiter**.

   Im Dialogfeld wird eine Liste mit allen Klassen angezeigt, die von der Sicherheitsbrücke bei der Ausführung verwendet werden. Sie können der Liste Klassen hinzufügen oder Klassen aus der Liste entfernen, falls erforderlich.
8. Klicken Sie auf **Weiter**.

   Das Dialogfeld fordert Sie zur Eingabe von Verbindungsinformationen für die BI-Plattform auf.
9. Geben Sie die entsprechenden Informationen für folgende Felder ein:

Feld	Beschreibung
Server	Der Name des Servers, auf dem sich der Central Management Server (CMS) befindet.
Benutzername	Ihr Benutzername

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Feld	Beschreibung
Kennwort	Ihr Kennwort
Authentifizierung	Ihr Authentifizierungstyp

10. Klicken Sie auf **Weiter**.
11. Wählen Sie eine BI-Plattform-Gruppe aus, und klicken Sie auf **Weiter**.

> **Hinweis**
>
> In der in diesem Feld angegebenen Gruppe werden die Mitglieder der verwalteten PeopleSoft-Rollen erstellt.

> **Hinweis**
>
> Wenn Sie eine noch nicht vorhandene Gruppe angeben, erstellt die Sicherheitsbrücke diese Gruppe.

Im Dialogfeld wird eine Liste mit den Rollen Ihres PeopleSoft-Systems angezeigt.

12. Wählen Sie die Option **Importiert** für die von der Sicherheitsbrücke zu verwaltenden Rollen aus, und klicken Sie auf **Weiter**.

> **Hinweis**
>
> Die Sicherheitsbrücke erstellt einen Benutzer in der verwalteten (und von Ihnen im vorherigen Schritt festgelegten) BI-Plattform-Gruppe für jedes Mitglied der ausgewählten Rolle(n).

Im Dialogfeld wird eine Liste mit den Universen in der BI-Plattform angezeigt.

13. Wählen Sie die Universen aus, in die die Sicherheitsbrücke die Sicherheitseinstellungen importieren soll, und klicken Sie auf **Weiter**.
14. Geben Sie einen Dateinamen und einen Speicherort für die Protokolldatei der Sicherheitsbrücke an. Aus der Protokolldatei ist ersichtlich, ob die Sicherheitsbrücke die Sicherheitseinstellungen von PeopleSoft EPM erfolgreich importiert hat.
15. Klicken Sie auf **Weiter**.

    Im Dialogfeld wird eine Vorschau der Antwortdatei angezeigt, die die Sicherheitsbrücke im Ausführungsmodus verwenden wird.
16. Klicken Sie auf **Speichern**, und wählen Sie einen Speicherort für die Antwortdatei aus.
17. Klicken Sie auf **Weiter**.

    Sie haben die Antwortdatei für die Sicherheitsbrücke erfolgreich erstellt.
18. Klicken Sie auf **Beenden**.

> **Hinweis**
>
> Die Antwortdatei ist eine Java-Eigenschaftsdatei, die Sie auch manuell ändern bzw. erstellen können. Weitere Informationen finden Sie im Abschnitt “PeopleSoft-Antwortdatei”.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.6.5.2 Anwenden der Sicherheitseinstellungen

Führen Sie zum Anwenden der Sicherheitseinstellungen die Batch-Datei `crpsepmsecuritybridge.bat` (unter Windows) oder `crpsempsecuritybridge.sh` (unter Unix) aus, und verwenden Sie die von Ihnen erstellte Antwortdatei als Argument. Sie können z.B. **`crpsepmsecuritybridge.bat myresponsefile.properties`** unter Windows oder **`crpsempsecuritybridge.sh myresponsefile.properties`** unter Unix eingeben.

Das Sicherheitsbrückenprogramm wird ausgeführt. Es erstellt Benutzer in der BI-Plattform für die Mitglieder der PeopleSoft-Rollen, die Sie in der Antwortdatei angegeben haben, und importiert die Sicherheitseinstellungen von PeopleSoft EPM in die entsprechenden Universen.

9.6.5.2.1 Hinweise für die Zuordnung

Im Ausführungsmodus erstellt die Sicherheitsbrücke in der BI-Plattform für jedes Mitglied einer verwalteten PeopleSoft-Rolle einen Benutzer.

Die Benutzer werden so erstellt, dass sie nur Enterprise-Authentifizierungsaliase haben, und die BI-Plattform ordnet diesen Benutzern Zufallskennwörter zu. Die Benutzer können sich daher erst bei der BI-Plattform anmelden, wenn der Administrator manuell neue Kennwörter zuweist oder die Rollen der BI-Plattform über das PeopleSoft-Sicherheits-Plugin zuordnet. Erst dann können sich die Benutzer mit ihren PeopleSoft-Anmeldedaten anmelden.

9.6.5.3 Verwalten von Sicherheitseinstellungen

Sie können die von Ihnen zugewiesenen Sicherheitseinstellungen durch Ändern der Objekte verwalten, die von der Sicherheitsbrücke verwaltet werden.

9.6.5.3.1 Verwaltete Benutzer

Die Sicherheitsbrücke verwaltet Benutzer auf der Grundlage folgender Kriterien:

- Ist der Benutzer ein Mitglied einer verwalteten PeopleSoft-Rolle?
- Ist der Benutzer ein Mitglied der verwalteten BI-Plattform-Gruppe?

Wenn Sie für einen Benutzer Zugriff auf PeopleSoft-Daten durch Universen in der BI-Plattform festlegen möchten, müssen Sie sicherstellen, dass der Benutzer ein Mitglied sowohl einer verwalteten PeopleSoft-Rolle *als auch* der verwalteten BI-Plattform-Gruppe ist.

- Für Mitglieder verwalteter PeopleSoft-Rollen ohne Konten in der BI-Plattform erstellt die Sicherheitsbrücke Konten und weist ihnen Zufallskennwörter zu. Der Administrator muss entscheiden, ob neue Kennwörter manuell zugewiesen werden oder ob die Rollen der BI-Plattform durch das PeopleSoft-Sicherheits-Plugin zugeordnet werden, damit sich die Benutzer bei der BI-Plattform anmelden können.
- Bei Mitgliedern verwalteter PeopleSoft-Rollen, die auch Mitglieder der verwalteten BI-Plattform-Gruppe sind, aktualisiert die Sicherheitsbrücke die den Benutzern zugewiesenen Sicherheitseinstellungen, damit sie auf die entsprechenden Daten von den verwalteten Universen zugreifen können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wenn ein Mitglied einer verwalteten PeopleSoft-Rolle über ein Konto in der BI-Plattform verfügt, aber *kein* Mitglied der verwalteten BI-Plattform-Gruppe ist, aktualisiert die Sicherheitsbrücke die dem Benutzer zugewiesenen Sicherheitseinstellungen *nicht*. Normalerweise kommt es nur dann zu dieser Situation, wenn der Administrator Benutzerkonten entfernt, die durch die Sicherheitsbrücke von der verwalteten BI-Plattform-Gruppe erstellt wurden.

> **Hinweis**
>
> Dies ist eine effektive Methode zur Sicherheitsverwaltung: Durch das Entfernen von Benutzern aus der verwalteten BI-Plattform-Gruppe können Sie ihre Sicherheitseinstellungen so konfigurieren, dass sie sich von den Sicherheitseinstellungen für die Benutzer in PeopleSoft unterscheiden.

Wenn andererseits ein Mitglied der verwalteten BI-Plattform-Gruppe *kein* Mitglied einer verwalteten PeopleSoft-Rolle ist, gewährt ihm die Sicherheitsbrücke *keinen* Zugriff auf die verwalteten Universen. Normalerweise kommt es nur dann zu dieser Situation, wenn PeopleSoft-Administratoren Benutzer entfernen, die zuvor durch die Sicherheitsbrücke von den verwalteten PeopleSoft-Rollen der BI-Plattform zugeordnet wurden.

> **Hinweis**
>
> Hierbei handelt es sich um eine weitere Methode zur Sicherheitsverwaltung: Durch das Entfernen von Benutzern aus verwalteten PeopleSoft-Rollen können Sie sicherstellen, dass die Benutzer keinen Zugriff auf Daten von PeopleSoft haben.

9.6.5.3.2 Verwaltete Universen

Die Sicherheitsbrücke verwaltet Universen durch Einschränkungsmengen, welche die Daten einschränken, auf die verwaltete Benutzer von den verwalteten Universen zugreifen können.

Einschränkungsmengen sind Gruppen von Einschränkungen (z.B. Einschränkungen zu Abfragesteuerung, SQL-Erstellung usw.). Die Sicherheitsbrücke wendet die Zeilenzugriffs- und Objektzugriffseinschränkungen für die verwalteten Universen an oder aktualisiert diese.

- Sie weist Dimensionstabellen Zeilenzugriffseinschränkungen zu, die in PeopleSoft EPM definiert sind. Diese Einschränkungen sind benutzerspezifisch und können für eine der folgenden Einstellungen konfiguriert werden:
  - Der Benutzer hat Zugriff auf alle Daten.
  - Der Benutzer hat Zugriff auf keine Daten.
  - Der Benutzer hat Zugriff auf Daten auf Grundlage ihrer Zeilenebenenberechtigungen in PeopleSoft, die durch die in PeopleSoft EPM definierten Security Join Tables (SJT) angezeigt werden.
- Sie weist Objektzugriffseinschränkungen zu, um Objekte auf Grundlage der Felder zu messen, auf die von den Kennzahlen zugegriffen wird.

  Wenn eine Kennzahl auf Felder zugreift, die in PeopleSoft als metrisch definiert sind, wird der Zugriff auf die Kennzahl erlaubt oder nicht erlaubt, je nachdem, ob der Benutzer in PeopleSoft auf die referenzierten Metriken zugreifen kann. Wenn ein Benutzer auf keine der Metriken zugreifen kann, wird der Zugriff auf die Kennzahl nicht zugelassen. Wenn ein Benutzer auf alle Metriken zugreifen kann, wird der Zugriff auf die Kennzahl zugelassen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Als Administrator können Sie auch die Daten beschränken, auf die Benutzer aus Ihrem PeopleSoft-System zugreifen können, indem Sie die Anzahl der Universen begrenzen, die durch die Sicherheitsbrücke verwaltet werden.

9.6.5.4 PeopleSoft-Antwortdatei

Die Funktion "Sicherheitsbrücke" der BI-Plattform wird auf der Grundlage der Einstellungen ausgeführt, die Sie in einer Antwortdatei festlegen.

Normalerweise erzeugen Sie die Antwortdatei durch Verwendung der Schnittstelle, die im Konfigurationsmodus der Sicherheitsbrücke verfügbar ist. Da die Datei eine Java-Eigenschaftsdatei ist, können Sie sie auch manuell ändern oder erstellen.

Dieser Anhang enthält Informationen über die Parameter, die Sie in der Antwortdatei angeben müssen, wenn Sie sich für eine manuelle Erstellung entscheiden.

> **Hinweis**
>
> Bei der Dateierstellung müssen Sie die Codewechselumschaltanforderungen für Java-Eigenschaftsdateien beachten (das Umschaltzeichen für ":" ist z.B. "\:").

9.6.5.4.1 Antwortdateiparameter

In der folgenden Tabelle sind die in der Antwortdatei enthaltenen Parameter beschrieben:

Parameter	Beschreibung
classpath	Klassenpfad zum Laden der erforderlichen .jar-Dateien. Sowohl bei Windows als auch bei UNIX müssen mehrere Klassenpfade durch ";" getrennt werden. Die benötigten Klassenpfade sind für die Datei `com.peoplesoft.epm.pf.jar` und für die .jar-Datei des JDBC-Treibers.
db.driver.name	JDBC-Treibername, der zur Verbindung mit der PeopleSoft-Datenbank verwendet wird (z.B. `com.microsoft.jdbc.sqlserver.SQLServerDriver`).
db.connect.str	JDBC-Verbindungszeichenfolge, die zur Verbindung mit der PeopleSoft-Datenbank verwendet wird (z.B. `jdbc:microsoft:sqlserver:// vanrdpsft01:1433;DatabaseName=PRDMO`)
db.user.name	Benutzername für die Anmeldung bei der PeopleSoft-Datenbank

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Beschreibung
db.password	Kennwort für die Anmeldung in der PeopleSoft-Datenbank
db.password.encrypted	Mit dem Wert dieses Parameters wird festgelegt, ob der Kennwortparameter in der Antwortdatei verschlüsselt ist oder nicht. Der Wert kann auf "True" oder "False" (Wahr oder Falsch) eingestellt werden. (Wenn kein Wert angegeben ist, lautet der Wert standardmäßig "False".)
enterprise.cms.name	CMS, auf dem sich die Universen befinden
enterprise.user.name	Benutzername für die Anmeldung beim CMS
enterprise.password	Kennwort für die Anmeldung am CMS
enterprise.password.encrypted	Mit dem Wert dieses Parameters wird festgelegt, ob der Kennwortparameter in der Antwortdatei verschlüsselt ist oder nicht. Der Wert kann auf "True" oder "False" (Wahr oder Falsch) eingestellt werden. (Wenn kein Wert angegeben ist, lautet der Wert standardmäßig "False".)
enterprise.authMethod	Authentifizierungsmethode für die Anmeldung am CMS
enterprise.role	Verwaltete BI-Plattform-Gruppe. Weitere Informationen finden Sie unter *Definieren verwalteter Objekte* [Seite 336].
enterprise.license	Bestimmt beim Importieren von Benutzern aus PeopleSoft den Lizenztyp. Mit "0" wird die Namenslizenz , mit "1" die Zugriffslizenz festgelegt.
peoplesoft.role.n	Liste der verwalteten PeopleSoft-Rollen. Weitere Informationen finden Sie unter *Definieren verwalteter Objekte* [Seite 336]. `<n>` ist eine ganze Zahl, und jeder Eintrag besetzt eine Eigenschaft des peoplesoft.role-Präfixes. **Hinweis** `<n>` basiert auf 1. Sie können "*" zur Bezeichnung aller verfügbaren PeopleSoft-Rollen verwenden, vorausgesetzt, dass n 1 ist, und es die einzige Eigenschaft ist, die peoplesoft.role als Präfix in der Antwortdatei hat.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Beschreibung
mapped.universe.n	Liste der Universen, die von der Sicherheitsbrücke aktualisiert werden sollen. Weitere Informationen finden Sie unter *Definieren verwalteter Objekte* [Seite 336]. `<n>` ist eine ganze Zahl, und jeder Eintrag besetzt eine Eigenschaft des mapped.universe-Präfixes. **Hinweis** `<n>` basiert auf 1. Sie können "*" zur Bezeichnung aller verfügbaren Universen verwenden, vorausgesetzt, dass n 1 ist, und es die einzige Eigenschaft ist, die mapped.universe als Präfix in der Antwortdatei hat.
log4j.appender.file.File	Von der Sicherheitsbrücke geschriebene Protokolldatei
log4j.*	Standardeigenschaften von log4j, die log4j für richtiges Funktionieren benötigt: log4j.rootLogger=INFO, file, stdout log4j.appender.file=org.apache.log4j.RollingFile Appender log4j.appender.file.layout=org.apache.log4j.PatternLayout log4j.appender.file.MaxFileSize=5000KB log4j.appender.file.MaxBackupIndex=100 log4j.appender.file.layout.ConversionPattern=%d [%-5] %c{1} - %m%n log4j.appender.stdout=org.apache.log4j.ConsoleAppender log4j.appender.stdout.layout=org.apache.log4j.PatternLayout log4j.appender.stdout.layout.ConversionPattern=%d [%-5] %c{1} - %m%n
peoplesoft classpath	Klassenpfad zu den .jar-Dateien von PeopleSoft EPM API Dieser Parameter ist optional.
enterprise.classpath	Klassenpfad zu den JAR-Dateien des BI-Plattform-SDK. Dieser Parameter ist optional.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Beschreibung
db.driver.type	PeopleSoft-Datenbanktyp. Diese Parameter können einen der folgenden Werte haben: Microsoft SQL Server 2000 Oracle Database 10.1 DB2 UDB 8.2 Fixpack 7 Benutzerdefiniert "Benutzerdefiniert" kann zum Angeben von Datenbanken mit anderen Formaten oder Versionen als den erkannten verwendet werden. Dieser Parameter ist optional.
sql.db.class.location sql.db.host sql.db.port sql.db.database	Der Speicherort der .jar-Dateien des SQL Server-JDB-Treibers, der SQL Server-Hostrechner, der SQL Server-Port und der SQL Server-Datenbankname. Diese Parameter können nur verwendet werden, wenn der db.driver.type Microsoft SQL Server 2000 ist. Diese Parameter sind optional.
oracle.db.class.location oracle.db.host oracle.db.port oracle.db.sid	Der Speicherort der .jar-Dateien des Oracle-JDBC-Treibers, der Oracle-Datenbank-Hostrechner, der Oracle-Datenbankanschluss und die Oracle-Datenbank-SID. Diese Parameter können nur verwendet werden, wenn der db.driver.type Oracle Database 10.1 ist. Diese Parameter sind optional.
db2.db.class.location db2.db.host db2.db.port db2.db.sid	Der Speicherort der .jar-Dateien des DB2-JDBC-Treibers, der DB2-Datenbank-Hostrechner, der DB2-Datenbankanschluss und die DB2-Datenbank-SID. Diese Parameter können nur verwendet werden, wenn der db.driver.type DB2 UDB 8.2 Fixpack 7 ist. Diese Parameter sind optional.
custom.db.class.location custom.db.drivername custom.db.connectStr	Speicherort, Name und Verbindungsstring des benutzerdefinierten JDBC-Treibers Diese Parameter können nur verwendet werden, wenn der db.driver.type "Benutzerdefiniert" ist. Diese Parameter sind optional.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.7 JD Edwards-Authentifizierung

9.7.1 Übersicht

Um JD Edwards-Daten mit der BI-Plattform zu verwenden, müssen Sie dem System Informationen über die JD Edwards-Implementierung bereitstellen. Mithilfe dieser Informationen kann die BI-Plattform Benutzer authentifizieren, damit diese sich mit ihren JD Edwards EnterpriseOne-Anmeldedaten bei der BI-Plattform anmelden können.

9.7.2 Aktivieren der JD Edwards EnterpriseOne-Authentifizierung

Damit JD-Edwards-EnterpriseOne-Informationen von der BI-Plattform genutzt werden können, benötigt die Plattform Angaben zur Authentifizierung im JD-Edwards-EnterpriseOne-System.

9.7.2.1 Aktivieren der JD Edwards-Authentifizierung in der BI-Plattform

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie im Verwaltungsbereich auf **Authentifizierung**.
3. Doppelklicken Sie auf **JD Edwards EnterpriseOne**.
   Die Seite *JD Edwards EnterpriseOne* wird angezeigt.
4. Aktivieren Sie auf der Registerkarte **Optionen** das Kontrollkästchen **JD Edwards EnterpriseOne-Authentifizierung aktivieren**.
5. Nehmen Sie unter **Neuer Alias**, **Aktualisierungsoptionen** und **Optionen für neue Benutzer** die Änderungen vor, die je nach Ihrer BI-Plattform-Implementierung erforderlich sind. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern, bevor Sie mit der Registerkarte **Systeme** fortfahren.
6. Klicken Sie auf die Registerkarte **Server**.
7. Kopieren Sie `jdeutil.jar`, `kernel.jar` und `log4j.jar` aus der JD-Edwards-Installation in diese Speicherorte (unter Windows): `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\java\lib\jdedwards\default\jdedwards\` und `<INSTALLVERZ>\Tomcat\lib\`.
8. Starten Sie Tomcat und den Server Intelligence Agent neu.
9. Geben Sie im Bereich *JD Edwards EnterpriseOne-Systembenutzer* einen Datenbank-Benutzernamen und ein Kennwort ein, die die BI-Plattform für die Anmeldung bei Ihrer JD Edwards EnterpriseOne-Datenbank verwenden soll.
10. Geben Sie im Bereich *JD Edwards EnterpriseOne-Domäne* den Namen, den Host und den Port ein, der zum Herstellen einer Verbindung zur JD Edwards EnterpriseOne-Umgebung verwendet wird, geben Sie einen Namen für die Umgebung ein und klicken auf **Hinzufügen**.
11. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.7.3 Zuordnen von JD-Edwards-EnterpriseOne-Rollen zur BI-Plattform

Die BI-Plattform erstellt für jede zugeordnete JD Edwards EnterpriseOne-Rolle automatisch eine Gruppe. Darüber hinaus erstellt das System Aliase, die die Mitglieder der zugeordneten JD Edwards EnterpriseOne-Rollen darstellen.

Sie können für jeden erstellten Alias ein Benutzerkonto erstellen.

Wenn Sie jedoch mehrere Systeme ausführen und Ihre Benutzer in mehreren Systemen über Konten verfügen, können Sie jeden Benutzer einem Alias mit demselben Namen zuordnen, bevor Sie die Konten in der BI-Plattform erstellen.

Auf diese Weise reduziert sich die Anzahl der Konten, die für ein und denselben Benutzer in der BI-Plattform erstellt werden muss.

Wenn Sie beispielsweise eine JD Edwards EnterpriseOne-Testumgebung und eine JD Edwards EnterpriseOne-Produktionsumgebung betreiben und 30 Ihrer Benutzer Zugriff auf beide Systeme haben, werden nur 30 Konten für diese Benutzer eingerichtet. Wenn Sie die Benutzer nicht jeweils einem Alias mit demselben Namen zuweisen, werden für die 30 Benutzer in der BI-Plattform 60 Konten eingerichtet.

Falls Sie jedoch mehrere Systeme ausführen und identische Benutzernamen vorhanden sind, muss für jeden erstellten Alias ein neues Mitgliedskonto erstellt werden.

Wenn Sie Ihre Testumgebung beispielsweise mit einem Benutzerkonto für Ronald Schneider (Benutzername "rschneider") und die Produktionsumgebung mit einem Benutzerkonto für Regina Schneider (Benutzername "rschneider") ausführen, müssen Sie ein separates Konto für den Alias jedes Benutzers erstellen. Andernfalls werden die beiden Benutzer demselben BI-Plattform-Konto hinzugefügt und können sich nicht mit ihren eigenen JD Edwards EnterpriseOne-Anmeldedaten bei der BI-Plattform anmelden.

9.7.3.1 Zuordnen einer JD Edwards EnterpriseOne-Rolle

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie im Bereich *Verwalten* auf **Authentifizierung**.
3. Doppelklicken Sie auf **JD Edwards EnterpriseOne**.
4. Wählen Sie im Bereich **Optionen für neuen Alias** eine der folgenden Optionen aus:
   - **Jeden hinzugefügten Alias einem Konto mit demselben Namen zuweisen**

     Aktivieren Sie diese Option bei Verwendung mehrerer JD Edwards EnterpriseOne Enterprise-Systeme mit Benutzern, die Konten auf mehr als einem System besitzen (dabei dürfen zwei Benutzer jedoch nicht denselben Benutzernamen auf unterschiedlichen Systemen haben).
   - **Neues Konto für jeden hinzugefügten Alias erstellen**

     Aktivieren Sie diese Option, wenn Sie nur ein JD Edwards EnterpriseOne-System ausführen und die Mehrheit Ihrer Benutzer nur ein Konto auf einem der Systeme hat oder falls für unterschiedliche Benutzer auf mindestens zwei Systemen identische Benutzernamen vorhanden sind.
5. Wählen Sie im Bereich **Aktualisierungsoptionen** eine der folgenden Optionen aus:
   - **Es werden neue Aliase hinzugefügt und neue Benutzer erstellt**

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wählen Sie diese Option, um einen neuen Alias für jeden Benutzer zu erstellen, der die BI-Plattform zugeordnet wird. Bei Benutzern ohne BI-Plattform-Konto oder bei Aktivierung der Option "Neues Konto für jeden hinzugefügten Alias erstellen" werden neue Konten für die Benutzer hinzugefügt.

- **Es werden keine neuen Aliase hinzugefügt und keine neuen Benutzer erstellt**

  Aktivieren Sie diese Option, wenn die zuzuordnende Rolle viele Benutzer umfasst, die BI-Plattform jedoch nur von einigen wenigen Benutzern genutzt wird. Aliase und Konten für die Benutzer werden vom System nicht automatisch erstellt. Vielmehr werden Aliase (und gegebenenfalls Konten) für die Benutzer erst dann erstellt, wenn sie sich zum ersten Mal bei der BI-Plattform anmelden. Dies ist die Standardoption.

6. Geben Sie unter **Optionen für neue Benutzer** an, wie neue Benutzer erstellt werden.

   Wählen Sie eine der folgenden Optionen:

   - **Neue Benutzer werden als Namenslizenzbenutzer erstellt**

     Neue Benutzerkonten werden für die Verwendung von Namenslizenzen konfiguriert. Namenslizenzen sind mit bestimmten Benutzern verbunden und ermöglichen den Zugriff auf das System auf der Grundlage von Benutzername und Kennwort. Dieser Lizenztyp ermöglicht Benutzern den Zugriff auf das System unabhängig von der Anzahl der derzeit verbundenen Benutzer. Für jedes mit dieser Option erstellte Benutzerkonto muss eine Namenslizenz verfügbar sein.
   - **Neue Benutzer werden als Zugriffslizenzbenutzer erstellt**

     Neue Benutzerkonten werden für die Verwendung von Zugriffslizenzen konfiguriert. Zugriffslizenzen geben die Anzahl der Personen an, die gleichzeitig mit der BI-Plattform verbunden sein können. Dieser Lizenztyp ist sehr flexibel, da mit einer geringen Anzahl von Zugriffslizenzen viele Benutzer unterstützt werden können. Je nach Häufigkeit und Dauer des Zugriffs auf die BI-Plattform können 100 Zugriffslizenzen beispielsweise 250, 500 oder auch 700 Benutzer unterstützen.

   Die ausgewählten Rollen werden jetzt als Gruppen in der BI-Plattform angezeigt.
7. Klicken Sie auf die Registerkarte **Rollen**.
8. Wählen Sie unter **Domänenliste** den JD-Edwards-Server, der die gewünschten Rollen enthält.
9. Wählen Sie unter *Verfügbare Rollen* die Rollen, die Sie der BI-Plattform zuweisen wollen, und klicken Sie auf **<**.
10. Klicken Sie auf **Aktualisieren**.
    Die Rollen werden der BI-Plattform zugeordnet.

9.7.3.2 Hinweise zum erneuten Zuordnen

Wenn Sie Benutzer einer Rolle hinzufügen, die der BI-Plattform bereits zugeordnet wurde, müssen Sie die Rolle erneut zuordnen, damit die Benutzer zur BI-Plattform hinzugefügt werden. Beim erneuten Zuordnen der Rolle hat die Option zum Zuordnen der Benutzer als Namenslizenz- oder Zugriffslizenzbenutzer nur Einfluss auf die neuen, der Rolle hinzugefügten Benutzer.

Beispiel: Zuerst ordnen Sie der BI-Plattform eine Rolle mit aktivierter Option "Neue Benutzer werden als *Namenslizenzbenutzer* erstellt" zu. Später fügen Sie derselben Rolle Benutzer hinzu und ordnen die Rolle dann erneut zu, während die Option "Neue Benutzer werden als *Zugriffslizenzbenutzer* erstellt" aktiviert ist.

In diesem Fall werden nur die neuen Benutzer in der Rolle der BI-Plattform als Zugriffslizenzbenutzer zugeordnet. Benutzer, die bereits zugeordnet waren, bleiben Namenslizenzbenutzer. Dasselbe gilt, wenn Sie Benutzer erst als Zugriffslizenzbenutzer zuordnen und später die Einstellungen ändern, um neue Benutzer als Namenslizenzbenutzer neu zuzuordnen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.7.3.3 Aufheben der Zuordnung einer Rolle

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie im Bereich *Verwalten* auf **Authentifizierung**.
3. Klicken Sie auf die Registerkarte für **JD Edwards EnterpriseOne**.
4. Wählen Sie im Bereich *Rollen* die zu entfernende Rolle aus, und klicken Sie auf **<**.
5. Klicken Sie auf **Aktualisieren**.

   Mitglieder der Rolle sind nicht mehr in der Lage, auf die BI-Plattform zuzugreifen, es sei denn, sie verfügen noch über andere Konten oder Aliase.

   > **Hinweis**
   >
   > Sie können auch einzelne Konten löschen oder Benutzer aus Rollen entfernen, bevor Sie die Rollen der BI-Plattform zuordnen, um zu verhindern, dass sich bestimmte Benutzer anmelden können.

9.7.4 Zeitgesteuertes Verarbeiten von Benutzeraktualisierungen

Um sicherzustellen, dass Änderungen Ihrer Benutzerdaten für das ERP-System in Ihren BI-Plattform-Benutzerdaten widergespiegelt werden, können Sie regelmäßige Benutzeraktualisierungen planen. Diese Aktualisierungen synchronisieren automatisch die ERP- und BI-Plattform-Benutzer in Übereinstimmung mit den Zuordnungseinstellungen, die Sie in der Central Management Console (CMC) konfiguriert haben.

Für die Ausführung und zeitgesteuerte Verarbeitung von Aktualisierungen für importierte Rollen stehen zwei Optionen zur Verfügung:

- Nur Rollen aktualisieren: Bei Verwendung dieser Option werden nur die Verknüpfungen zwischen den aktuell zugeordneten Rollen aktualisiert, die in die BI-Plattform importiert wurden. Verwenden Sie diese Option, wenn Sie voraussichtlich häufig Aktualisierungen ausführen müssen und Bedenken hinsichtlich der Systemressourcennutzung haben. Wenn Sie nur Rollen aktualisieren, werden keine neuen Benutzerkonten erstellt.
- Rollen und Aliase aktualisieren: Bei Verwendung dieser Option werden nicht nur Verknüpfungen zwischen Rollen aktualisiert, sondern auch neue Benutzerkonten in der BI-Plattform für neue Benutzeraliase erstellt, die zum ERP-System hinzugefügt wurden.

> **Hinweis**
>
> Wenn Sie bei der Aktivierung der Authentifizierung nicht angegeben haben, dass Benutzeraliase automatisch für Aktualisierungen erstellt werden sollen, werden keine Konten für neue Aliase erstellt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.7.4.1 Zeitgesteuertes Verarbeiten von Benutzeraktualisierungen

Nachdem Sie Rollen in der BI-Plattform zugeordnet haben, müssen Sie angeben, wie das System diese Rollen aktualisiert.

1. Klicken Sie auf die Registerkarte **Benutzeraktualisierung**.
2. Klicken Sie im Abschnitt *Nur Rollen aktualisieren* oder *Rollen und Aliase aktualisieren* auf **Zeitgesteuert verarbeiten**.

   ➡ Tipp

   Wenn Sie die Aktualisierung sofort ausführen möchten, klicken Sie auf **Jetzt aktualisieren**.

   ➡ Tipp

   Verwenden Sie die Option *Nur Rollen aktualisieren*, wenn Sie häufig aktualisieren möchten und Bedenken bezüglich der Systemressourcen haben. Das System benötigt mehr Zeit, um sowohl Rollen als auch Aliase zu aktualisieren.

   Das Dialogfeld *Wiederholung* wird angezeigt.
3. Wählen Sie in der Liste *Objekt ausführen* eine Option aus, und geben Sie alle angeforderten Informationen zur zeitgesteuerten Verarbeitung ein.

   Bei der zeitgesteuerten Verarbeitung einer Aktualisierung stehen Ihnen die Wiederholungsmuster in der folgenden Tabelle zur Verfügung:

Wiederholungsmuster	Beschreibung
Stündlich	Die Aktualisierung wird stündlich ausgeführt. Sie legen die Startzeit sowie Anfangs- und Enddatum für das Objekt fest.
Täglich	Die Aktualisierung wird täglich oder alle n angegebenen Tage ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum für das Objekt festlegen.
Wöchentlich	Die Aktualisierung wird wöchentlich ausgeführt. Es kann einmal die Woche oder mehrmals wöchentlich ausgeführt werden. Sie können festlegen, an welchen Tagen und zu welcher Uhrzeit das Objekt ausgeführt wird, und das Anfangs- und Enddatum der Ausführung bestimmen.
Monatlich	Die Aktualisierung wird einmal monatlich oder alle n Monate ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am n-ten Tag des Monats	Die Aktualisierung wird an einem bestimmten Tag des Monats ausgeführt. Sie können festlegen, an welchem Tag des Monats und zu welcher Uhrzeit die Aktualisierung ausgeführt wird, sowie Anfangs- und Enddatum der Ausführung bestimmen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wiederholungsmuster	Beschreibung
Am ersten Montag des Monats	Die Aktualisierung wird jeden Monat am ersten Montag ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am letzten Tag des Monats	Die Aktualisierung wird am letzten Tag jedes Monats ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am x-ten Tag der n-ten Woche des Monats	Die Aktualisierung wird an einem bestimmten Tag einer bestimmten Woche im Monat ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Kalender	Die Aktualisierung wird zu den Terminen ausgeführt, die in einem zuvor erstellten Kalender festgelegt wurden.

4. Klicken Sie auf **Zeitgesteuert verarbeiten**, nachdem Sie die Informationen für die zeitgesteuerte Verarbeitung angegeben haben.
   In der Registerkarte **Benutzeraktualisierung** wird das Datum der nächsten zeitgesteuert verarbeiteten Rollenaktualisierung angezeigt.

> **Hinweis**
>
> Sie können die nächste zeitgesteuert verarbeitete Aktualisierung jederzeit abbrechen, indem Sie im Abschnitt *Nur Rollen aktivieren* oder *Rollen und Aliase aktivieren* auf **Geplante Aktualisierungen abbrechen** klicken.

9.8 Siebel-Authentifizierung

9.8.1 Aktivieren der Siebel-Authentifizierung

Damit Siebel-Informationen von der BI-Plattform verwendet werden können, benötigt diese Informationen zur Authentifizierung im Siebel-System.

9.8.1.1 Aktivieren der Siebel-Authentifizierung in BI-Plattform

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie im Verwaltungsbereich auf **Authentifizierung**.
3. Doppelklicken Sie auf **Siebel**.
   Die Seite *Siebel* wird angezeigt. Sie verfügt über vier Registerkarten: **Optionen**, **Systeme**, **Zuständigkeiten** und **Benutzeraktualisierung**.
4. Aktivieren Sie auf der Registerkarte **Optionen** das Kontrollkästchen **Siebel-Authentifizierung aktivieren**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

5. Nehmen Sie unter **Neuer Alias**, **Aktualisierungsoptionen** und **Optionen für neue Benutzer** die Änderungen vor, die je nach Ihrer BI-Plattform-Implementierung erforderlich sind. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern, bevor Sie mit der Registerkarte **Systeme** fortfahren.
6. Klicken Sie auf die Registerkarte **Domänen**.
7. Geben Sie im Feld **Domänenname** den Domänennamen für das Siebel-System ein, zu dem Sie eine Verbindung herstellen möchten.
8. Geben Sie unter **Verbindung** die Verbindungszeichenfolge für diese Domäne ein.
9. Geben Sie im Bereich **Benutzername** einen Datenbank-Benutzernamen und ein Kennwort ein, die die BI-Plattform für die Anmeldung bei der Siebel-Datenbank verwenden soll.
10. Geben Sie im Bereich **Kennwort** das Kennwort für den Benutzer ein, den Sie ausgewählt haben.
11. Klicken Sie auf **Hinzufügen**, um die Systeminformationen zu der Liste *Aktuelle Domänen* hinzuzufügen.
12. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

9.8.2 Zuordnen von Rollen zur BI-Plattform

Die BI-Plattform erstellt für jede zugeordnete Siebel-Rolle automatisch eine Gruppe. Darüber hinaus erstellt das Programm Aliase, die die Mitglieder der zugeordneten Siebel-Rollen darstellen.

Sie können für jeden erstellten Alias ein Benutzerkonto erstellen.

Wenn Sie jedoch mehrere Systeme ausführen und Ihre Benutzer in mehreren Systemen über Konten verfügen, können Sie jeden Benutzer einem Alias mit demselben Namen zuordnen, bevor Sie die Konten in der BI-Plattform erstellen

Auf diese Weise reduziert sich die Anzahl der Konten, die für ein und denselben Benutzer im Programm erstellt werden müssen.

Wenn Sie beispielsweise eine Siebel-eBusiness-Testumgebung und eine Produktionsumgebung betreiben und 30 Ihrer Benutzer Zugriff auf beide Systeme haben, werden nur 30 Konten für diese Benutzer eingerichtet. Wenn Sie die Benutzer nicht jeweils einem Alias mit demselben Namen zuweisen, werden für die 30 Benutzer in der BI-Plattform 60 Konten eingerichtet.

Falls Sie jedoch mehrere Systeme ausführen und identische Benutzernamen vorhanden sind, muss für jeden erstellten Alias ein neues Mitgliedskonto erstellt werden.

Wenn Sie Ihre Testumgebung beispielsweise mit einem Benutzerkonto für Ronald Schneider (Benutzername "rschneider") und die Produktionsumgebung mit einem Benutzerkonto für Regina Schneider (Benutzername "rschneider") ausführen, müssen Sie ein separates Konto für den Alias jedes Benutzers erstellen. Andernfalls werden die beiden Benutzer demselben Konto hinzugefügt, und sie können sich nicht mit ihren eigenen Siebel eBusiness-Anmeldedaten bei der BI-Plattform anmelden.

9.8.2.1 Zuordnen einer Siebel-eBusiness-Rolle zur BI-Plattform

1. Melden Sie sich als Administrator bei der Central Management Console an.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Klicken Sie auf **Authentifizierung**.
3. Doppelklicken Sie auf **Siebel**.
4. Markieren Sie das Kontrollkästchen **Siebel-Authentifizierung aktivieren**.
5. Wählen Sie im Bereich **Optionen für neuen Alias** eine der folgenden Optionen aus:
   - **Jeden hinzugefügten Alias einem Konto mit demselben Namen zuweisen**

     Aktivieren Sie diese Option bei Verwendung mehrerer Siebel eBusiness-Systeme mit Benutzern, die über Konten auf mehreren Systemen verfügen (dabei dürfen zwei Benutzer jedoch nicht denselben Benutzernamen auf unterschiedlichen Systemen besitzen).
   - **Neues Konto für jeden hinzugefügten Alias erstellen**

     Aktivieren Sie diese Option, wenn Sie nur ein Siebel eBusiness-System ausführen und die Mehrheit Ihrer Benutzer nur über ein Konto auf einem der Systeme verfügt oder falls für unterschiedliche Benutzer auf mindestens zwei Systemen identische Benutzernamen vorhanden sind.
6. Wählen Sie im Bereich **Aktualisierungsoptionen für Aliase** eine der folgenden Optionen aus:
   - **Neue Aliase bei der Aliasaktualisierung erstellen**

     Wählen Sie diese Option, um einen neuen Alias für jeden Benutzer zu erstellen, den Sie der BI-Plattform zuordnen. Bei Benutzern ohne BI-Plattform-Konto oder bei Aktivierung der Option "Neues Konto für jeden hinzugefügten Alias erstellen" werden neue Konten für die Benutzer hinzugefügt.
   - **Neue Aliase nur bei der Benutzeranmeldung erstellen**

     Aktivieren Sie diese Option, wenn die zuzuordnende Rolle viele Benutzer umfasst, die BI-Plattform jedoch nur von einigen wenigen Benutzern genutzt wird. Aliase und Konten für die Benutzer werden vom Programm nicht automatisch erstellt. Vielmehr werden Aliase (und ggf. Konten) für die Benutzer erst dann erstellt, wenn sie sich zum ersten Mal bei der BI-Plattform anmelden. Dies ist die Standardoption.
7. Geben Sie unter **Optionen für neue Benutzer** an, wie neue Benutzer erstellt werden.

   Falls Ihre BI-Plattform-Lizenz auf Benutzerrollen basiert, wählen Sie eine der folgenden Optionen:

   Wählen Sie eine der folgenden Optionen:
   - **Neue Benutzer werden als vordefinierte Benutzer erstellt**

     Neue Benutzerkonten werden für die Verwendung von Namenslizenzen konfiguriert. Namenslizenzen sind mit bestimmten Benutzern verbunden und ermöglichen den Zugriff auf das System auf der Grundlage von Benutzername und Kennwort. Dieser Lizenztyp ermöglicht Benutzern den Zugriff auf das System unabhängig von der Anzahl der derzeit verbundenen Benutzer. Für jedes mit dieser Option erstellte Benutzerkonto muss eine Namenslizenz verfügbar sein.
   - **Neue Benutzer werden als gleichzeitige Benutzer erstellt**

     Neue Benutzerkonten werden für die Verwendung von Zugriffslizenzen konfiguriert. Zugriffslizenzen geben die Anzahl der Personen an, die gleichzeitig mit der BI-Plattform verbunden sein können. Dieser Lizenztyp ist sehr flexibel, da mit einer geringen Anzahl von Zugriffslizenzen viele Benutzer unterstützt werden können. Je nach Häufigkeit und Dauer des Zugriffs auf die BI-Plattform können 100 Zugriffslizenzen beispielsweise 250, 500 oder auch 700 Benutzer unterstützen.
8. Klicken Sie auf die Registerkarte **Rollen**.
9. Wählen Sie die Domäne, die dem Siebel-Server entspricht, für den Sie Rollen zuordnen möchten.
10. Wählen Sie unter *Verfügbare Rollen* die zuzuordnenden Rollen, und klicken Sie auf **>**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Sie können die Suche über das Feld **Rollen suchen, die wie folgt anfangen:** eingrenzen, wenn Sie eine große Anzahl von Rollen haben. Geben Sie die Zeichen ein, mit denen die Rolle bzw. Rollen beginnen sollen, gefolgt von einem Platzhalterzeichen (%), und klicken Sie auf **Suchen**.

> **Hinweis**
>
> Damit die Suchfunktion funktioniert, muss eine Siebel-Plugin-jar-Datei im lib-Verzeichnis von Tomcat implementiert werden: `<INSTALLVERZ>\tomcat\webapps\BOE\WEB-INF\lib` und `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\java\lib\siebel\default\siebel`. Starten Sie den Tomcat-Server und den Server Intelligence Agent neu.

11. Klicken Sie auf **Aktualisieren**.
    Die Rollen werden der BI-Plattform zugeordnet.

9.8.2.2 Hinweise zum erneuten Zuordnen

Um die Gruppen- und Benutzersynchronisierung zwischen der BI-Plattform und Siebel zu erzwingen, aktivieren Sie die Option **Benutzersynchronisierung erzwingen**.

> **Hinweis**
>
> Um **Benutzersynchronisierung erzwingen** auswählen zu können, müssen Sie zuerst **Es werden neue Aliase hinzugefügt und neue Benutzer erstellt** auswählen.

Beim erneuten Zuordnen der Rolle hat die Option zum Zuordnen der Benutzer als Namenslizenz- oder Zugriffslizenzbenutzer nur Einfluss auf die neuen, der Rolle hinzugefügten Benutzer.

Beispiel: Zuerst ordnen Sie der BI-Plattform eine Rolle mit aktivierter Option "Neue Benutzer werden als *Namenslizenzbenutzer* erstellt" zu. Später fügen Sie derselben Rolle Benutzer hinzu und ordnen die Rolle dann erneut zu, während die Option "Neue Benutzer werden als *Zugriffslizenzbenutzer* erstellt" aktiviert ist.

In diesem Fall werden nur die neuen Benutzer in der Rolle der BI-Plattform als Zugriffslizenzbenutzer zugeordnet. Benutzer, die bereits zugeordnet waren, bleiben Namenslizenzbenutzer. Dasselbe gilt, wenn Sie Benutzer erst als Zugriffslizenzbenutzer zuordnen und später die Einstellungen ändern, um neue Benutzer als Namenslizenzbenutzer neu zuzuordnen.

9.8.2.3 Aufheben der Zuordnung einer Rolle

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie im Bereich *Verwalten* auf **Authentifizierung**.
3. Doppelklicken Sie auf **Siebel**.
4. Wählen Sie auf der Registerkarte **Domänen** die Siebel-Domäne, die der Rolle bzw. den Rollen entsprechen, deren Zuordnung Sie aufheben möchten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

5. Wählen Sie auf der Registerkarte **Rollen** die zu entfernende Rolle aus, und klicken Sie auf **<**.
6. Klicken Sie auf **Aktualisieren**.

   Mitglieder der Rolle sind nicht mehr in der Lage, auf die BI-Plattform zuzugreifen, es sei denn, sie verfügen noch über andere Konten oder Aliase.

   > **Hinweis**
   >
   > Sie können auch einzelne Konten löschen oder Benutzer aus Rollen entfernen, bevor Sie die Rollen der BI-Plattform zuordnen, um zu verhindern, dass sich bestimmte Benutzer anmelden können.

9.8.3 Zeitgesteuertes Verarbeiten von Benutzeraktualisierungen

Um sicherzustellen, dass Änderungen Ihrer Benutzerdaten für das ERP-System in Ihren BI-Plattform-Benutzerdaten widergespiegelt werden, können Sie regelmäßige Benutzeraktualisierungen planen. Diese Aktualisierungen synchronisieren automatisch die ERP- und BI-Plattform-Benutzer in Übereinstimmung mit den Zuordnungseinstellungen, die Sie in der Central Management Console (CMC) konfiguriert haben.

Für die Ausführung und zeitgesteuerte Verarbeitung von Aktualisierungen für importierte Rollen stehen zwei Optionen zur Verfügung:

- Nur Rollen aktualisieren: Bei Verwendung dieser Option werden nur die Verknüpfungen zwischen den aktuell zugeordneten Rollen aktualisiert, die in die BI-Plattform importiert wurden. Verwenden Sie diese Option, wenn Sie voraussichtlich häufig Aktualisierungen ausführen müssen und Bedenken hinsichtlich der Systemressourcennutzung haben. Wenn Sie nur Rollen aktualisieren, werden keine neuen Benutzerkonten erstellt.
- Rollen und Aliase aktualisieren: Bei Verwendung dieser Option werden nicht nur Verknüpfungen zwischen Rollen aktualisiert, sondern auch neue Benutzerkonten in der BI-Plattform für neue Benutzeraliase erstellt, die zum ERP-System hinzugefügt wurden.

> **Hinweis**
>
> Wenn Sie bei der Aktivierung der Authentifizierung nicht angegeben haben, dass Benutzeraliase automatisch für Aktualisierungen erstellt werden sollen, werden keine Konten für neue Aliase erstellt.

9.8.3.1 Zeitgesteuertes Verarbeiten von Benutzeraktualisierungen

Nachdem Sie Rollen in der BI-Plattform zugeordnet haben, müssen Sie angeben, wie das System diese Rollen aktualisiert.

1. Klicken Sie auf die Registerkarte **Benutzeraktualisierung**.
2. Klicken Sie im Abschnitt *Nur Rollen aktualisieren* oder *Rollen und Aliase aktualisieren* auf **Zeitgesteuert verarbeiten**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

➔ Tipp

Wenn Sie die Aktualisierung sofort ausführen möchten, klicken Sie auf **Jetzt aktualisieren**.

➔ Tipp

Verwenden Sie die Option *Nur Rollen aktualisieren*, wenn Sie häufig aktualisieren möchten und Bedenken bezüglich der Systemressourcen haben. Das System benötigt mehr Zeit, um sowohl Rollen als auch Aliase zu aktualisieren.

Das Dialogfeld *Wiederholung* wird angezeigt.

3. Wählen Sie in der Liste *Objekt ausführen* eine Option aus, und geben Sie alle angeforderten Informationen zur zeitgesteuerten Verarbeitung ein.

   Bei der zeitgesteuerten Verarbeitung einer Aktualisierung stehen Ihnen die Wiederholungsmuster in der folgenden Tabelle zur Verfügung:

Wiederholungsmuster	Beschreibung
Stündlich	Die Aktualisierung wird stündlich ausgeführt. Sie legen die Startzeit sowie Anfangs- und Enddatum für das Objekt fest.
Täglich	Die Aktualisierung wird täglich oder alle n angegebenen Tage ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum für das Objekt festlegen.
Wöchentlich	Die Aktualisierung wird wöchentlich ausgeführt. Es kann einmal die Woche oder mehrmals wöchentlich ausgeführt werden. Sie können festlegen, an welchen Tagen und zu welcher Uhrzeit das Objekt ausgeführt wird, und das Anfangs- und Enddatum der Ausführung bestimmen.
Monatlich	Die Aktualisierung wird einmal monatlich oder alle n Monate ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am n-ten Tag des Monats	Die Aktualisierung wird an einem bestimmten Tag des Monats ausgeführt. Sie können festlegen, an welchem Tag des Monats und zu welcher Uhrzeit die Aktualisierung ausgeführt wird, sowie Anfangs- und Enddatum der Ausführung bestimmen.
Am ersten Montag des Monats	Die Aktualisierung wird jeden Monat am ersten Montag ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am letzten Tag des Monats	Die Aktualisierung wird am letzten Tag jedes Monats ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am x-ten Tag der n-ten Woche des Monats	Die Aktualisierung wird an einem bestimmten Tag einer bestimmten Woche im Monat ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Kalender	Die Aktualisierung wird zu den Terminen ausgeführt, die in einem zuvor erstellten Kalender festgelegt wurden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Klicken Sie auf **Zeitgesteuert verarbeiten**, nachdem Sie die Informationen für die zeitgesteuerte Verarbeitung angegeben haben.
   In der Registerkarte **Benutzeraktualisierung** wird das Datum der nächsten zeitgesteuert verarbeiteten Rollenaktualisierung angezeigt.

> **Hinweis**
>
> Sie können die nächste zeitgesteuert verarbeitete Aktualisierung jederzeit abbrechen, indem Sie im Abschnitt *Nur Rollen aktivieren* oder *Rollen und Aliase aktivieren* auf **Geplante Aktualisierungen abbrechen** klicken.

9.9 Oracle EBS-Authentifizierung

9.9.1 Aktivieren der Oracle-EBS-Authentifizierung

Damit Oracle-EBS-Informationen von der BI-Plattform verwendet werden können, benötigt das System Informationen zur Authentifizierung im Oracle-EBS-System.

9.9.1.1 Aktivieren der Oracle E-Business Suite-Authentifizierung

Vor dem Durchführen des Vorgangs müssen Oracle-DLL- und -JAR-Dateien auf der BI-Plattform installiert werden:

1. Laden Sie die Datei `ojdbc11.dll` von der Oracle-Datenbank-Clientanwendung herunter.
2. Kopieren Sie die Datei an diesem Speicherort:
   - Windows: `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`
   - UNIX: `<INSTALLVERZ>/sap_bobj/enterprise_xi40/platform`
3. Laden Sie die Datei `ojdbc5.jar` von der Oracle-Datenbank-Clientanwendung herunter.
4. Kopieren Sie die Datei an diesem Speicherort:
   - Windows: `<INSTALLVERZ>\Tomcat\lib`
   - UNIX: `<INSTALLVERZ>/sap_bobj/tomcat/lib`

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie im Verwaltungsbereich auf **Authentifizierung**.
3. Klicken Sie auf **Oracle EBS**.
   Die Seite *Oracle EBS* wird angezeigt. Sie enthält vier Registerkarten: **Optionen**, **Systeme**, **Zuständigkeiten** und **Benutzeraktualisierung**.
4. Aktivieren Sie auf der Registerkarte **Optionen** das Kontrollkästchen **Oracle EBS-Authentifizierung ist aktiviert**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

5. Nehmen Sie unter **Neuer Alias**, **Aktualisierungsoptionen** und **Optionen für neue Benutzer** die Änderungen vor, die je nach Ihrer BI-Plattform-Implementierung erforderlich sind. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern, bevor Sie mit der Registerkarte **Systeme** fortfahren.
6. Klicken Sie auf die Registerkarte **Systeme**.
7. Geben Sie im Bereich *Oracle EBS-Systembenutzer* einen Datenbank-Benutzernamen und ein Kennwort ein, die die BI-Plattform für die Anmeldung bei Ihrer Oracle-E-Business Suite-Datenbank verwenden soll.
8. Geben Sie im Bereich *Oracle EBS Services* den Service-Namen ein, der von Ihrer Oracle EBS-Umgebung verwendet wird, und klicken Sie auf **Hinzufügen**.
9. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

Sie müssen nun in dem System Oracle EBS-Rollen zuordnen.

Weitere Informationen

Zuordnen von Oracle-E-Business-Suite-Rollen [Seite 358]

9.9.2 Zuordnen von Oracle-E-Business Suite-Rollen zur BI-Plattform

Die BI-Plattform erstellt automatisch eine Gruppe für jede Oracle-E-Business Suite-Rolle (EBS), die Sie zuordnen. Das System erstellt außerdem Aliase für die Mitglieder der zugeordneten Oracle E-Business Suite-Rollen.

Sie können für jeden erstellten Alias ein Benutzerkonto erstellen. Wenn Sie jedoch mehrere Systeme ausführen und Ihre Benutzer in mehreren Systemen über Konten verfügen, können Sie jeden Benutzer einem Alias mit demselben Namen zuordnen, bevor Sie die Konten in der BI-Plattform erstellen.

Auf diese Weise reduziert sich die Anzahl der Konten, die für ein und denselben Benutzer im System erstellt werden müssen.

Wenn Sie beispielsweise eine EBS-Testumgebung und eine Produktionsumgebung betreiben und 30 Ihrer Benutzer Zugriff auf beide Systeme haben, werden nur 30 Konten für diese Benutzer eingerichtet. Wenn Sie die Benutzer nicht jeweils einem Alias mit demselben Namen zuweisen, werden für die 30 Benutzer in der BI-Plattform 60 Konten eingerichtet.

Falls Sie jedoch mehrere Systeme ausführen und identische Benutzernamen vorhanden sind, muss für jeden erstellten Alias ein neues Mitgliedskonto erstellt werden.

Wenn Sie Ihre Testumgebung beispielsweise mit einem Benutzerkonto für Ronald Schneider (Benutzername "rschneider") und die Produktionsumgebung mit einem Benutzerkonto für Regina Schneider (Benutzername "rschneider") ausführen, müssen Sie ein separates Konto für den Alias jedes Benutzers erstellen. Andernfalls werden die beiden Benutzer demselben BI-Plattform-Konto hinzugefügt, können sich mit ihren eigenen Oracle EBS-Anmeldedaten am System anmelden und haben Zugriff auf Daten aus beiden EBS-Umgebungen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.9.2.1 Zuordnen von Oracle-E-Business-Suite-Rollen

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie im Verwaltungsbereich auf **Authentifizierung**.
3. Klicken Sie auf **Oracle EBS**.
   Auf der Seite *Oracle EBS* wird die Registerkarte **Optionen** angezeigt.
4. Wählen Sie im Bereich *Optionen für neuen Alias* eine der folgenden Optionen aus:
   - **Jeden hinzugefügten Oracle EBS-Alias einem Konto mit demselben Namen zuordnen**

     Aktivieren Sie diese Option bei Verwendung mehrerer Oracle E-Business Suite-Systeme mit Benutzern, die über Konten auf mehreren Systemen verfügen (dabei dürfen zwei Benutzer jedoch nicht denselben Benutzernamen auf unterschiedlichen Systemen besitzen).
   - **Neues Konto für jeden hinzugefügten Oracle EBS-Alias erstellen**

     Aktivieren Sie diese Option, wenn Sie nur ein Oracle E-Business Suite-System ausführen und die Mehrheit Ihrer Benutzer nur über ein Konto auf einem der Systeme verfügt oder falls für unterschiedliche Benutzer auf mindestens zwei Systemen identische Benutzernamen vorhanden sind.
5. Wählen Sie im Bereich *Aktualisierungsoptionen* eine der folgenden Optionen aus:
   - **Neue Aliase bei der Aliasaktualisierung erstellen**

     Wählen Sie diese Option, um einen neuen Alias für jeden Benutzer zu erstellen, den Sie der BI-Plattform zuordnen. Bei Benutzern ohne BI-Plattform-Konten oder bei Aktivierung der Option **Neues Konto für jeden hinzugefügten Oracle EBS-Alias erstellen** werden neue Konten für die Benutzer hinzugefügt.
   - **Neue Aliase nur bei der Benutzeranmeldung erstellen**

     Aktivieren Sie diese Option, wenn die zuzuordnende Rolle viele Benutzer umfasst, die BI-Plattform jedoch nur von einigen wenigen Benutzern genutzt wird. Aliase und Konten für die Benutzer werden von der Plattform nicht automatisch erstellt. Vielmehr werden Aliase (und gegebenenfalls Konten) für die Benutzer erst dann erstellt, wenn sie sich zum ersten Mal bei der BI-Plattform anmelden. Dies ist die Standardoption.
6. Geben Sie unter *Optionen für neue Benutzer* an, wie neue Benutzer erstellt werden, und klicken Sie dann auf **Aktualisieren**.

   Wählen Sie eine der folgenden Optionen:
   - **Neue Benutzer werden als Namenslizenzbenutzer erstellt**

     Neue Benutzerkonten werden für die Verwendung von Namenslizenzen konfiguriert. Namenslizenzen sind mit bestimmten Benutzern verbunden und ermöglichen den Zugriff auf das System auf der Grundlage von Benutzername und Kennwort. Dieser Lizenztyp ermöglicht Benutzern den Zugriff auf das System unabhängig von der Anzahl der derzeit verbundenen Benutzer. Für jedes mit dieser Option erstellte Benutzerkonto muss eine Namenslizenz verfügbar sein.
   - **Neue Benutzer werden als Zugriffslizenzbenutzer erstellt**

     Neue Benutzerkonten werden für die Verwendung von Zugriffslizenzen konfiguriert. Zugriffslizenzen geben die Anzahl der Personen an, die gleichzeitig mit der BI-Plattform verbunden sein können. Dieser Lizenztyp ist sehr flexibel, da mit einer geringen Anzahl von Zugriffslizenzen viele Benutzer unterstützt werden können. Je nach Häufigkeit und Dauer des Zugriffs auf die Plattform können 100 Zugriffslizenzen beispielsweise 250, 500 oder auch 700 Benutzer unterstützen.

   Die ausgewählten Rollen werden jetzt als Gruppen in der BI-Plattform angezeigt.
7. Klicken Sie auf die Registerkarte **Zuständigkeiten**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8. Wählen Sie unter **Aktuelle Oracle EBS Services** den Oracle EBS Service mit den Rollen, die Sie zuordnen möchten.
9. Unter *Zugeordnete Oracle EBS-Rollen* können Sie Filter für Oracle EBS-Benutzer angeben.
   a) Wählen Sie für die neue Rolle in der Liste **Zugeordnete Oracle EBS-Rollen**, welche Anwendungen Benutzer verwenden können.
   b) Wählen Sie in der Liste **Zuständigkeiten**, welche Oracle-Anwendungen, -Funktionen, -Berichte und gleichzeitig laufenden Programme der Benutzer ausführen kann.
   c) Wählen Sie unter **Sicherheitsgruppe** die der neuen Rolle zugewiesene Sicherheitsgruppe.
   d) Klicken Sie unter **Aktuelle Rolle** auf **Hinzufügen** oder *Löschen*, um die Sicherheitsgruppenzuweisungen für diese Rolle festzulegen.
10. Klicken Sie auf **Aktualisieren**.
    Die Rollen werden der BI-Plattform zugeordnet.

Nachdem Sie Rollen in der BI-Plattform zugeordnet haben, müssen Sie angeben, wie das System diese Rollen aktualisiert.

9.9.2.1.1 Aktualisieren von Oracle EBS-Rollen und -Benutzern

Nach der Aktivierung der Oracle-EBS-Authentifizierung müssen regelmäßige Aktualisierungen von zugeordneten Rollen, die in die BI-Plattform importiert wurden, zeitgesteuert verarbeitet und ausgeführt werden. Dadurch ist gewährleistet, dass aktualisierte Oracle EBS-Rolleninformationen in der BI-Plattform genau widergespiegelt werden.

Für die Ausführung und zeitgesteuerte Verarbeitung von Oracle EBS-Rollen stehen zwei Optionen zur Verfügung:

- Nur Rollen aktualisieren: Bei Verwendung dieser Option werden nur die Verknüpfungen zwischen den aktuell zugeordneten Rollen aktualisiert, die in die BI-Plattform importiert wurden. Es wird empfohlen, diese Option nur dann zu verwenden, wenn Sie häufig Aktualisierungen ausführen müssen und Bedenken hinsichtlich der Systemressourcennutzung haben. Wenn Sie nur Oracle EBS-Rollen aktualisieren, werden keine neuen Benutzerkonten erstellt.
- Rollen und Aliase aktualisieren: Bei Verwendung dieser Option werden nicht nur Verknüpfungen zwischen Rollen aktualisiert, sondern auch neue Benutzerkonten in der BI-Plattform für Benutzeraliase erstellt, die zu Rollen im Oracle-EBS-System hinzugefügt wurden.

> **Hinweis**
>
> Wenn Sie bei der Aktivierung der Oracle EBS-Authentifizierung nicht angegeben haben, dass Benutzeraliase automatisch für Aktualisierungen erstellt werden sollen, werden keine Konten für neue Aliase erstellt.

9.9.2.1.2 Zeitgesteuertes Verarbeiten für Oracle EBS-Rollen

Nachdem Sie Rollen in der BI-Plattform zugeordnet haben, müssen Sie angeben, wie das System diese Rollen aktualisiert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Klicken Sie auf die Registerkarte **Benutzeraktualisierung**.
2. Klicken Sie im Abschnitt *Nur Rollen aktualisieren* oder *Rollen und Aliase aktualisieren* auf **Zeitgesteuert verarbeiten**.

> **Tipp**
>
> Wenn Sie die Aktualisierung sofort ausführen möchten, klicken Sie auf **Jetzt aktualisieren**.

> **Tipp**
>
> Verwenden Sie die Option *Nur Rollen aktualisieren*, wenn Sie häufig aktualisieren möchten und Bedenken bezüglich der Systemressourcen haben. Das System benötigt mehr Zeit, um sowohl Rollen als auch Aliase zu aktualisieren.

Das Dialogfeld *Wiederholung* wird angezeigt.

3. Wählen Sie in der Pulldownliste *Objekt ausführen* eine Option aus, und geben Sie alle angeforderten Informationen zur zeitgesteuerten Verarbeitung in die vorgesehenen Felder ein.

Bei der zeitgesteuerten Verarbeitung einer Aktualisierung stehen Ihnen die Wiederholungsmuster in der folgenden Tabelle zur Verfügung:

Wiederholungsmuster	Beschreibung
Stündlich	Die Aktualisierung wird stündlich ausgeführt. Sie legen die Startzeit sowie Anfangs- und Enddatum für das Objekt fest.
Täglich	Die Aktualisierung wird täglich oder alle n angegebenen Tage ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum für das Objekt festlegen.
Wöchentlich	Die Aktualisierung wird wöchentlich ausgeführt. Sie kann einmal die Woche oder mehrmals wöchentlich ausgeführt werden. Sie können festlegen, an welchen Tagen und zu welcher Uhrzeit das Objekt ausgeführt wird, und das Anfangs- und Enddatum der Ausführung bestimmen.
Monatlich	Die Aktualisierung wird einmal monatlich oder alle n Monate ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am n-ten Tag des Monats	Die Aktualisierung wird an einem bestimmten Tag des Monats ausgeführt. Sie können festlegen, an welchem Tag des Monats und zu welcher Uhrzeit die Aktualisierung ausgeführt wird, sowie Anfangs- und Enddatum der Ausführung bestimmen.
Am ersten Montag des Monats	Die Aktualisierung wird jeden Monat am ersten Montag ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Am letzten Tag des Monats	Die Aktualisierung wird am letzten Tag jedes Monats ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wiederholungsmuster	Beschreibung
Am x-ten Tag der n-ten Woche des Monats	Die Aktualisierung wird an einem bestimmten Tag einer bestimmten Woche im Monat ausgeführt. Sie können die Ausführungszeit sowie Anfangs- und Enddatum festlegen.
Kalender	Die Aktualisierung wird zu den Terminen ausgeführt, die in einem zuvor erstellten Kalender festgelegt wurden.

4. Klicken Sie auf **Zeitgesteuert verarbeiten**, nachdem Sie die Informationen für die zeitgesteuerte Verarbeitung angegeben haben.
   In der Registerkarte **Benutzeraktualisierung** wird das Datum der nächsten zeitgesteuert verarbeiteten Rollenaktualisierung angezeigt.

> **Hinweis**
>
> Sie können die nächste zeitgesteuert verarbeitete Aktualisierung jederzeit abbrechen, indem Sie im Abschnitt *Nur Rollen aktivieren* oder *Rollen und Aliase aktivieren* auf **Geplante Aktualisierungen abbrechen** klicken.

9.9.3 Aufheben der Zuordnung von Rollen

Um zu verhindern, dass sich bestimmte Benutzergruppen bei der BI-Plattform anmelden, können Sie die Zuordnung der Rollen, denen sie angehören, aufheben.

9.9.3.1 Aufheben der Zuordnung einer Rolle

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie im Verwaltungsbereich auf **Authentifizierung**.
3. Doppelklicken Sie auf das ERP-System, für das Sie die Zuordnung von Rollen aufheben möchten.
   Auf der Seite des ERP-Systems wird die Registerkarte **Optionen** angezeigt.
4. Klicken Sie auf die Registerkarte **Zuständigkeiten**.
5. Wählen Sie die **Aktuelle Oracle EBS Services**.
6. Wählen Sie unter *Aktuelle Rolle* eine Rolle, und klicken Sie dann auf die Schaltfläche **Löschen**.
7. Klicken Sie auf **Aktualisieren**.

   Mitglieder der Rolle sind nicht mehr in der Lage, auf die BI-Plattform zuzugreifen, es sei denn, sie verfügen noch über andere Konten oder Aliase.

> **Hinweis**
>
> Sie können auch einzelne Konten löschen oder Benutzer aus Rollen entfernen, bevor Sie die Rollen der BI-Plattform zuordnen, um zu verhindern, dass sich bestimmte Benutzer anmelden können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9.9.4 Anpassen von Rechten für zugeordnete Oracle EBS-Gruppen und -Benutzer

Beim Zuordnen von Rollen zur BI-Plattform können Sie für die erstellten Gruppen und Benutzer Rechte festlegen oder Berechtigungen gewähren.

9.9.4.1 So weisen Sie Verwaltungsrechte zu

Um Benutzern die Verwaltung der BI-Plattform zu ermöglichen, müssen Sie sie zur standardmäßigen Administratorgruppe hinzufügen. Mitglieder dieser Gruppe haben vollständige Kontrolle über alle Aspekte des Systems, einschließlich Konten, Server, Ordner, Objekte Einstellungen usw.

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie im Bereich *Organisieren* auf **Benutzer und Gruppen**.
3. Klicken Sie in der Spalte *Name* mit der rechten Maustaste auf **Administratoren**, und wählen Sie **Mitglieder zur Gruppe hinzufügen**.

   Die Seite *Verfügbare Benutzer oder Gruppen* wird angezeigt.
4. Wählen Sie im Bereich **Benutzerliste** oder **Gruppenliste** die zugeordnete Rolle aus, der Verwaltungsrechte zugewiesen werden sollen.
5. Klicken Sie auf **>**, um die Rolle als Untergruppe unter der Administratorgruppe anzuordnen, und klicken Sie auf **OK**.

Jetzt verfügen die Mitglieder der Rolle über Administratorrechte für die BI-Plattform.

> **Hinweis**
>
> Sie können auch eine Rolle innerhalb von Oracle EBS erstellen, ihr die geeigneten Benutzer hinzufügen, die Rolle der BI-Plattform zuordnen und die zugeordnete Rolle als Untergruppe der standardmäßigen Administratorgruppe konfigurieren, um Mitgliedern der Rolle Administratorrechte zu gewähren.

9.9.4.2 Zuweisen von Veröffentlichungsrechten

Wenn in Ihrem Unternehmen Benutzer für das Erstellen von Inhalten verantwortlich sind, können Sie ihnen Rechte zum Veröffentlichen von Objekten in der BI-Plattform gewähren.

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie im Bereich *Organisieren* auf **Ordner**.
3. Wechseln Sie zu dem Ordner, dem Benutzer Objekte hinzufügen können.
4. Klicken Sie auf **Verwalten**, **Sicherheit auf oberster Ebene** und dann auf **Alle Ordner**.
5. Klicken Sie auf **Prinzipale hinzufügen**.

   Die Seite "Prinzipale hinzufügen" wird angezeigt.
6. Wählen Sie in der Liste **Verfügbare Benutzer oder Gruppen** die Gruppe mit den Mitgliedern aus, denen Sie Veröffentlichungsrechte gewähren möchten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7. Klicken Sie auf **>**, damit die Gruppe auf den Ordner zugreifen kann, und klicken Sie dann auf **Sicherheit hinzufügen und zuweisen**.

   Die Seite "Sicherheit zuweisen" wird angezeigt.
8. Wählen Sie in der Liste **Verfügbare Zugriffsberechtigungen** die gewünschte Zugriffsberechtigung aus, und klicken Sie auf **>**, um die Zugriffsberechtigung explizit zuzuweisen.
9. Wenn die Optionen **Vom übergeordneten Ordner übernehmen** und **Von übergeordneter Gruppe übernehmen** aktiviert sind, deaktivieren Sie diese und klicken auf **Anwenden**.
10. Klicken Sie auf **OK**.

Jetzt sind Mitglieder der Rolle berechtigt, dem Ordner und allen untergeordneten Ordnern Objekte hinzuzufügen. Um zugewiesene Berechtigungen zu entfernen, wählen Sie eine Gruppe und klicken auf **Entfernen**.

9.9.5 Konfigurieren der Einzelanmeldung für SAP Crystal Reports und Oracle EBS

Die BI-Plattform ist standardmäßig so konfiguriert, dass Benutzer von SAP Crystal Reports mit der Einzelanmeldung auf Oracle-EBS-Daten zugreifen können.

9.9.5.1 Deaktivieren von SSO für Oracle EBS und SAP Crystal Reports

1. Klicken Sie in der Central Management Console (CMC) auf **Anwendungen**.
2. Doppelklicken Sie auf **Crystal-Reports-Konfiguration**.
3. Klicken Sie auf **Einzelanmeldungsoptionen**.
4. Wählen Sie **crdb_oraapps**.
5. Klicken Sie auf **Entfernen**.
6. Klicken Sie auf **Speichern und schließen**.
7. Wechseln Sie auf die Seite *Server* in der CMC, und wählen Sie **Crystal-Reports-Dienst**.
8. Klicken Sie auf die Schaltfläche **Server neu starten**.

9.9.5.2 Erneutes Aktivieren der Einzelanmeldung für Oracle EBS und SAP Crystal Reports

Führen Sie die folgenden Schritte aus, um die Einzelanmeldung für Oracle EBS und SAP Crystal Reports erneut zu aktivieren.

1. Klicken Sie in der Central Management Console (CMC) auf **Anwendungen**.
2. Doppelklicken Sie auf **Crystal-Reports-Konfiguration**.
3. Klicken Sie auf **Einzelanmeldungsoptionen**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Geben Sie unter *SSO-Kontext für Datenbankanmeldung mit folgenden Treibern verwenden* den Eintrag `crdb_oraapps` ein.
5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Speichern und schließen**.
7. Wechseln Sie auf die Seite *Server* in der CMC, und wählen Sie **Crystal-Reports-Dienst**.
8. Klicken Sie auf die Schaltfläche **Server neu starten**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10 Serververwaltung

10.1 Arbeiten mit dem Verwaltungsbereich "Server" in der CMC

Der Verwaltungsbereich "Server" der CMC ist Ihr primäres Tool für Serververwaltungsaufgaben. Das Tool bietet eine Liste aller in Ihrer Implementierung enthaltenen Server. Bei den meisten Verwaltungs- und Konfigurationsaufgaben wählen Sie einen Server aus der Liste aus und wählen anschließend einen Befehl aus dem Menü "Verwalten" oder "Aktion".

Informationen zur Navigationsstruktur

Mithilfe der Navigationsstruktur auf der linken Seite des Verwaltungsbereichs "Server" können Sie die Serverliste auf unterschiedliche Weisen anzeigen lassen. Wählen Sie Elemente in der Navigationsstruktur aus, um die im *Detail*-Bereich angezeigten Informationen zu ändern.

Option in der Navigationsstruktur	Beschreibung
Serverliste	Zeigt eine vollständige Liste aller in der Implementierung enthaltenen Server an.
Servergruppenliste	Zeigt eine unstrukturierte Liste aller verfügbaren Servergruppen im Detailbereich an. Wählen Sie diese Option, wenn Sie Servergruppeneinstellungen oder Sicherheitseinstellungen konfigurieren möchten.
Servergruppen	Listet die Servergruppen und die in den einzelnen Servergruppen enthaltenen Server auf. Wenn Sie eine Servergruppe auswählen, werden die zugehörigen Server und Servergruppen in hierarchischer Form im Detailbereich angezeigt.
Knoten	Zeigt eine Liste der in der Implementierung enthaltenen Knoten an. Knoten werden im CCM konfiguriert. Sie können einen Knoten auswählen, indem Sie auf ihn klicken, um die Server auf dem Knoten anzuzeigen oder zu verwalten.
Dienstkategorien	Stellt eine Liste der Diensttypen bereit, die in Ihrer Implementierung enthalten sein können. Die Dienstkategorien unterteilen sich in die Kerndienste der BI-Plattform und Dienste, die mit bestimmten SAP-BusinessObjects-Komponenten verknüpft sind. Die Dienstkategorien umfassen: • **Konnektivitätsdienste** • **Kerndienste** • **Crystal-Reports-Dienste** • **Datenföderations-Dienste** • **Promotion-Management-Dienste** • **Analysis Services** • **Web-Intelligence-Dienste**

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option in der Navigations-struktur	Beschreibung
	• **Dashboards-Dienste** Wählen Sie eine Dienstkategorie in der Navigationsliste aus, um die Server in der Kategorie anzuzeigen oder zu verwalten. **Hinweis** Auf einem Server können Dienste gehostet werden, die mehreren Dienstkategorien angehören. Daher kann ein Server in mehreren Dienstkategorien angezeigt werden.
Serverstatus	Zeigt die Server entsprechend ihrem aktuellen Status an. Dieses Tool ist hilfreich, wenn Sie feststellen möchten, welche Server ausgeführt werden bzw. gestoppt wurden. Wenn Sie beispielsweise einen Leistungsabfall im System bemerken, können Sie mithilfe der Liste *Serverstatus* schnell feststellen, ob sich einer Ihrer Server in einem anormalen Zustand befindet. Der Serverstatus kann wie folgt lauten: • **Gestoppt** • **Starten** • **Initialisieren** • **Wird ausgeführt** • **Wird gestoppt** • **Gestartet mit Fehlern** • **Fehlgeschlagen** • **Auf Ressourcen wird gewartet**

Informationen zum Detailbereich

Je nach den Optionen, die Sie in der Navigationsstruktur ausgewählt haben, wird im *Detail*-Bereich auf der rechten Seite des Server-Verwaltungsbereichs eine Liste der Server, Servergruppen, Statusinformationen, Kategorien oder Knoten angezeigt. In der folgenden Tabelle werden die Informationen beschrieben, die für Server im *Detail*-Bereich aufgeführt sind.

Hinweis

Für Knoten, Servergruppen, Kategorien und Statusangaben werden im *Detail*-Bereich normalerweise Namen und Beschreibungen angezeigt.

Spalte des Detailbereichs	Beschreibung
Servername oder **Name**	Zeigt den Namen des Servers an.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Spalte des Detailbereichs	Beschreibung
Status	Zeigt den aktuellen Status des Servers an. Sie können über die Liste *Serverstatus* in der Navigationsstruktur nach Serverstatusangaben sortieren. Der Serverstatus kann wie folgt lauten: • **Gestoppt** • **Starten** • **Initialisieren** • **Wird ausgeführt** • **Wird gestoppt** • **Gestartet mit Fehlern** • **Fehlgeschlagen** • **Auf Ressourcen wird gewartet**
Aktiviert	Zeigt an, ob der Server aktiviert oder deaktiviert ist.
Veraltet	Wenn der Server als **Veraltet** markiert ist, muss er neu gestartet werden. Wenn Sie bestimmte Servereinstellungen im Fenster *Eigenschaften* des Servers ändern, muss der Server u.U. neu gestartet werden, damit die Änderungen wirksam werden.
Typ	Zeigt den Servertyp an.
Hostname	Zeigt den Hostnamen für den Server an.
Serverstatus	Gibt den allgemeinen Zustand des Servers an. Der Serverstatus kann wie folgt lauten: • **Grün** (fehlerfrei) • **Gelb** (Achtung) • **Rot** (Gefahr) Der Status eines Servers hängt direkt vom Status des Serverkontrollmoduls ab. Beispielsweise ist der Status des Central Management Servers vom Status des `<KNOTENNAME>.CentralManagementServer-Kontrollmoduls` abhängig. Auf der Seite *Überwachung* in der CMC können Sie auf die Details von Kontrollmodulen zugreifen: Wählen Sie auf der Registerkarte *Kontrollmodulliste* das Kontrollmodul aus und klicken auf **Bearbeiten**. Ihnen werden die *Regel für Achtung* und die *Regel für Gefahr* für das Kontrollmodul angezeigt, die dem Status "Gelb" bzw. "Rot" entsprechen.
PID	Zeigt die eindeutige Prozess-ID-Nummer für den Server an.
Beschreibung	Zeigt eine Beschreibung des Servers an. Sie können diese Beschreibung auf der Seite *Eigenschaften* des Servers ändern.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Spalte des Detailbereichs	Beschreibung
Änderungsdatum	Zeigt das Datum an, zu dem der Server zuletzt geändert wurde bzw. zu dem sich der Serverzustand geändert hat. Diese Spalte ist sehr hilfreich, wenn Sie den Status kürzlich geänderter Server überprüfen möchten.

Weitere Informationen

Verwaltung von Servergruppen [Seite 383]
Mithilfe von Servergruppen können Sie BI-Plattform-Server auf Ihrem System organisieren und besser verwalten. Sie können einen bestimmten Server oder eine bestimmte Servergruppe pro Veröffentlichung (nicht pro Benutzer) auswählen, und Sie können Server nach Region oder Typ gruppieren.

Verwenden von Knoten [Seite 404]

Anzeigen des Status von Servern [Seite 369]

Starten, Stoppen und Neustarten von Servern [Seite 370]

Ändern der Eigenschaften eines Servers [Seite 392]

Verwalten von Verbindungen zur CMS-Systemdatenbank [Seite 437]

10.2 Verwalten von Servern mithilfe von Skripts unter Windows

Mit der ausführbaren Datei `ccm.exe` können Sie Server in einer Windows-Implementierung über die Befehlszeile starten, stoppen, neu starten, aktivieren und deaktivieren.

Weitere Informationen

ccm.exe [Seite 892]

10.3 Verwalten von Servern unter Unix

Mithilfe der ausführbaren Datei `ccm.sh` können Sie die Server über die Befehlszeile in der Unix-Implementierung starten, stoppen, neu starten, aktivieren und deaktivieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

ccm.sh [Seite 884]

10.4 Anzeigen und Ändern des Serverstatus

10.4.1 Anzeigen des Status von Servern

Der Status eines Servers entspricht dessen aktuellem Betriebszustand: ein Server kann gerade ausgeführt, gestartet oder gestoppt werden bzw. gestoppt sein, einen Fehler aufweisen oder initialisiert, mit Fehlern gestartet worden sein bzw. auf Ressourcen warten. Um auf BI-Plattform-Anforderungen reagieren zu können, muss ein Server ausgeführt werden und aktiviert sein. Ein deaktivierter Server wird weiterhin als Prozess ausgeführt, er nimmt jedoch keine Anforderungen mehr von der BI-Plattform an. Ein gestoppter Server wird nicht mehr als Prozess ausgeführt.

In diesem Abschnitt erfahren Sie, wie der Serverstatus über die CMC geändert wird.

Weitere Informationen

So lassen Sie den Status eines Servers anzeigen [Seite 369]
Anzeigen des Status von Diensten [Seite 370]
Starten, Stoppen und Neustarten von Servern [Seite 370]
Aktivieren und Deaktivieren von Servern [Seite 374]
Anhalten eines Central Management Servers [Seite 373]
Automatisches Starten von Servern [Seite 372]

10.4.1.1 So lassen Sie den Status eines Servers anzeigen

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.

   Der *Detailbereich* zeigt die Dienstkategorien in Ihrer Implementierung an.
2. Zum Anzeigen einer Serverliste in einer Servergruppe, einem Knoten oder einer Dienstkategorie klicken Sie in der Navigationsliste auf die Servergruppe, den Knoten oder die Kategorie.
   Die Liste der Server in der Implementierung wird im Bereich *Details* angezeigt. Die Spalte **Status** enthält den Status der einzelnen Server in der Liste.
3. Wenn Sie eine Liste aller Server einsehen möchten, die derzeit über einen bestimmten Status verfügen, erweitern Sie die Option **Serverstatus** in der Navigationsstruktur und wählen den gewünschten Status aus.

   Eine Liste der Server mit dem ausgewählten Status wird im Detailbereich angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Dies ist besonders hilfreich, wenn Sie schnell eine Liste der Server anzeigen lassen möchten, die nicht ordnungsgemäß gestartet bzw. unerwartet gestoppt wurden.

Weitere Informationen

Anzeigen des Status von Diensten [Seite 370]

10.4.1.2 Anzeigen des Status von Diensten

Wenn ein Dienst fehlschlägt, wird der Status des Host-Servers entweder auf *Gestartet mit Fehlern* (d.h. mindestens ein Dienst wurde erfolgreich gestartet) oder *Fehlgeschlagen* (d.h. kein Dienst wurde erfolgreich gestartet) gesetzt. Sie können die Serverstatus in der CMC und im CCM anzeigen. Auf der Seite *Eigenschaften* in der CMC können Sie jedoch auch den Status einzelner Dienste anzeigen.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.

   Der *Detailbereich* zeigt die Dienstkategorien in Ihrer Implementierung an.
2. Zum Anzeigen einer Serverliste in einer Servergruppe, einem Knoten oder einer Dienstkategorie klicken Sie in der Navigationsliste auf die Servergruppe, den Knoten oder die Kategorie.
   Die Liste der Server in der Implementierung wird im Bereich *Details* angezeigt.
3. Doppelklicken Sie auf einen Server, um die Seite *Eigenschaften* des Servers anzuzeigen.

   Die Seite *Eigenschaften* zeigt die Eigenschaften des Servers und der auf ihm gehosteten Dienste an. Für fehlgeschlagene Dienste werden auch Fehlermeldungen angezeigt.

Weitere Informationen

Anzeigen des Status von Servern [Seite 369]

10.4.2 Starten, Stoppen und Neustarten von Servern

Starten, Stoppen und Neustarten von Servern sind Aktionen, die Sie häufig durchführen, wenn Sie Server konfigurieren oder sie offline nehmen. Wenn Sie beispielsweise den Namen eines Servers ändern möchten, muss zuerst der Server gestoppt werden. Sobald Sie die Änderungen vorgenommen haben, starten Sie den Server neu, damit die Änderungen wirksam werden. Wenn Sie Änderungen an den Konfigurationseinstellungen eines Servers vornehmen, gibt die CMC eine Aufforderung aus, wenn der Server neu gestartet werden muss.

Im Verlauf dieses Abschnitts erfahren Sie, wann Sie bei einer bestimmten Konfigurationsänderung zunächst den Server anhalten oder neu starten müssen. Da diese Aufgaben jedoch regelmäßig auftreten, werden zunächst die Begriffe und Unterschiede erläutert und dann die allgemeinen Vorgehensweisen beschrieben.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Aktion	Beschreibung
Stoppen von Servern	Es kann erforderlich sein, BI-Plattform-Server zu stoppen, bevor Sie bestimmte Eigenschaften und Einstellungen ändern können.
Starten von Servern	Wenn Sie einen Server gestoppt haben, um ihn zu konfigurieren, müssen Sie ihn neu starten, damit die Änderungen wirksam werden und der Server die Verarbeitung von Anforderungen fortsetzen kann.
Neustarten von Servern	Beim Neustart wird ein Server vollständig gestoppt und anschließend wieder gestartet. Wenn ein Server neu gestartet werden muss, nachdem eine Servereinstellung geändert wurde, erhalten Sie von der CMC eine entsprechende Aufforderung.
Automatisches Starten eines Servers	Sie können festlegen, dass Server automatisch gestartet werden, sobald der Server Intelligence Agent startet.
Beendigung erzwingen	Ein Server wird unverzüglich gestoppt. (Wenn Sie einen Server stoppen, wird er hingegen erst gestoppt, nachdem alle aktuellen Verarbeitungsaktivitäten abgeschlossen wurden.) Erzwingen Sie die Beendigung eines Servers nur dann, wenn das Stoppen des Servers fehlgeschlagen ist und der Server sofort gestoppt werden muss.

➔ Tipp

Wenn Sie einen Server stoppen (oder neu starten), wird der Serverprozess beendet. Dadurch wird der Server vollständig angehalten. Vor dem Stoppen eines Servers sollten Sie

- den Server deaktivieren, damit dieser die Verarbeitung von laufenden Aufträgen abschließen kann und
- sicherstellen, dass keine Überwachungsereignisse mehr in der Warteschlange stehen. Wechseln Sie zum Anzeigen der Anzahl der Überwachungsereignisse in der Warteschlange zum Bildschirm *Metriken* des Servers, und zeigen Sie die Metrik *Aktuelle Anzahl der Überwachungsereignisse in der Warteschlange* an.

Weitere Informationen

Aktivieren und Deaktivieren von Servern [Seite 374]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10.4.2.1 Starten, Stoppen oder Neustarten von Servern über die CMC

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.

   Der *Detailbereich* zeigt die Dienstkategorien in Ihrer Implementierung an.
2. Um eine Liste der Server für eine bestimmte Servergruppe, einen bestimmten Knoten oder eine bestimmte Dienstkategorie anzuzeigen, wählen Sie die Gruppe, den Knoten oder die Kategorie im Navigationsbereich aus.
   Im *Detailbereich* wird eine Liste der Server angezeigt.
3. Wenn Sie eine Liste aller Server einsehen möchten, die derzeit über einen bestimmten Status verfügen, erweitern Sie die Option **Serverstatus** in der Navigationsstruktur und wählen den gewünschten Status aus.

   Eine Liste der Server mit dem ausgewählten Status wird im *Detailbereich* angezeigt.

   > **Hinweis**
   >
   > Dies ist besonders hilfreich, wenn Sie schnell eine Liste der Server anzeigen lassen möchten, die nicht ordnungsgemäß gestartet bzw. unerwartet gestoppt wurden.
4. Klicken Sie mit der rechten Maustaste auf den Server, dessen Status Sie ändern möchten, und wählen Sie anschließend **Server starten**, **Server neu starten**, **Server stoppen** oder **Beendigung erzwingen**.

Weitere Informationen

Anzeigen des Status von Servern [Seite 369]

10.4.2.2 So starten oder halten Sie einen Windows-Server mit dem CCM an oder führen einen Neustart durch

1. Klicken Sie im CCM in der Symbolleiste auf die Schaltfläche **Server verwalten**.
2. Melden Sie sich bei Eingabeaufforderung mit einem Administratorkonto am CMS an.
3. Wählen Sie im Dialogfeld *Server verwalten* den Server aus, den Sie starten, stoppen oder neu starten möchten.
4. Klicken Sie auf **Starten**, **Stoppen**, **Neu starten** oder **Beendigung erzwingen**.
5. Klicken Sie auf **Schließen**, um zum CCM zurückzukehren.

10.4.2.3 Automatisches Starten von Servern

In Ihrer Implementierung enthaltene Server werden standardmäßig automatisch gestartet, wenn der Server Intelligence Agent startet. In dieser Aufgabe wird dargestellt, wo die Option für das automatische Starten eingerichtet wird.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den Server, der automatisch gestartet werden soll.
   Der Bildschirm *Eigenschaften* wird angezeigt.
3. Aktivieren Sie unter *Allgemeine Einstellungen* das Kontrollkästchen **Diesen Server beim Start des Server Intelligence Agents automatisch starten**, und klicken Sie auf **Speichern** oder **Speichern & schließen**.

   Hinweis

   Wenn das Kontrollkästchen **Diesen Server beim Start des Server Intelligence Agents automatisch starten** für jeden CMS im Cluster deaktiviert ist, müssen Sie das System über den CCM neu starten. Nachdem Sie den SIA mit dem CCM gestoppt haben, klicken Sie mit der rechten Maustaste auf den SIA und wählen **Eigenschaften** aus. Klicken Sie auf der Registerkarte **Start** auf **Eigenschaften**, um die Seite "Servereigenschaften" für den CMS zu öffnen. Wählen Sie **Automatisch Starten**, klicken Sie dann auf **OK**, um die Seite "Servereigenschaften" zu schließen, und klicken Sie dann erneut auf **OK**. Starten Sie den SIA neu. Die Option **Autostart** steht nur zur Verfügung, wenn das Kontrollkästchen **Diesen Server beim Start des Server Intelligence Agents automatisch starten** für jeden CMS im Cluster deaktiviert ist.

10.4.3 Anhalten eines Central Management Servers

Wenn die BI-Plattform-Installation über mehr als einen aktiven Central Management Server (CMS) verfügt, können Sie einen einzelnen CMS herunterfahren, ohne dass Datenverluste auftreten oder die Systemfunktionalität beeinträchtigt wird. Die Arbeitslast des gestoppten Servers wird von einem anderen CMS auf dem Knoten übernommen. Durch das Clustern mehrerer CMS können Sie Verwaltungsaufgaben auf den einzelnen Central Management Servern nacheinander ausführen, ohne die BI-Plattform außer Betrieb zu setzen.

Wenn die BI-Plattform-Implementierung jedoch nur einen CMS umfasst, ist die Plattform nach dem Herunterfahren dieses Servers für die Benutzer nicht mehr verfügbar, und die Verarbeitung von Berichten und Programmen wird unterbrochen. Um dieses Problem zu vermeiden, stellt der Server Intelligence Agent für jeden Knoten sicher, dass stets mindestens ein CMS ausgeführt wird. Sie können einen CMS weiterhin stoppen, indem Sie den zugehörigen SIA stoppen. Vor dem Stoppen des SIA sollten Sie jedoch die Verarbeitungsserver über die CMC deaktivieren, damit alle Aufträge, die sich in Verarbeitung befinden, vor dem Herunterfahren der BI-Plattform abgeschlossen werden können, da alle anderen Server auf dem Knoten ebenfalls heruntergefahren werden.

Hinweis

Es kann vorkommen, dass der CMS gestoppt wurde und Sie das System über den CCM neu starten möchten. Wenn Sie beispielsweise jeden CMS auf einem Knoten herunterfahren und das Kontrollkästchen **Diesen Server beim Start des Server Intelligence Agents automatisch starten** beim Start des SIA für jeden CMS im Cluster deaktiviert ist, müssen Sie das System über den CCM neu starten. Klicken Sie im CCM mit der rechten Maustaste auf den SIA, und wählen Sie **Eigenschaften** aus. Klicken Sie auf der Registerkarte **Start** auf **Eigenschaften**, um die Seite "Servereigenschaften" für den CMS zu öffnen. Wählen Sie **Automatisch Starten**, klicken Sie dann auf **OK**, um die Seite "Servereigenschaften" zu schließen, und klicken Sie dann erneut auf **OK**. Starten Sie den SIA neu. Die Option **Autostart** steht nur zur Verfügung, wenn das Kontrollkästchen **Diesen Server beim Start des Server Intelligence Agents automatisch starten** für jeden CMS im Cluster deaktiviert ist.

Wenn Sie Ihr System so konfigurieren möchten, dass der Central Management Server im Cluster gestartet und gestoppt werden kann, ohne andere Server starten und stoppen zu müssen, setzen Sie den CMS auf einen

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

anderen Knoten. Erstellen Sie einen neuen Knoten, und klonen Sie den CMS auf dem Knoten. Wenn sich der CMS auf einem eigenen Knoten befindet, können Sie den Knoten problemlos herunterfahren, ohne dass andere Server davon betroffen sind.

Weitere Informationen

Verwenden von Knoten [Seite 404]
Klonen von Servern [Seite 376]
Clustern von Central Management Servern [Seite 378]

10.4.4 Aktivieren und Deaktivieren von Servern

Wenn Sie einen BI-Plattformserver deaktivieren, verhindern Sie, dass er neue Anforderungen erhält und auf diese reagiert. Der eigentliche Serverprozess wird jedoch nicht gestoppt. Diese Funktion ist besonders nützlich, wenn ein Server vor einem vollständigen Stopp alle aktuellen Anforderungen verarbeiten soll.

Angenommen, Sie möchten einen Job Server stoppen, bevor der Rechner, auf dem er ausgeführt wird, neu gestartet wird. Der Server soll jedoch alle ausstehenden Berichtsanforderungen verarbeiten, die sich in seiner Warteschlange befinden. Deaktivieren Sie zunächst den Job Server, damit dieser keine weiteren Anforderungen mehr übernimmt. Wechseln Sie dann zur Central Management Console, um den Zeitpunkt zu überwachen, zu dem der Server die in Bearbeitung befindlichen Aufträge abschließt. (Klicken Sie im *Server*-Verwaltungsbereich mit der rechten Maustaste auf den Server, und wählen Sie *Metriken*.) Sobald alle aktuellen Anforderungen verarbeitet sind, können Sie den Server sicher stoppen.

> **Hinweis**
>
> Der CMS muss ausgeführt werden, damit Sie andere Server aktivieren bzw. deaktivieren können.

> **Hinweis**
>
> Ein CMS kann nicht aktiviert bzw. deaktiviert werden.

10.4.4.1 Aktivieren und deaktivieren von Servern über die CMC

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Klicken Sie mit der rechten Maustaste auf den Server, dessen Status Sie ändern möchten, und anschließend auf **Server aktivieren** bzw. **Server deaktivieren**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10.4.4.2 So aktivieren oder deaktivieren Sie einen Windows-Server mit dem CCM

1. Klicken Sie im CCM auf **Server verwalten**.
2. Wenn Sie dazu aufgefordert werden, melden Sie sich beim CMS mit den Anmeldedaten an, die Ihnen Administratorrechte für die BI-Plattform gewähren.
3. Wählen Sie im Dialogfeld *Server verwalten* den Server aus, den Sie aktivieren oder deaktivieren möchten.
4. Klicken Sie auf **Aktivieren** oder **Deaktivieren**.
5. Klicken Sie auf **Schließen**, um zum CCM zurückzukehren.

10.5 Hinzufügen, Klonen oder Löschen von Servern

10.5.1 Hinzufügen, Klonen und Löschen von Servern

Wenn Sie der BI-Plattform durch Installation von Serverkomponenten auf zusätzlichen Rechnern neue Hardware hinzufügen möchten, sollten Sie das im Lieferumfang des Produkts enthaltene BI-Plattform-Installationsprogramm auf diesen Rechnern ausführen. Das Setup-Programm ermöglicht Ihnen die Durchführung einer benutzerdefinierten Installation. Während der benutzerdefinierten Installation geben Sie den CMS Ihrer bereits vorhandenen Implementierung an und wählen die Komponenten aus, die Sie auf dem lokalen Rechner installieren möchten. Ausführliche Informationen zu den Optionen für die benutzerdefinierte Installation finden Sie im *Installationshandbuch für SAP BusinessObjects Business Intelligence*.

10.5.1.1 Hinzufügen von Servern

Sie können mehrere Instanzen desselben BI-Plattform-Servers auf demselben Rechner ausführen. So fügen Sie einen Server hinzu:

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Klicken Sie im Menü **Verwalten** auf **Neu** > **Neuer Server**.
   Das Dialogfeld *Neuen Server erstellen* wird angezeigt.
3. Wählen Sie **Dienstkategorie** aus.
4. Wählen Sie den benötigten Diensttyp aus der Liste **Dienst auswählen** aus, und klicken Sie dann auf **Weiter**.
5. Um dem Server einen weiteren Dienst hinzuzufügen, wählen Sie den Dienst in der Liste **Verfügbare zusätzliche Dienste** aus und klicken auf **>**.

   > **Hinweis**
   >
   > Zusätzliche Dienste sind nicht für alle Servertypen verfügbar.

6. Nachdem Sie die zusätzlichen Dienste hinzugefügt haben, klicken Sie auf **Weiter**.
7. Wenn sich Ihre BI-Plattform-Architektur aus mehreren Knoten zusammensetzt, wählen Sie den Knoten, dem der neue Server hinzugefügt werden soll, aus der Liste **Knoten** aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8. Geben Sie im Feld **Servername** einen Namen für den Server ein.

   Jeder Server im System muss einen eindeutigen Namen haben. Die Benennungskonvention lautet standardmäßig `<KNOTENNAME>.<Servertyp>`. (Eine Ziffer dahinter zeigt an, dass mehrere Server desselben Typs auf dem Host-Rechner vorhanden sind.)
9. Um eine Beschreibung für den Server einzufügen, geben Sie sie in das Feld **Beschreibung** ein.
10. Wenn Sie einen neuen Central Management Server hinzufügen, geben Sie eine Portnummer im Feld **Name Server-Port** ein.
11. Klicken Sie auf **Erstellen**.
    Der neue Server wird in der Serverliste im Bereich **Server** der CMC aufgeführt, er wird jedoch weder gestartet noch aktiviert.
12. Verwenden Sie die CMC, um den neuen Server zu starten und anschließend zu aktivieren, wenn er auf BI-Plattform-Anforderungen antworten soll.

Weitere Informationen

Server, Dienste, Knoten und Hosts [Seite 25]
Konfigurieren von Servereinstellungen [Seite 391]
Konfigurieren von Portnummern [Seite 401]
Anzeigen des Status von Servern [Seite 369]

10.5.1.2 Klonen von Servern

Wenn Sie eine neue Serverinstanz zu Ihrer Implementierung hinzufügen möchten, können Sie einen vorhandenen Server klonen. Der geklonte Server behält die Konfigurationseinstellungen des ursprünglichen Servers bei. Dies kann besonders hilfreich sein, wenn Sie Ihre Implementierung erweitern und neue Serverinstanzen erstellen möchten, die nahezu dieselben Serverkonfigurationseinstellungen wie ein vorhandener Server verwenden.

Außerdem vereinfacht das Klonen auch das Verschieben von Servern zwischen Knoten. Um einen vorhandenen CMS auf einen anderen Knoten zu verschieben, können Sie ihn auf dem neuen Knoten klonen. Der geklonte CMS wird auf dem neuen Knoten angezeigt und behält alle Konfigurationseinstellungen des ursprünglichen CMS bei.

Einige Dinge sollten beim Klonen von Servern berücksichtigt werden. Möglicherweise möchten Sie nicht alle Einstellungen klonen. Aus diesem Grund empfiehlt es sich, den geklonten Server zu überprüfen, um sicherzustellen, dass er Ihren Anforderungen entspricht. Wenn Sie beispielsweise einen CMS auf demselben Rechner klonen, achten Sie darauf, die Einstellungen für die Portnummer zu ändern, die vom ursprünglichen CMS auf den geklonten CMS kopiert wurden.

> **Hinweis**
>
> Vor dem Klonen von Servern sollten Sie sicherstellen, dass alle Rechner in Ihrer Implementierung über identische BI-Plattform-Versionen (und gegebenenfalls Aktualisierungen) verfügen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Sie können Server von einem beliebigen Rechner klonen. Sie können Server jedoch nur auf Rechnern klonen, auf denen die erforderlichen Binärdateien für den Server installiert sind.

> **Hinweis**
>
> Wenn Sie einen Server klonen, bedeutet dies nicht unbedingt, dass der neue Server dieselben Betriebssystem-Anmeldedaten verwendet. Das Benutzerkonto wird vom Server Intelligence Agent gesteuert, unter dem der Server ausgeführt wird.

10.5.1.2.1 Verwenden von Platzhaltern für Servereinstellungen

Platzhalter sind Variablen auf Knotenebene, die von auf dem Knoten ausgeführten Servern verwendet werden. Platzhalter werden auf einer speziellen Seite in der Central Management Console (CMC) aufgeführt. Wenn Sie in der CMC auf einen der unter *Server* aufgelisteten Server doppelklicken, wird im Navigationsbereich auf der linken Seite eine Verknüpfung für "Platzhalter" angezeigt. Auf der Seite *Platzhalter* sind alle verfügbaren Platzhalternamen und die zugehörigen Werte für den ausgewählten Server aufgeführt. Platzhalter enthalten schreibgeschützte Werte, und ihre Namen beginnen und enden mit dem Prozentzeichen `%`.

> **Hinweis**
>
> Eine Platzhaltereinstellung kann auf der CMC-Seite *Eigenschaften* eines Servers immer mit einer spezifischen Zeichenfolge überschrieben werden.

> **Beispiel**
>
> Platzhalter sind beim Klonen von Servern hilfreich. Beispielsweise ist die BI-Plattform auf Rechner A mit mehreren Laufwerken im Verzeichnis `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0` installiert. Daher ist der Platzhalter `%DefaultAuditingDir%` `D:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`.
>
> Ein anderer Rechner (Rechner B) verfügt lediglich über ein Festplattenlaufwerk (also kein Laufwerk D), und die BI-Plattform ist unter `C:\Programme\ SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0` installiert. In diesem Fall ist der Platzhalter `%DefaultAuditingDir%` `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`.
>
> Wenn Sie den Event Server von Rechner A auf Rechner B klonen möchten und für das temporäre Verzeichnis zur Überwachung Platzhalter verwendet werden, werden die Platzhalter automatisch aufgelöst und der Event Server ordnungsgemäß ausgeführt. Falls keine Platzhalter verwendet werden, verursacht der Event Server einen Fehler, sofern Sie die Einstellung "Temporäres Verzeichnis für die Überwachung" nicht manuell überschreiben.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10.5.1.2.2 So klonen Sie einen Server

1. Wechseln Sie auf dem Rechner, zu dem Sie den geklonten Server hinzufügen möchten, in den *Server*-Verwaltungsbereich des CMC.
2. Klicken Sie mit der rechten Maustaste auf den zu klonenden Server und wählen **Server klonen**.
   Das Dialogfeld *Server klonen* wird angezeigt.
3. Geben Sie den Namen für den Server in das Feld **Neuer Servername** ein (oder verwenden Sie den Standardnamen).
4. Wenn Sie einen Central Management Server klonen, geben Sie eine Portnummer im Feld **Name Server-Port** ein.
5. Wählen Sie in der Liste **Für Knoten klonen** den Knoten aus, an dem der geklonte Server hinzugefügt werden soll, und klicken Sie dann auf **OK**.
   Der neue Server wird im *Server*-Verwaltungsbereich des CMC angezeigt.

> **Hinweis**
>
> Portnummerneinstellungen werden auch geklont. In vielen Fällen, z.B. beim Klonen eines CMS, empfiehlt es sich, die Portnummer zu ändern, um Portkonflikte zwischen dem ursprünglichen Server und dessen Klon zu vermeiden.

10.5.1.3 Löschen von Servern

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Stoppen Sie den Server, den Sie löschen möchten.
3. Klicken Sie mit der rechten Maustaste auf den Server, und wählen Sie **Löschen**.
4. Wenn Sie zum Bestätigen aufgefordert werden, klicken Sie auf **OK**.

10.6 Clustern von Central Management Servern

10.6.1 Clustern von Central Management Servern

Bei einer großen oder unternehmenskritischen Implementierung von SAP BusinessObjects Business Intelligence sollten Sie mehrere CMS-Rechner zu einem Cluster zusammenschließen. Ein Cluster besteht aus mindestens zwei CMS-Servern, die gemeinsam eine allgemeine CMS-Systemdatenbank verwenden. Wenn ein Rechner ausfällt, auf dem ein CMS ausgeführt wird, übernimmt ein anderer CMS-Rechner dessen Aufgabe, BI-Plattform-Anforderungen zu verarbeiten. Die Unterstützung der "Hochverfügbarkeit" stellt sicher, dass BI-Plattform-Benutzer weiterhin auf Informationen zugreifen können, wenn ein Teil des Systems ausfällt.

In diesem Abschnitt wird erläutert, wie einem bereits in Betrieb befindlichen Produktionssystem ein neues CMS-Clustermitglied hinzugefügt wird. Wenn Sie einem bestehenden Cluster einen neuen CMS hinzufügen, weisen Sie den neuen CMS an, eine Verbindung mit der bestehenden CMS-Systemdatenbank herzustellen und einen Teil der

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Verarbeitungslast von den bestehenden CMS-Rechnern zu übernehmen. Informationen zu Ihrem aktuellen CMS erhalten Sie im Verwaltungsbereich "*Server*" der CMC.

Vor dem CMS-Clustering müssen Sie sicherstellen, dass die einzelnen CMS auf einem System installiert sind, das die genauen Anforderungen (auch für die Versionsebene und die Patchebene) für Betriebssystem, Datenbankserver, Datenbankzugriffsmethode, Datenbanktreiber und Datenbank-Client erfüllt, wie in der Produkt Availability Matrix beschrieben.

Außerdem müssen die folgenden Clusteranforderungen erfüllt sein:

- Optimale Leistungen erzielen Sie, wenn der Datenbankserver, der als Host für die Systemdatenbank verwendet wird, kleine Querys in sehr kurzer Zeit verarbeiten kann. Der CMS kommuniziert häufig mit der Systemdatenbank und sendet viele kleine Abfragen an die Datenbank. Wenn der Datenbankserver die Anforderungen nicht rechtzeitig verarbeiten kann, wird die Leistung der BI-Plattform stark beeinträchtigt.
- Beste Leistungen erzielen Sie, wenn Sie jedes Mitglied des CMS-Clusters auf Rechnern mit gleich viel Hauptspeicher und dem gleichen CPU-Typ ausführen.
- Verwenden Sie für jeden Rechner dieselbe Konfiguration:
  - Installieren Sie das gleiche Betriebssystem und die gleiche Version der Service Packs und Patches für das Betriebssystem.
  - Installieren Sie dieselbe Version der BI-Plattform (einschließlich Patches, sofern zutreffend).
  - Stellen Sie sicher, dass jeder CMS auf dieselbe Art und Weise eine Verbindung mit der CMS-Systemdatenbank herstellt: über systemeigene oder ODBC-Treiber. Vergewissern Sie sich, dass die Treiber auf den einzelnen Rechnern identisch sind und einer unterstützten Version entsprechen.
  - Stellen Sie sicher, dass die einzelnen CMS für das Herstellen einer Verbindung mit der Systemdatenbank den gleichen Datenbank-Client verwenden und die entsprechende Version unterstützt wird.
  - Stellen Sie sicher, dass jeder CMS dasselbe Datenbankbenutzerkonto und -kennwort für die Verbindung mit der CMS-Systemdatenbank verwendet. Für das Konto sind Berechtigungen zum Erstellen, Löschen und Aktualisieren der Systemdatenbank erforderlich.
  - Stellen Sie sicher, dass die Knoten, auf denen sich die einzelnen CMS befinden, unter demselben Betriebssystemkonto ausgeführt werden. (Bei Windows ist dies standardmäßig das Konto "LocalSystem".)
  - Überprüfen Sie, ob das aktuelle Datum und die aktuelle Uhrzeit auf den einzelnen CMS-Rechnern korrekt eingestellt sind (auch die Einstellungen für die Sommerzeit).
  - Stellen Sie sicher, dass alle Rechner in einem Cluster (einschließlich der Rechner, auf denen der CMS gehostet wird) auf dieselbe Systemzeit gesetzt werden. Um optimale Ergebnisse zu erzielen, sollten die Rechner auf einem Zeitserver (wie `time.nist.gov`) synchronisiert oder eine zentrale Überwachungslösung verwendet werden.
  - Stellen Sie sicher, dass auf sämtlichen Webanwendungsservern im Cluster dieselben WAR-Dateien installiert sind. Weitere Informationen zur Implementierung von WAR-Dateien finden Sie im *Installationshandbuch für SAP BusinessObjects Business Intelligence*.
- Stellen Sie sicher, dass sich alle CMS des Clusters im gleichen LAN (Local Area Network) befinden.
- Out-of-Band-Threads (-oobthreads) werden von Cluster-Pings und Cluster-Benachrichtigungen verwendet. Da beide Vorgänge schnell sind (Benachrichtigungen sind asynchron), benötigt die BI-Plattform nicht mehr mehrere "oobthreads" und nur ein "-oobthread" wird erstellt.

  Wenn dem Cluster mehr als acht CMS-Clustermitglieder angehören, stellen Sie sicher, dass die Befehlszeile für die einzelnen CMS die Option `-oobthreads` **`<AnzCMS>`** enthält, wobei **`<AnzCMS>`** der Anzahl der CMS-Server im Cluster entspricht. Diese Option stellt sicher, dass der Cluster hohe Auslastungen bewältigen kann. Informationen zum Konfigurieren von Serverbefehlszeilen finden Sie im Anhang "Serverbefehlszeilen" im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Wenn die Überwachung aktiviert werden soll, müssen die einzelnen CMS so konfiguriert werden, dass die gleiche Überwachungsdatenbank verwendet und die Verbindung mit dieser Datenbank auf die gleiche Art und Weise hergestellt wird. Die Anforderungen an die Überwachungsdatenbank sind mit denen für die Systemdatenbank im Hinblick auf Datenbankserver, Clients, Zugriffsmethoden, Treiber und Benutzer-IDs identisch.

Tipp

Ein Clustername spiegelt standardmäßig den Rechner-Hostnamen des zuerst installierten CMS wider.

Weitere Informationen

Umbenennen von CMS-Clustern [Seite 382]

10.6.1.1 Hinzufügen eines CMS zu einem Cluster

Es gibt mehrere Möglichkeiten, um ein neues CMS-Clustermitglied hinzuzufügen. Führen Sie das entsprechende Verfahren aus:

- Sie können einen neuen Knoten mit einem CMS auf einem neuen Rechner installieren.
- Wenn Sie bereits über einen Knoten mit CMS-Binärdateien verfügen, können Sie über die CMC einen neuen CMS-Server hinzufügen.
- Wenn Sie bereits über einen Knoten mit CMS-Binärdateien verfügen, können Sie auch einen neuen CMS-Server durch Klonen eines vorhandenen CMS-Servers hinzufügen.

Hinweis

Sichern Sie die aktuelle CMS-Systemdatenbank, die Serverkonfiguration sowie den Inhalt der Input und Output File Repositorys, bevor Sie Änderungen vornehmen. Wenden Sie sich gegebenenfalls an den Datenbankadministrator.

Weitere Informationen

Hinzufügen eines neuen Knotens zu einem Cluster [Seite 381]
Hinzufügen von Servern [Seite 375]
Klonen von Servern [Seite 376]
Übersicht über Sicherung und Wiederherstellung [Seite 487]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10.6.1.2 Hinzufügen eines neuen Knotens zu einem Cluster

Wenn Sie einen Knoten hinzufügen (ein Knoten ist eine Sammlung von BI-Plattform-Servern, die von einem einzigen Server Intelligence Agent verwaltet werden), werden Sie aufgefordert, entweder einen neuen CMS zu erstellen, oder den Knoten auf einem vorhandenen CMS zu clustern.

Falls Sie einen Knoten mit einem vorhandenen CMS clustern möchten, können Sie auch das bei der Installation verwendete Setup-Programm nutzen. Führen Sie das Installations- und Setup-Programm der BI-Plattform auf dem Rechner aus, auf dem das neue CMS-Clustermitglied installiert werden soll. Das Setup-Programm ermöglicht Ihnen die Durchführung einer benutzerdefinierten Installation. Während der benutzerdefinierten Installation geben Sie den bereits vorhandenen CMS an, dessen System Sie erweitern möchten und wählen die Komponenten aus, die Sie auf dem lokalen Rechner installieren möchten. Geben Sie in diesem Fall den Namen des CMS an, der auf dem vorhandenen System ausgeführt wird, wählen Sie die Option für die Installation eines neuen CMS auf dem lokalen Rechner, und stellen Sie dem Setup-Programm die Informationen bereit, die es benötigt, um eine Verbindung mit der vorhandenen CMS-Systemdatenbank herzustellen. Wenn das Setup-Programm den neuen CMS auf dem lokalen Rechner installiert, wird der Server automatisch dem vorhandenen Cluster hinzugefügt.

> **Hinweis**
>
> Bevor Sie einen neuen Knoten auf einem vorhandenen CMS clustern, und es sich bei dem neuen Knoten um einen ganz neuen Server handelt, stellen Sie sicher, dass die BI-Plattform-Installation auf diesem Server dieselbe Patch-Ebene aufweist, wie die bestehende BI-Plattform-Umgebung.

Weitere Informationen

Verwenden von Knoten [Seite 404]

10.6.1.3 Hinzufügen von Clustern zu den Eigenschaftendateien der Webanwendung

Wenn Sie mehrere CMS zu Ihrer Implementierung hinzugefügt haben und einem Java-Anwendungsserver verwenden, müssen Sie die Datei `PlatformServices.properties` im Verzeichnis `\webapps\BOE\WEB-INF\config\custom` der Webanwendungsimplementierung ändern.

10.6.1.3.1 Definieren von Clustereigenschaften für die BOE-Webanwendung

1. Greifen Sie auf den Ordner "custom" für die Datei `BOE.war` auf dem Rechner zu, auf dem die Webanwendungen gehostet werden:

   `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Sie müssen die geänderte Datei `BOE.war` später erneut implementieren.

2. Erstellen Sie eine neue Datei mit einem Texteditor.
3. Geben Sie die CMS-Clustereigenschaften an.

   Über die Eigenschaft `cms.clusters` können Sie alle Cluster in der Implementierung angeben. Stellen Sie allen Clusternamen das Zeichen `@` voran, und trennen Sie sie durch ein Komma. Beispiel: `cms.clusters=@samplecluster,@samplecluster2,@samplecluster3`. Verwenden Sie die Eigenschaft `cms.clusters.<[Clustername]>`, um jeden im Cluster enthaltenen CMS anzugeben. Beispiel:

```
cms.clusters=@samplecluster,@samplecluster2, @samplecluster3
cms.clusters.samplecluster=cmsone:6400,cmstwo
cms.clusters.samplecluster2=cms3,cms4, cms5
cms.clusters.samplecluster3=aps05
```

   Hinweis

   Die Portnummer wird vom CMS-Namen durch einen Doppelpunkt abgetrennt. Als Portnummer wird 6400 vorausgesetzt, sofern nicht anders angegeben.

4. Speichern Sie die Datei unter folgendem Namen:

   `PlatformServices.properties`
5. Starten Sie Ihren Anwendungsserver neu.

Die neuen Eigenschaften werden erst wirksam, wenn die geänderte `BOE`-Webanwendung auf dem Rechner, auf dem der Webanwendungsserver ausgeführt wird, erneut implementiert wird. Verwenden Sie zur erneuten Implementierung der WAR-Datei auf dem Webanwendungsserver WDeploy. Weitere Informationen zum Umgang mit WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.

10.6.1.4 Umbenennen von CMS-Clustern

Mit diesem Verfahren können Sie den Namen eines bereits installierten Clusters ändern. Nachdem der Name des CMS-Clusters geändert wurde, konfiguriert der Server Intelligence Agent die einzelnen SAP-BusinessObjects-Server automatisch neu, sodass die Registrierung im CMS-Cluster und nicht auf einem einzelnen CMS erfolgt.

Hinweis

Erfahrene BI-Plattform-Administratoren sollten beachten, dass die Option `-ns` nicht mehr in der Serverbefehlszeile verwendet werden kann, um festzulegen, bei welchem CMS ein Server registriert werden soll. Die Registrierung wird nun automatisch vom SIA vorgenommen.

10.6.1.4.1 Ändern des Clusternamens unter Windows

1. Verwenden Sie den CCM zum Stoppen des Server Intelligence Agents für den Knoten, der einen Central Management Server enthält, der wiederum ein Mitglied des Clusters ist, dessen Namen Sie ändern möchten.
2. Klicken Sie mit der rechten Maustaste auf den Server Intelligence Agent, und wählen Sie **Eigenschaften**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Klicken Sie im Dialogfeld "Eigenschaften" auf die Registerkarte **Konfiguration**.
4. Aktivieren Sie das Kontrollkästchen **Clusternamen ändern zu**.
5. Geben Sie den neuen Namen für das Cluster ein.
6. Klicken Sie auf **OK**, und starten Sie den Server Intelligence Agent neu.

   Der Name des CMS-Clusters ist jetzt geändert. Alle anderen CMS-Clustermitglieder werden dynamisch über den neuen Clusternamen benachrichtigt (wenngleich es mehrere Minuten dauern kann, bis Ihre Änderungen an alle Clustermitglieder weitergeleitet wurden).
7. Wechseln Sie zum Verwaltungsbereich **Server** der CMC, und stellen Sie sicher, dass alle Server weiterhin aktiviert sind. Aktivieren Sie gegebenenfalls die Server, die durch Ihre Änderungen deaktiviert wurden.

10.6.1.4.2 Ändern des Clusternamens unter UNIX

Verwenden Sie das Skript `cmsdbsetup.sh`. Weitere Informationen finden Sie im Abschnitt “Unix-Skripte” im Kapitel Befehlszeilenverwaltung des *Administratorhandbuchs für SAP BusinessObjects Business Intelligence*.

Weitere Informationen

Unix-Skripte [Seite 884]

10.7 Verwaltung von Servergruppen

Mithilfe von Servergruppen können Sie BI-Plattform-Server auf Ihrem System organisieren und besser verwalten. Sie können einen bestimmten Server oder eine bestimmte Servergruppe pro Veröffentlichung (nicht pro Benutzer) auswählen, und Sie können Server nach Region oder Typ gruppieren.

Sie können Server nach Region gruppieren, um Standardverarbeitungseinstellungen, regelmäßige Zeitpläne und Zieloptionen für die zeitgesteuerte Verarbeitung für Benutzer an einem bestimmten regionalen Standort einzurichten. Sie können ein Berichtsobjekt (z. B. einen Crystal-Reports-Bericht oder ein Web-Intelligence-Dokument) mit einer einzelnen Servergruppe verknüpfen, sodass das Objekt immer von denselben Servern verarbeitet wird, und Sie können zeitgesteuert verarbeitete Berichtsobjekte mit einer bestimmten Servergruppe verknüpfen, um sicherzustellen, dass die zeitgesteuert verarbeiteten Objekte an die richtigen Drucker, Dateiserver usw. gesendet werden. Besonders bei der Verwaltung von Systemen, die über mehrere Standorte und Zeitzonen verteilt sind, erweisen sich Servergruppen als praktisch.

Besonders bei der Verwaltung von Systemen, die über mehrere Standorte und Zeitzonen verteilt sind, erweisen sich Servergruppen als praktisch. Verwenden Sie z. B. Servergruppen, um Ihr BI-Plattform-System für Berichte anzupassen, die an verschiedenen Standorten angezeigt werden, und für verschiedene Berichtstypen. Bei der Organisation von Servern nach Region können Sie die folgenden Aktionen für Servergruppen durchführen:

- Standardverarbeitungseinstellungen konfigurieren
- Regelmäßige Zeitpläne konfigurieren

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Zieloptionen für die zeitgesteuerte Verarbeitung für die Benutzer eines bestimmten regionalen Standorts konfigurieren
- Ein Berichtsobjekt (z. B. ein Crystal-Reports-Bericht oder ein Web-Intelligence-Dokument) mit einer einzelnen Servergruppe verknüpfen, damit das Objekt immer vom selben Server verarbeitet wird
- Zeitgesteuert verarbeitete Berichtsobjekte mit einer bestimmten Servergruppe verknüpfen, um sicherzustellen, dass diese an die richtigen Drucker, Dateiserver usw. gesendet werden

Gruppieren Sie Server nach Typ, wenn Sie für bestimmte Objekte festlegen möchten, dass diese Objekte von speziell optimierten Servern verarbeitet werden.

Nachdem Sie Servergruppen erstellt haben, konfigurieren Sie Objekte für die Verwendung bestimmter Servergruppen zur zeitgesteuerten Verarbeitung oder zum Anzeigen und Ändern von Berichten. Verwenden Sie die Navigationsstruktur im Verwaltungsbereich *Server* der CMC, um Servergruppen anzuzeigen. Mit der Option **Servergruppenliste** wird eine Liste der Servergruppen im **Detailbereich** angezeigt, und mit der Option **Servergruppen** können Sie die Server in der Gruppe anzeigen.

Beispiel

Verarbeitungsserver nach Typ gruppieren

Verarbeitungsserver müssen häufig mit der Datenbank kommunizieren, die die Daten für veröffentlichte Berichte enthält. Durch Platzieren der Verarbeitungsserver in der Nähe der von ihnen benötigten Datenbankserver wird die Systemleistung gesteigert und der Netzwerkverkehr verringert. Wenn Sie mehrere Berichte über eine DB2-Datenbank ausgeführt haben, können Sie eine Gruppe von Verarbeitungsservern erstellen, die Berichte nur über den DB2-Datenbankserver verarbeiten. Um die Systemleistung bei der Anzeige von Berichten zu verbessern, können Sie die Berichte so konfigurieren, dass immer diese Verarbeitungsserver-Gruppe für die Anzeige verwendet wird.

10.7.1 Erstellen von Servergruppen

Um eine Servergruppe zu erstellen, müssen Sie den Namen und das Ziel der Gruppe angeben und anschließend Server zur Gruppe hinzufügen.

10.7.1.1 Erstellen von Servergruppen

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Wählen Sie **Verwalten** > **Neu** > **Servergruppe erstellen**.

   Das Dialogfeld *Servergruppe erstellen* wird angezeigt.
3. Geben Sie im Feld **Name** einen Namen für die neue Servergruppe ein.
4. Zusätzliche Informationen zu den Servergruppen können Sie in das Feld **Beschreibung** eingeben.
5. Klicken Sie auf **OK**.
6. Klicken Sie im Verwaltungsbereich *Server* in der Navigationsstruktur auf **Servergruppen**, und wählen Sie die neue Servergruppe aus.
7. Wählen Sie im Menü **Aktionen** die Option **Elemente hinzufügen**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8. Wählen Sie die Server, die Sie zur Gruppe hinzufügen möchten, und klicken Sie anschließend auf **>**.

   > **Tipp**
   >
   > Um mehrere Server auszuwählen, drücken Sie die Taste *Strg wählen* sie durch einen Mausklick aus.

9. Klicken Sie auf **OK**.

   Im Verwaltungsbereich *Server* werden nun alle zur Gruppe hinzugefügten Server angezeigt. Sie können hier Statusänderungen vornehmen, Servermetriken abrufen und die Eigenschaften der Server in der Gruppe ändern.

Weitere Informationen

Anzeigen des Status von Servern [Seite 369]

10.7.2 Arbeiten mit Serveruntergruppen

Serveruntergruppen ermöglichen eine weitergehende Strukturierung der Server. Eine Serveruntergruppe ist eine Servergruppe, die zu einer anderen Servergruppe gehört.

Wenn Sie beispielsweise Ihre Server nach Regionen und Ländern gruppieren, können Sie die regionalen Gruppen als Untergruppen der Ländergruppen definieren. Erstellen Sie dazu für jede Region eine eigene Gruppe, der Sie die Server in der jeweiligen Region hinzufügen. Anschließend erstellen Sie weitere Gruppen für jedes Land, denen Sie die verschiedenen regionalen Gruppen hinzufügen.

Beim Einrichten von Untergruppen können Sie zwischen zwei Methoden wählen: Sie können die Untergruppen einer Servergruppe bearbeiten oder eine Servergruppe zu einer anderen hinzufügen. Das Ergebnis ist in beiden Fällen dasselbe. Wählen Sie die Methode, mit der Sie im jeweiligen Fall am schnellsten zum Ziel gelangen.

10.7.2.1 Hinzufügen von Untergruppen zu Servergruppen

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Klicken Sie in der Navigationsstruktur auf **Servergruppen**, und wählen Sie die Servergruppe aus, der Sie Untergruppen hinzufügen möchten.

   Diese Gruppe ist die übergeordnete Gruppe.
3. Wählen Sie im Menü **Aktionen** die Option **Elemente hinzufügen**.
4. Klicken Sie in der Navigationsstruktur auf **Servergruppen**, wählen Sie die Servergruppen aus, die dieser Gruppe hinzugefügt werden sollen, und klicken Sie auf **>**.

   > **Tipp**
   >
   > Um mehrere Servergruppen auszuwählen, drücken Sie die *STRG-Taste wählen* sie durch einen Mausklick aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

5. Klicken Sie auf **OK**.

   Im Verwaltungsbereich *Server* werden nun alle zur übergeordneten Gruppe hinzugefügten Servergruppen angezeigt.

10.7.2.2 So fügen Sie eine Servergruppe zu einer anderen hinzu

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Klicken Sie auf die Gruppe, die Sie einer anderen Gruppe hinzufügen möchten.
3. Wählen Sie im Menü **Aktionen** die Option **Zu Servergruppe hinzufügen**.
4. Markieren Sie in der Liste **Verfügbare Servergruppen** die anderen Gruppen, denen Sie die Gruppe hinzufügen möchten, und klicken Sie auf **>**.

   ➡ Tipp

   Um mehrere Servergruppen auszuwählen, drücken Sie die *STRG-Taste wählen* sie durch einen Mausklick aus.

5. Klicken Sie auf **OK**.

10.7.3 Ändern der Gruppenzugehörigkeit eines Servers

Sie können die Gruppenzugehörigkeit eines Servers ändern und ihn so auf einfache Weise zu einer beliebigen bereits bestehenden Gruppe oder Untergruppe hinzufügen bzw. daraus entfernen.

Beispiel: Es wurden Servergruppen für verschiedene Regionen erstellt. Möglicherweise möchten Sie einen einzelnen Central Management Server (CMS) für mehrere Regionen verwenden. Der CMS braucht hierzu nicht den einzelnen regionalen Servergruppen hinzugefügt werden. Sie können einfach auf die Verknüpfung **Mitglied von** für den Server klicken und ihn in einem Durchgang allen drei Regionen hinzufügen.

10.7.3.1 So ändern Sie die Gruppenzugehörigkeit eines Servers

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Klicken Sie mit der rechten Maustaste auf den Server, dessen Gruppenzugehörigkeitsinformationen Sie ändern möchten, und wählen Sie **Vorhandene Servergruppen**.
   In der Liste **Verfügbare Servergruppen** im Detailfenster werden die Gruppen angezeigt, denen Sie den Server hinzufügen können. In der Liste **Mitglied von Servergruppen** werden alle Servergruppen angezeigt, denen der Server momentan angehört.
3. Um die Gruppen zu ändern, denen der Server angehört, verschieben Sie die Servergruppen mithilfe der Pfeilschaltflächen zwischen den Listen und klicken anschließend auf **OK**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10.7.4 Zugriffsrechte auf Server und Servergruppen für Benutzer

Durch die Vergabe von Administratorrechten an Benutzer können diese Server- und Servergruppen-Aufgaben durchführen, z. B. Server starten und stoppen.

Je nach Systemkonfiguration und Sicherheitskonzept können Sie die Serververwaltung allein dem BI-Plattform-Administrator überlassen oder auch anderen Personen, die diese Server verwenden, Zugriffsrechte gewähren. In vielen Unternehmen ist eine Gruppe von IT-Experten mit der Serververwaltung betraut. Wenn das Serverteam regelmäßig Wartungsaufgaben ausführt, für die Server heruntergefahren und neu gestartet werden müssen, benötigt das Team Administratorrechte für die Server. Oder Sie möchten BI-Plattform-Server-Administrationsaufgaben an andere Personen delegieren bzw. eine bestimmte Gruppe in Ihrer Organisation dazu in die Lage versetzen, die Serververwaltung eigenständig durchzuführen.

> **Hinweis**
>
> Sie können einen Server oder eine Servergruppe für eine Veröffentlichung (nicht für einen bestimmten Benutzer) auswählen. Sie können jedoch Benutzern und Benutzergruppen Administratorrechte für einen bestimmten Server oder eine bestimmte Servergruppe gewähren.

10.7.4.1 Gewähren von Zugriffsrechten auf einen Server oder eine Servergruppe

Sie können Benutzern und Benutzergruppen Administratorrechte für einen bestimmten Server oder eine bestimmte Servergruppe gewähren.

> **Hinweis**
>
> Sie können einen Server oder eine Servergruppe für eine Veröffentlichung (nicht für einen Benutzer) auswählen.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Klicken Sie mit der rechten Maustaste auf den Server oder die Servergruppe, für den/die die Zugriffsberechtigung gewährt werden soll, und wählen Sie **Benutzersicherheit**.
3. Klicken Sie auf **Prinzipale hinzufügen**, um Benutzer oder Gruppen hinzuzufügen, denen Administrationsrechte für den ausgewählten Server bzw. die ausgewählte Servergruppe gewährt werden sollen.
4. Wählen Sie im Dialogfeld *Prinzipale hinzufügen* einen Benutzer oder eine Gruppe aus, dem/der Administrationsrechte für den Server bzw. die Servergruppe gewährt werden sollen, und klicken Sie auf **>**.
5. Klicken Sie auf **Sicherheit hinzufügen und zuweisen**.
6. Wählen Sie auf dem Bildschirm *Sicherheit zuweisen* die Sicherheitseinstellungen für den Benutzer oder die Gruppe aus, und klicken Sie auf **OK**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Funktionsweise von Rechten in der BI-Plattform [Seite 124]

10.7.4.2 Objektrechte für den Report Application Server

Um Benutzern das Erstellen und Ändern von Berichten über das Web mithilfe des Report Application Servers (RAS) zu ermöglichen, muss das System über RAS Report Modification-Lizenzen verfügen. Außerdem muss den Benutzern ein Mindestsatz an Objektrechten eingeräumt werden. Wenn Sie Benutzern diese Rechte für ein Berichtsobjekt gewähren, können diese den Bericht als Datenquelle für einen neuen Bericht wählen oder den Bericht direkt ändern:

- Objekte anzeigen (oder ggf. auch “Dokumentinstanzen anzeigen”)
- Objekte bearbeiten
- Berichtsdaten regenerieren
- Berichtsdaten exportieren

Die Benutzer müssen auch die Berechtigung haben, Objekte mindestens einem Ordner hinzufügen zu können, bevor Sie neue Berichte wieder in der BI-Plattform speichern können.

Um zu gewährleisten, dass Benutzer auch weiterhin andere Berichtsverarbeitungsaufgaben (z.B. Kopieren, zeitgesteuerte Verarbeitung, Drucken usw.) ausführen können, wird empfohlen, dass Sie zuerst die entsprechende Zugriffsberechtigung zuweisen und die Änderungen übernehmen. Ändern Sie anschließend die Zugriffsberechtigung in "Weitere", und fügen Sie weitere benötigte Rechte hinzu, die noch nicht gewährt wurden. Wenn die Benutzer bereits über das Recht "Ansicht auf Abruf" für ein Berichtsobjekt verfügen, gestatten Sie ihnen das Bearbeiten des Berichts durch Ändern der Zugriffsberechtigung in "Weitere" und Gewähren des zusätzlichen Objektrechts "Bearbeiten".

Wenn die Benutzer die Berichte über den Erweiterten DHTML-Viewer und den RAS anzeigen, ist die Zugriffsberechtigung "Ansicht" für das Anzeigen des Berichts ausreichend. Um jedoch die erweiterten Suchfunktionen nutzen zu können, ist "Ansicht auf Abruf" erforderlich. Das zusätzliche Objektrecht "Bearbeiten" ist nicht erforderlich.

10.8 Konfigurieren von Adaptive Processing Servern für Produktionssysteme

Mit dem Installationsprogramm wird ein Adaptive Processing Server (APS) pro Hostsystem installiert. Je nach installierten Funktionen kann dieser APS eine große Anzahl von Diensten hosten, beispielsweise den Überwachungsdienst, Promotion-Management-Dienst, Multi-Dimensional Analysis Service (MDAS), Veröffentlichungsdienst und andere.

Für Produktions- oder Testsysteme besteht die optimale Vorgehensweise darin, zusätzliche APS zu erstellen und diese gemäß Ihren Geschäftsanforderungen zu konfigurieren.

Zusätzliche APS können auf zwei Arten erstellt werden:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Sie führen den Systemkonfigurationsassistenten aus.

  Der Assistent hilft Ihnen bei den grundlegenden Konfigurationseinstellungen für das BI-Plattform-System, u.a. auch bei der APS-Konfiguration gemäß vordefinierten Implementierungsvorlagen. Die vom Assistenten bereitgestellte APS-Konfiguration ist ein guter Ausgangspunkt, allerdings muss das System-Sizing noch durchgeführt werden.
  Der Assistent steht in der Central Management Console (CMC) zur Verfügung. Weitere Informationen zum Assistenten finden Sie unter *Einführung in den Systemkonfigurationsassistenten* [Seite 87]. Weitere Informationen zu Standardimplementierungsvorlagen finden Sie im Dokument *SAP BusinessObjects BI platform Deployment Templates*, das im Assistenten und auch unter *http://help.sap.com/bobip41* zur Verfügung steht.
- In der CMC können Sie zusätzliche APS manuell erstellen und konfigurieren. Ausführliche Informationen finden Sie unter *Hinzufügen, Klonen und Löschen von Servern* [Seite 375].

➔ Nicht vergessen

Die Auswahl einer Implementierungsvorlage im Assistenten oder die manuelle Erstellung zusätzlicher APS ersetzt nicht das System-Sizing. Stellen Sie sicher, dass das Sizing durchgeführt wird: *http://www.sap.com/bisizing*.

10.9 Ermitteln der Systemleistung

10.9.1 Überwachen der BI-Plattform-Server

Das Überwachungstool ermöglicht die Ermittlung der Laufzeit- und Verlaufsmetriken von BI-Plattform-Servern für die Berichtserstellung und Benachrichtigung. Mithilfe des Tools können Systemadministratoren ermitteln, ob Server ordnungsgemäß funktionieren und die Antwortzeiten den Erwartungen entsprechen.

Weitere Informationen

Informationen zur Überwachung [Seite 666]

10.9.2 Analysieren der Servermetrik

Die Central Management Console (CMC) ermöglicht die Anzeige der Metriken für die Server in Ihrem System. Dazu gehören Informationen über jeden Rechner und Details, die für jeden Servertyp spezifisch sind. Die CMC ermöglicht Ihnen zudem die Anzeige der Systemmetrik, zu der Informationen über die Produktversion, den CMS und die aktuelle Systemaktivität zählen.

ℹ Hinweis

Sie können nur Metriken für Server anzeigen, die aktuell ausgeführt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10.9.2.1 So zeigen Sie die Servermetrik an

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Klicken Sie mit der rechten Maustaste auf den Server, dessen Metriken Sie anzeigen möchten, und wählen Sie **Metriken**.

In der Registerkarte *Metriken* wird eine Liste der Metriken für den Server angezeigt.

Weitere Informationen

Ändern der Eigenschaften eines Servers [Seite 392]
Info zu Servermetriken (Anhang) [Seite 989]

10.9.3 Anzeigen der Systemmetrik

Im Verwaltungsbereich *Einstellungen* der CMC werden Systemmetriken mit allgemeinen Informationen zur BI-Plattform-Installation angezeigt. Der Bereich *Eigenschaften* enthält Informationen zu Produktversion und Build. Zudem sind Datenquelle, Datenbankname und Datenbankbenutzername der CMS-Datenbank aufgeführt. Im Bereich *Globale Systemmetrik anzeigen* werden die aktuelle Kontoaktivität sowie Statistiken über aktuelle und verarbeitete Aufträge angezeigt. Im Bereich *Cluster* befinden sich der Name des CMS, mit dem Sie verbunden sind, der Name des CMS-Clusters sowie die Namen der anderen Clustermitglieder.

10.9.3.1 So zeigen Sie die Systemmetrik an

1. Wechseln Sie zum Verwaltungsbereich *Einstellungen* der CMC.
2. Klicken Sie auf einen Pfeil, um die Einstellungen in den Bereichen **Eigenschaften**, **Globale Systemmetrik anzeigen**, **Cluster** oder **Hotbackup** aufzuklappen und anzuzeigen.

10.9.4 Protokollieren der Serveraktivität

Die BI-Plattform ermöglicht es Ihnen, bestimmte Informationen über die BI-Plattform-Webaktivität zu protokollieren.

- Darüber hinaus ist jeder BI-Plattform-Server für die Protokollierung von Meldungen im Standardsystemprotokoll des Betriebssystems ausgelegt.
  - Unter Windows werden die Protokolle der BI-Plattform an den Dienst "Ereignisprotokoll" gesendet. Sie können die Ergebnisse mit dem Event Viewer (im Anwendungsprotokoll) anzeigen.
  - Unter UNIX werden die Protokolle der BI-Plattform an den syslog-Dämon als Benutzeranwendung gesendet. Jeder Server setzt seinen Namen und seine PID vor jede protokollierte Meldung.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Jeder Server speichert zudem Bestätigungsmeldungen im Protokollverzeichnis der Produktinstallation. Die in diesen Dateien protokollierten Programminformationen sind in der Regel nur für Supportmitarbeiter von SAP BusinessObjects zur Durchführung komplexer Fehlerbehebungsvorgänge von Interesse. Der Speicherort dieser Protokolldateien hängt vom Betriebssystem ab:

- Unter Windows ist das standardmäßige Protokollierungsverzeichnis **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\logging`.
- Unter UNIX ist das standardmäßige Protokollierungsverzeichnis der Installation **<INSTALLVERZ>**`/sap_bobj/logging`.

Hierbei sollte beachtet werden, dass diese Protokolldateien automatisch geleert werden, damit nur maximal 1 MB protokollierter Daten pro Server gespeichert werden.

> **Hinweis**
>
> Damit die Protokollierung auf UNIX-Rechnern funktioniert, auf denen BI-Plattform-Server gehostet werden, muss die Systemprotokollierung so eingerichtet und konfiguriert werden, dass alle bei der “user”-Komponente mit dem Level “info” oder höher protokollierten Meldungen aufgezeichnet werden. Sie müssen außerdem `SYSLOGD` konfigurieren, um die Remoteprotokollierung zu akzeptieren.
>
> Die Vorgehensweise beim Setup ist von System zu System verschieden. Entsprechende Hinweise finden Sie in der Dokumentation zu Ihrem Betriebssystem.

10.10 Konfigurieren von Servereinstellungen

Dieser Abschnitt enthält technische Informationen und Verfahren, mit denen das Ändern von Einstellungen für BI-Plattform-Server erklärt wird.

Die meisten der in diesem Abschnitt behandelten Einstellungen ermöglichen es Ihnen, die BI-Plattform effektiver in Ihre aktuellen Hardware-, Software- und Netzwerkkonfigurationen zu integrieren. Folglich hängen die von Ihnen gewählten Einstellungen zum großen Teil von Ihren eigenen Anforderungen ab.

Zum Ändern der Servereinstellungen mit der Central Management Console (CMC) gibt es zwei Möglichkeiten.

- Sie verwenden den Bildschirm *Eigenschaften* für den Server.
- Sie verwenden den Bildschirm *Gemeinsame Dienste bearbeiten* für den Server.

Es sollte beachtet werden, dass nicht alle Änderungen unverzüglich in Kraft treten. Wenn eine Einstellung nicht sofort geändert werden kann, werden auf den Bildschirmen *Eigenschaften* und *Gemeinsame Dienste bearbeiten* sowohl die aktuelle Einstellung (roter Text) als auch die gewünschte Einstellung angezeigt. Wenn Sie zum Verwaltungsbereich "Server" zurückkehren, ist der Server als "Veraltet" gekennzeichnet. Beim Neustart des Servers verwendet er die gewünschten Einstellungen, und das Kennzeichen "Veraltet" wird vom Server entfernt.

> **Hinweis**
>
> Die Konfiguration des Webanwendungsservers zur Implementierung von BI-Plattform-Anwendungen wird in diesem Abschnitt nicht behandelt. Diese Aufgabe wird in der Regel bei der Installation des Produkts ausgeführt. Einzelheiten hierzu finden Sie im *Installationshandbuch für SAP BusinessObjects Business Intelligence*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Konfigurieren von Portnummern [Seite 401]
Ändern der Eigenschaften eines Servers [Seite 392]
Neu erstellen der CMS-Systemdatenbank [Seite 441]
Auswählen einer neuen oder bereits vorhandenen CMS-Datenbank [Seite 439]

10.10.1 Ändern der Eigenschaften eines Servers

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den Server, dessen Einstellungen Sie ändern möchten.
   Der Bildschirm *Eigenschaften* wird angezeigt.
3. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie dann auf **Speichern** oder **Speichern und schließen**.

> **Hinweis**
>
> Nicht alle Änderungen treten unverzüglich in Kraft. Wenn eine Einstellung nicht sofort geändert werden kann, werden im Dialogfeld "Eigenschaften" sowohl die aktuelle Einstellung (roter Text) als auch die gewünschte Einstellung angezeigt. Wenn Sie zum Verwaltungsbereich "Server" zurückkehren, ist der Server als "Veraltet" gekennzeichnet. Wenn Sie den Server neu starten, verwendet er die gewünschten Einstellungen aus dem Dialogfeld "Eigenschaften", und das Kennzeichen "Veraltet" wird vom Server entfernt.

10.10.2 Anwenden von Diensteinstellungen auf mehrere Server

Sie können dieselbe Einstellung auf Dienste anwenden, die auf mehreren Servern gehostet werden.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Halten Sie die *Strg*-Taste gedrückt, und klicken Sie auf jeden Server, auf dem Dienste gehostet werden, für die Sie Einstellungen ändern möchten. Klicken Sie dann mit der rechten Maustaste, und wählen Sie **Gemeinsame Dienste bearbeiten** aus.
   Das Dialogfeld *Gemeinsame Dienste bearbeiten* wird angezeigt. Es enthält eine Liste der auf den von Ihnen ausgewählten Servern gehosteten Dienste, die Einstellungen haben, die Sie ändern können.
3. Wenn im Dialogfeld *Gemeinsame Dienste bearbeiten* mehrere Dienste aufgeführt werden, wählen Sie den zu bearbeitenden Dienst aus, und klicken Sie auf **Weiter**.
4. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie auf **OK**.

> **Hinweis**
>
> Sie werden zum *Server*-Verwaltungsbereich der CMC umgeleitet. Wenn der Server neu gestartet werden muss, ist er als "Veraltet" markiert. Wenn Sie den Server neu starten, verwendet er die neuen Einstellungen und die Kennzeichnung "Veraltet" wird entfernt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10.10.3 Arbeiten mit Konfigurationsvorlagen

Mithilfe von Konfigurationsvorlagen können Sie leicht mehrere Serverinstanzen konfigurieren. In Konfigurationsvorlagen wird eine Liste von Einstellungen für die einzelnen Diensttypen gespeichert, über die zusätzliche Serverinstanzen konfiguriert werden können. Wenn Sie beispielsweise über 12 Web Intelligence Processing Server verfügen, die identisch konfiguriert werden sollen, müssen nur die Einstellungen eines Servers konfiguriert werden. Über den konfigurierten Dienst können Sie die Konfigurationsvorlage für die Web Intelligence Processing Server festlegen und die Vorlage dann auf die übrigen 11 Dienstinstanzen anwenden.

Jeder BI-Plattform-Dienst verfügt über eine eigene Konfigurationsvorlage. Beispielsweise gibt es eine Konfigurationsvorlage für den Web-Intelligence-Verarbeitungsdiensttyp, eine für den Publishing-Diensttyp usw. Die Konfigurationsvorlage wird in den Servereigenschaften in der Central Management Console (CMC) definiert.

Wenn Sie für einen Server eine Konfigurationsvorlage verwenden, werden vorhandene Servereinstellungen mit den Werten aus der Vorlage überschrieben. Wenn Sie die Vorlage später nicht mehr verwenden möchten, werden die ursprünglichen Einstellungen nicht wiederhergestellt. Nachfolgende Änderungen an der Konfigurationsvorlage haben keinen weiteren Einfluss auf den Server.

Es empfiehlt sich, Konfigurationsvorlagen wie folgt zu verwenden:

1. Legen Sie die Konfigurationsvorlage auf einem Server fest.
2. Wenn Sie dieselbe Konfiguration auf alle Server desselben Typs anwenden möchten, aktivieren Sie **Konfigurationsvorlage verwenden** für alle Server desselben Typs, einschließlich des Servers, auf dem Sie die Konfigurationsvorlage festlegen.
3. Wenn Sie später die Konfiguration aller Dienste dieses Typs ändern möchten, lassen Sie die Eigenschaften eines dieser Dienste anzeigen und deaktivieren das Kontrollkästchen **Konfigurationsvorlage verwenden**. Ändern Sie die gewünschten Einstellungen, wählen Sie **Konfigurationsvorlage festlegen** für diesen Server, und klicken Sie auf **Speichern**. Alle Dienste dieses Typs werden aktualisiert. Dadurch, dass Sie über keinen Server verfügen, der immer als Konfigurationsvorlage festgelegt ist, stellen Sie sicher, dass nicht versehentlich die Konfigurationseinstellungen aller Server dieses Typs geändert werden.

Weitere Informationen

So legen Sie eine Konfigurationsvorlage fest [Seite 393]
So wenden Sie eine Konfigurationsvorlage auf einen Server an [Seite 394]

10.10.3.1 So legen Sie eine Konfigurationsvorlage fest

Sie können eine Konfigurationsvorlage für jeden Diensttyp festlegen. Sie können nicht mehrere Konfigurationsvorlagen für einen Dienst festlegen. Sie können die Seite *Eigenschaften* eines beliebigen Servers verwenden, um die Einstellungen zu konfigurieren, die von der Konfigurationsvorlage für einen auf dem Server gehosteten Diensttyp verwendet werden.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den Server, der die Dienste hostet, deren Konfigurationsvorlage Sie festlegen möchten. Der Bildschirm *Eigenschaften* wird angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Konfigurieren Sie die Diensteinstellungen, die Sie in der Vorlage verwenden möchten, aktivieren Sie das Kontrollkästchen **Konfigurationsvorlage festlegen**, und klicken Sie auf **Speichern** oder **Speichern & schließen**.

Die Konfigurationsvorlage für den ausgewählten Diensttyp wird gemäß den Einstellungen des aktuellen Servers definiert. Andere Server desselben Typs, die dieselben Dienste hosten, werden automatisch und unmittelbar neu konfiguriert, damit sie der Konfigurationsvorlage entsprechen, sofern die Option **Konfigurationsvorlage verwenden** in ihren Eigenschaften aktiviert wurde.

> **Hinweis**
>
> Wenn Sie die Einstellungen für die Konfigurationsvorlage nicht explizit festlegen, werden die Standardeinstellungen des Diensts verwendet.

Weitere Informationen

So wenden Sie eine Konfigurationsvorlage auf einen Server an [Seite 394]

10.10.3.2 So wenden Sie eine Konfigurationsvorlage auf einen Server an

Bevor Sie eine Konfigurationsvorlage anwenden, sollten Sie sicherstellen, dass Sie die Einstellungen der Konfigurationsvorlage für den Typ des Servers festgelegt haben, auf den die Vorlage angewendet werden soll. Wenn Sie die Einstellungen für die Konfigurationsvorlage nicht explizit definiert haben, werden die Standardeinstellungen für den Dienst verwendet.

> **Hinweis**
>
> Server, für die die Einstellung "Konfigurationsvorlage verwenden" nicht aktiviert wurde, werden nicht aktualisiert, wenn Sie die Einstellungen der Konfigurationsvorlage ändern.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den Server, der einen Dienst hostet, auf den Sie die Konfigurationsvorlage anwenden möchten.
   Der Bildschirm *Eigenschaften* wird angezeigt.
3. Aktivieren Sie das Kontrollkästchen **Konfigurationsvorlage verwenden**, und klicken Sie auf **Speichern** oder **Speichern & schließen**.

   > **Hinweis**
   >
   > Wenn der Server einen Neustart erfordert, damit die neuen Einstellungen wirksam werden, ist er in der Serverliste mit "Veraltet" gekennzeichnet.

Die entsprechende Konfigurationsvorlage wird auf den aktuellen Server angewendet. Durch die nachfolgenden Änderungen an der Konfigurationsvorlage ändert sich die Konfiguration aller Server, die diese Konfigurationsvorlage verwenden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wenn **Konfigurationsvorlage verwenden** deaktiviert wird, wird die Serverkonfiguration nicht auf die Werte zurückgesetzt, die vor Anwendung der Konfigurationsvorlage gültig waren. Nachfolgende Änderungen an der Konfigurationsvorlage wirken sich nicht auf die Konfiguration der Server aus, die die Konfigurationsvorlage verwenden.

Weitere Informationen

So legen Sie eine Konfigurationsvorlage fest [Seite 393]

10.10.3.3 Wiederherstellen der Systemstandardwerte

Vielleicht möchten Sie die Konfiguration eines Dienstes auf die Einstellungen zurücksetzen, mit denen er anfänglich installiert wurde (wenn Server beispielsweise falsch konfiguriert wurden oder Leistungsprobleme auftreten).

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den Server mit dem Dienst, für den Sie die Systemstandardeinstellungen wiederherstellen möchten.
   Der Bildschirm *Eigenschaften* wird angezeigt.
3. Aktivieren Sie das Kontrollkästchen **Systemstandardwerte wiederherstellen**, und klicken Sie auf **Speichern** oder **Speichern & schließen**.
   Die Standardeinstellungen des jeweiligen Diensttyps werden wiederhergestellt.

10.11 Konfigurieren von Netzwerkeinstellungen für Server

Die Netzwerkeinstellungen für BI-Plattform-Server werden über die CMC verwaltet. Diese Einstellungen werden in zwei Kategorien unterteilt: Porteinstellungen und Hostidentifikation.

Standardeinstellungen

Während der Installation werden die Serverhostkennungen auf **Automatisch zuweisen** festgelegt. Jedem Server kann jedoch eine bestimmte IP-Adresse oder ein bestimmter Hostname zugewiesen werden. Der CMS-Standardport ist 6400. Die übrigen BI-Plattform-Server werden dynamisch an verfügbare Ports gebunden. Portnummern werden automatisch von der BI-Plattform verwaltet, Sie können Portnummern jedoch auch über die CMC festlegen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10.11.1 Optionen für die Netzwerkumgebung

Die BI-Plattform unterstützt sowohl Netzwerk-Datenverkehr der Versionen IPv 6 (Internetprotokoll 6) als auch IPv 4 (Internetprotokoll 4). Sie können Server- und Clientkomponenten in einer beliebigen der folgenden Umgebungen verwenden:

- IPv4-Netzwerk: Alle Server- und Clientkomponenten werden nur mit dem IPv4-Protokoll ausgeführt.
- IPv6-Netzwerk: Alle Server- und Clientkomponenten werden nur mit dem IPv6-Protokoll ausgeführt.
- Gemischtes IPv6/IPv4-Netzwerk: Server- und Clientkomponenten werden sowohl mit dem IPv6- als auch mit dem IPv4-Protokoll ausgeführt.

> **Hinweis**
>
> Die Netzwerkkonfiguration sollte vom System- und Netzwerkadministrator ausgeführt werden. Die BI-Plattform bietet keinen Mechanismus zum Benennen einer Netzwerkumgebung. Über die CMC können Sie einen beliebigen BI-Plattform-Server an eine bestimmte IPv6- oder IPv4-Adresse binden.

10.11.1.1 Gemischte IPv6/IPv4-Umgebung

Die IPv6/IPv4-Netzwerkumgebung bietet folgende Möglichkeiten:

- BI-Plattform-Server können sowohl IPv6- als auch IPv4-Anforderungen verarbeiten, wenn sie im gemischten IPv6/IPv4-Modus ausgeführt werden.
- Clientkomponenten können mit Servern als Nur-IPv4-Knoten, Nur-IPv4-Knoten oder IPv6/IPv4-Knoten zusammenarbeiten.

Der gemischte Modus ist besonders in den folgenden Szenarios hilfreich:

- Sie wechseln von einer Nur-IPv4- zu einer Nur-IPv6-Knotenumgebung. Alle Client- und Serverkomponenten arbeiten bis zum Ende des Übergangs nahtlos weiter zusammen. Sie können anschließend die IPv4-Einstellungen für sämtliche Server deaktivieren.
- Software von Drittanbietern, die nicht IPv6-kompatibel ist, kann in der IPv6/IPv4-Knotenumgebung weiterhin eingesetzt werden.

10.11.2 Optionen zur Identifizierung des Serverhosts

Optionen zur Hostidentifikation können in der CMC für alle BI-Plattform-Server festgelegt werden. In der folgenden Tabelle werden die im Bereich *Allgemeine Einstellungen* verfügbaren Optionen zusammengefasst:

Option	Beschreibung
Automatisch zuweisen	Dies ist die Standardeinstellung für alle Server. Wenn dieses Kontrollkästchen ausgewählt ist, bindet der Server den Anforderungs-Port des Servers automatisch an die erste Netzwerkschnittstelle auf dem Rechner.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung
	Hinweis Es empfiehlt sich, das Kontrollkästchen **Automatisch zuweisen** für den Hostnamen zu aktivieren. In einigen Fällen, z.B. wenn der Server auf einem mehrfach vernetzten Rechner ausgeführt wird oder mit einer bestimmten Firewallkonfiguration zusammenarbeiten muss, sollten Sie die Verwendung eines bestimmten Hostnamens oder einer bestimmten IP-Adresse erwägen. Weitere Informationen finden Sie in den Abschnitten zum Konfigurieren eines mehrfach vernetzten Rechners und zum Arbeiten mit Firewalls im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.
Hostname	Gibt den Hostnamen der Netzwerkschnittstelle an, die vom Server auf Anforderungen überwacht wird. Für den CMS gibt diese Einstellung den Hostnamen der Netzwerkschnittstelle an, an die Name Server-Port und Anforderungs-Port vom CMS gebunden werden.
IP-Adresse	Gibt die IP-Adresse der Netzwerkschnittstelle an, die vom Server auf Anforderungen überwacht wird. Für den CMS gibt diese Einstellung die Adresse der Netzwerkschnittstelle an, an die Name Server-Port und Anforderungs-Port vom CMS gebunden werden. Für alle Server werden separate Felder zur Angabe von IPv4- und/oder IPv6-IP-Adressen angeboten.

Achtung

Wenn Sie das Kontrollkästchen **Automatisch zuweisen** auf einem mehrfach vernetzten Rechner aktivieren, wird der CMS u.U. automatisch an die falsche Netzwerkschnittstelle gebunden. Um dies zu verhindern, müssen die Netzwerkschnittstellen auf dem Hostrechner in der richtigen Reihenfolge aufgeführt sein (unter Verwendung der Betriebssystemtools des Rechners). Außerdem muss der Hostname für den CMS in der CMC festgelegt werden.

Hinweis

Wenn Sie mit mehrfach vernetzten Rechnern oder in einigen Konfigurationen mit einer NAT-Firewall arbeiten, sollten Sie den Hostnamen ggf. unter Verwendung des voll qualifizierten Domänennamens statt mit Hostnamen angeben.

Weitere Informationen

Konfigurieren des Systems für Firewalls [Seite 192]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Konfigurieren eines mehrfach vernetzten Rechners [Seite 398]
Beheben von Fehlern bei mehreren Netzwerkschnittstellen [Seite 400]

10.11.2.1 Ändern der Hostidentifikation eines Servers

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Wählen Sie den Server und dann **Server anhalten** aus dem Menü **Aktionen** aus.
3. Wählen Sie im Menü **Verwalten** den Befehl **Eigenschaften** aus.
4. Wählen Sie unter **Allgemeine Einstellungen** eine der folgenden Optionen:

Option	Beschreibung
Automatisch zuweisen	Der Server wird an eine der verfügbaren Netzwerkschnittstellen gebunden.
Hostname	Geben Sie den Hostnamen der Netzwerkschnittstelle ein, die vom Server auf Anforderungen überwacht wird.
IP-Adresse	Geben Sie in die vorhandenen Felder entweder eine IPv4- oder IPv6-IP-Adresse für die Netzwerkschnittstelle ein, die vom Server auf Anforderungen überwacht wird. **Hinweis** Damit der Server als dualer IPv4/IPv6-Knoten fungieren kann, geben Sie in beide Felder eine gültige IP-Adresse ein.

5. Klicken Sie auf **Speichern** oder **Speichern und schließen**.
   Die Änderungen werden in der Befehlszeile in der Registerkarte *Eigenschaften* angezeigt.
6. Starten und aktivieren Sie den Server.

10.11.3 Konfigurieren eines mehrfach vernetzten Rechners

Ein mehrfach vernetzter Rechner ist ein Rechner mit mehreren Netzwerkadressen. Sie können dies mit mehreren Netzwerkschnittstellen erreichen, von denen jede eine oder mehrere IP-Adressen hat, oder mit einer Netzwerkschnittstelle, der mehrere IP-Adressen zugeordnet wurden.

Wenn Sie mehrere Netzwerkschnittstellen mit einer jeweils eigenen IP-Adresse verwenden, ändern Sie die Bindungsreihenfolge, sodass die an erster Stelle stehende Netzwerkschnittstelle diejenige ist, mit der die BI-Plattform-Server eine Bindung herstellen sollen. Falls die Schnittstelle über mehrere IP-Adressen verfügt, verwenden Sie die Option "Hostkennungen" in der CMC, um eine Netzwerkschnittstellenkarte für den BI-Plattform-Server anzugeben. Dazu können Hostname oder IP-Adresse angegeben werden. Weitere Informationen über das Konfigurieren der Einstellung **Hostkennungen** finden Sie unter “Beheben von Fehlern bei mehreren Netzwerkschnittstellen”.

Tipp

In diesem Abschnitt wird beschrieben, wie Sie alle Server auf dieselbe Netzwerkadresse beschränken können. Es ist jedoch möglich, einzelne Server an unterschiedliche Adressen zu binden. Beispielsweise sollen die File Repository Server an eine private Adresse gebunden werden, die von Benutzerrechnern aus nicht routbar ist.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Bei solch erweiterten Konfigurationen muss die DNS-Konfiguration die Kommunikation effektiv zwischen allen BI-Plattform-Serverkomponenten routen. In diesem Beispiel muss der DNS die Kommunikation von den anderen BI-Plattform-Servern zu der privaten Adresse der File Repository Server routen.

Weitere Informationen

Beheben von Fehlern bei mehreren Netzwerkschnittstellen [Seite 400]

10.11.3.1 Konfigurieren des CMS für das Binden an eine Netzwerkadresse

> **Hinweis**
>
> Bei einem mehrfach vernetzten Rechner kann die Hostkennung der voll qualifizierte Domänenname oder die IP-Adresse der Schnittstelle sein, an die der Server gebunden werden soll.

1. Wechseln Sie zum Verwaltungsbereich **Server** der CMC.
2. Doppelklicken Sie auf den CMS.
3. Wählen Sie unter *Allgemeine Einstellungen* eine der folgenden Optionen:
   - **Hostname**
   - Geben Sie den Hostnamen der Netzwerkschnittstelle ein, an die der Server gebunden wird.
   - **IP-Adresse**
   - Geben Sie in die vorhandenen Felder entweder eine IPv4- oder eine IPv6-IP-Adresse für die Netzwerkschnittstelle ein, an die der Server gebunden wird.

     > **Hinweis**
     >
     > Damit der Server als dualer IPv4/IPv6-Knoten fungieren kann, geben Sie in beide Felder eine gültige IP-Adresse ein.

   > **Achtung**
   >
   > Lassen Sie die automatische Zuweisung deaktiviert.

4. Für **Anforderungs-Port** können Sie einen der folgenden Schritte ausführen:
   - Wählen Sie die Option **Automatisch zuweisen**.
   - Geben Sie eine gültige Portnummer in das Feld **Anforderungs-Port** ein.
5. Stellen Sie sicher, dass im Dialogfeld "Name Server-Port" eine Portnummer angegeben wird.

   > **Hinweis**
   >
   > Der Standardport ist 6400.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10.11.3.2 Konfigurieren der übrigen Server für das Binden an eine Netzwerkadresse

Für die übrigen BI-Plattform-Server werden die Ports standardmäßig dynamisch ausgewählt. Informationen zum Deaktivieren der Einstellung für automatische Zuordnung, mit der diese Informationen dynamisch propagiert werden, finden Sie unter "Ändern des Ports, den ein Server zum Entgegennehmen von Anforderungen verwendet".

Weitere Informationen

Ändern des Ports, den ein Server zum Entgegennehmen von Anforderungen verwendet [Seite 404]

10.11.3.3 Beheben von Fehlern bei mehreren Netzwerkschnittstellen

Bei einem mehrfach vernetzten Rechner kann der CMS automatisch an die falsche Netzwerkschnittstelle gebunden werden. Um dies zu verhindern, können Sie sicherstellen, dass die Netzwerkschnittstellen auf dem Hostrechner in der richtigen Reihenfolge aufgelistet werden (unter Verwendung der Betriebssystemtools des Rechners) oder dass die Einstellung "Hostname" für den CMS in der CMC angegeben ist. Wenn die primäre Netzwerkschnittstelle nicht routbar ist, können Sie die BI-Plattform so konfigurieren, dass eine Bindung an eine nicht primäre routbare Netzwerkschnittstelle vorgenommen wird. Führen Sie diese Schritte direkt nach der Installation der BI-Plattform auf dem lokalen Rechner aus, bevor Sie die BI-Plattform auf anderen Rechnern installieren.

1. Öffnen Sie den CCM, und stoppen Sie den SIA für den Knoten auf dem Rechner, der über mehrere Netzwerkschnittstellen verfügt.
2. Klicken Sie mit der rechten Maustaste auf den SIA, und wählen Sie **Eigenschaften**.
3. Klicken Sie im Dialogfeld *Eigenschaften* auf die Registerkarte *Konfiguration*.
4. Um den SIA an eine bestimmte Netzwerkschnittstelle zu binden, geben Sie die Portnummer der Zielnetzwerkschnittstelle im Feld **Port** ein.
5. Klicken Sie auf **OK**, und wählen Sie die Registerkarte *Start*.
6. Wählen Sie in der Liste *Lokale CMS-Server* den CMS, und klicken Sie auf **Eigenschaften**.
7. Um den CMS an eine bestimmte Netzwerkschnittstelle zu binden, geben Sie die Portnummer der Zielnetzwerkschnittstelle im Feld **Port** ein.
8. Klicken Sie auf **OK**, um die neuen Einstellungen anzuwenden.
9. Starten Sie den SIA, und warten Sie, bis die Server gestartet werden.
10. Starten Sie die Central Management Console (CMC), und wechseln Sie zum Verwaltungsbereich *Server*. Wiederholen Sie die Schritte 11 bis 14 für jeden Server.
11. Wählen Sie den Server und dann **Server anhalten** aus dem Menü **Aktionen** aus.
12. Wählen Sie im Menü **Verwalten** den Befehl **Eigenschaften** aus.
13. Wählen Sie unter **Allgemeine Einstellungen** eine der folgenden Optionen:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Hostname: Geben Sie den Hostnamen der Netzwerkschnittstelle ein, an die der Server gebunden wird.
- IP-Adresse: Geben Sie in die vorhandenen Felder entweder eine IPv4- oder eine IPv6-IP-Adresse für die Netzwerkschnittstelle ein, an die der Server gebunden wird.

> **Hinweis**
>
> Damit der Server als dualer IPv4/IPv6-Knoten fungieren kann, geben Sie in beide Felder eine gültige IP-Adresse ein.

> **Achtung**
>
> Lassen Sie die automatische Zuweisung deaktiviert.

14. Klicken Sie auf **Speichern** oder **Speichern und schließen**.
15. Kehren Sie zum CCM zurück, und starten Sie den SIA neu.

    Alle im Knoten enthaltenen Server werden vom SIA neu gestartet. Alle Server auf dem Rechner sind jetzt an die richtige Netzwerkschnittstelle gebunden.

10.11.4 Konfigurieren von Portnummern

Während der Installation wird der CMS für die Verwendung von Standardports eingerichtet. Der CMS-Standardport ist 6400. Dieser Port gehört in den Bereich der Ports, die für SAP BusinessObjects reserviert sind (6400 bis 6410). Daher sollte die Kommunikation über diese Ports keine Konflikte mit Anwendungen von Drittherstellern auslösen.

Beim Start und bei der Aktivierung wird jeder der anderen BI-Plattform-Server dynamisch an einen verfügbaren Port gebunden (höher als 1024). Er wird mit diesem Port beim CMS registriert und wartet dann auf BI-Plattform-Anforderungen. Falls erforderlich, können Sie jede Serverkomponente anweisen, einen bestimmten Port zu überwachen (statt einen beliebigen verfügbaren Port dynamisch auszuwählen). Beispielsweise müssen Sie für jeden BI-Plattform-Server manuell einen Anforderungsport konfigurieren, der über eine Firewall hinweg kommunizieren muss.

Portnummern können in der CMC auf jeder Registerkarte "Eigenschaften" der einzelnen Server angegeben werden. In der folgenden Tabelle sind die Optionen unter *Allgemeine Einstellungen* für die jeweilige Portnutzung für bestimmte Servertypen zusammengefasst:

Einstellung	CMS	Andere Server
Anforderungs-Port	Gibt den Port an, den der CMS verwendet, um alle Anforderungen von anderen Servern (außer Name Server-Anforderungen) zu akzeptieren. Verwendet dieselbe Netzwerkschnittstelle wie der Name Server-Port. Wenn **Automatisch zuweisen** ausgewählt ist, verwendet der Server automatisch eine vom Betriebssystem zugewiesene Portnummer.	Gibt den Port an, den der Server auf sämtliche Anforderungen überwacht. Wenn **Automatisch zuweisen** ausgewählt ist, verwendet der Server automatisch eine vom Betriebssystem zugewiesene Portnummer.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Einstellung	CMS	Andere Server
Name Server-Port	Gibt den BI-Plattform-Port an, den der CMS auf Namensdienst-Anforderungen überwacht. Der Standardwert ist 6400.	Nicht zutreffend.

10.11.4.1 Ändern des standardmäßigen CMS-Ports in der CMC

Wenn bereits ein CMS auf dem Cluster ausgeführt wird, können Sie die Standardportnummer des CMS über die CMC ändern. Falls auf dem Cluster kein CMS ausgeführt wird, verwenden Sie den CCM unter Windows or das Skript `serverconfig.sh` unter UNIX, um die Portnummer zu ändern.

> **Hinweis**
>
> Der CMS verwendet dieselbe NIC (Network Interface Card, Netzwerkschnittstellenkarte) für den Anforderungs- und den Name Server-Port.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den CMS in der Serverliste.
3. Ersetzen Sie **Name Server-Port** durch den Port, den der CMS überwachen soll. (Der Standardport ist 6400.)
4. Klicken Sie auf **Speichern und schließen**.
5. Starten Sie den CMS neu.

   Der CMS beginnt mit der Überwachung des angegebenen Ports. Der Server Intelligence Agent übergibt die neuen Einstellungen dynamisch an die anderen Server im Knoten, wenn für den Anforderungs-Port dieser Server die Option **Automatisch zuweisen** aktiviert wurde. (Es kann einige Minuten dauern, bis die Änderungen in den Eigenschafteneinstellungen sämtlicher Knotenmitglieder angezeigt werden.)

   Die auf der Seite *Eigenschaften* ausgewählten Einstellungen werden in der Serverbefehlszeile angezeigt, die ebenfalls auf der Seite *Eigenschaften* zu sehen ist.

10.11.4.2 Ändern des standardmäßigen CMS-Ports im CCM unter Windows

Falls kein CMS im Cluster verfügbar ist und Sie den Standard-CMS-Port für einen oder mehrere CMS in Ihrer Implementierung ändern möchten, müssen Sie den CCM zum Ändern der CMS-Portnummer verwenden.

1. Öffnen Sie den CCM, und stoppen Sie den SIA für den Knoten.
2. Klicken Sie mit der rechten Maustaste auf den SIA, und wählen Sie **Eigenschaften**.
3. Klicken Sie im Dialogfeld *Eigenschaften* auf die Registerkarte *Start*.
4. Wählen Sie in der Liste *Lokale CMS-Server* den CMS aus, dessen Portnummer geändert werden soll und klicken auf **Eigenschaften**.
5. Um den CMS an einen bestimmten Port zu binden, geben Sie die Portnummer im Feld **Port** ein.
6. Klicken Sie auf **OK**, um die neuen Einstellungen anzuwenden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7. Starten Sie den SIA, und warten Sie, bis die Server gestartet werden.

10.11.4.3 Ändern des standardmäßigen CMS-Ports im CCM unter UNIX

Falls kein CMS im Cluster verfügbar ist und Sie den standardmäßigen CMS-Port für einen oder mehrere CMS in der Implementierung ändern möchten, verwenden Sie das Skript `serverconfig.sh` zum Ändern der CMS-Portnummer.

1. Verwenden Sie das Skript `ccm.sh` zum Anhalten des Server Intelligence Agents (SIA), der den CMS hostet, dessen Portnummer Sie ändern möchten.
2. Führen Sie das Script `serverconfig.sh` aus.

   Dieses Skript befindet sich standardmäßig im Verzeichnis **`<INSTALLVERZ>`**`/sap_bobj`.
3. Wählen Sie **3 – Modify node** (Knoten ändern) aus, und drücken Sie die *Eingabetaste*.
4. Wählen Sie den Knoten aus, der den zu ändernden CMS hostet, und drücken Sie die *Eingabetaste*.
5. Wählen Sie **3 – Lokalen CMS ändern**, und drücken Sie die *Eingabetaste*.
   Eine Liste der auf dem Knoten gehosteten CMS wird angezeigt.
6. Wählen Sie den zu ändernden CMS aus, und drücken Sie die *Eingabetaste*.
7. Geben Sie die neue Portnummer für den CMS ein, und drücken Sie die *Eingabetaste*.
8. Geben Sie an, ob der CMS beim Start des SIA automatisch gestartet werden soll, und drücken Sie die *Eingabetaste*.
9. Geben Sie die Befehlszeilenargumente für den CMS ein, oder akzeptieren Sie die aktuellen Argumente, und drücken Sie die *Eingabetaste*.
10. Geben Sie **`quit`** ein, um das Skript zu beenden.
11. Starten Sie den SIA über das Skript`ccn.sh` und warten Sie, bis die Server gestartet werden.

10.11.4.4 Ändern des Ports, den ein CMS zum Entgegennehmen von Anforderungen verwendet

1. Wechseln Sie zum Verwaltungsbereich **Server** der CMC.
2. Wählen Sie den CMS und im Menü **Verwalten** die Option **Eigenschaften** aus.
3. Deaktivieren Sie unter **Allgemeine Einstellungen** das Kontrollkästchen **Automatisch zuweisen** für **Anforderungs-Port**, und geben Sie dann die Portnummer ein, die der Server überwachen soll.
4. Klicken Sie auf **Speichern** oder **Speichern und schließen**.
5. Starten Sie den CMS neu.

Der CMS stellt eine Bindung zum neuen Port her und hört diesen auf Anforderungen von anderen Servern ab.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10.11.4.5 Ändern des Ports, den ein Server zum Entgegennehmen von Anforderungen verwendet

> **Hinweis**
>
> Diese Schritte können nicht zum Ändern des Anforderungsports für den Central Management Server (CMS) verwendet werden. Siehe "Ändern des von einem CMS zur Annahme von Anforderungen verwendeten Ports".

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Wählen Sie den Server und dann **Server anhalten** aus dem Menü **Aktionen** aus.
3. Doppelklicken Sie auf den Server.
   Der Bildschirm *Eigenschaften* wird angezeigt.
4. Deaktivieren Sie unter *Allgemeine Einstellungen* das Kontrollkästchen **Automatisch zuweisen** für **Anforderungs-Port**, und geben Sie dann die Portnummer ein, die der Server überwachen soll.
5. Klicken Sie auf **Speichern** oder **Speichern und schließen**.
6. Starten und aktivieren Sie den Server.

Der Server wird an den neuen Port gebunden, registriert sich anschließend beim CMS und beginnt mit der Überwachung des neuen Ports auf BI-Plattform-Anforderungen.

10.12 Verwalten von Knoten

10.12.1 Verwenden von Knoten

Ein Knoten ist eine Gruppe von BI-Plattform-Servern, die auf demselben Host ausgeführt und von demselben Server Intelligence Agent (SIA) verwaltet werden. Alle Server auf einem Knoten werden unter demselben Benutzerkonto ausgeführt. Ein Rechner kann viele Knoten beinhalten, sodass Sie Prozesse unter verschiedenen Benutzerkonten ausführen können. Ein SIA verwaltet und überwacht alle Server auf einem Knoten und stellt so sicher, dass sie ordnungsgemäß funktionieren.

> **Hinweis**
>
> Zur sicheren Ausführung aller Knotenverwaltungsvorgänge ist ein Administratorkonto mit Enterprise-Authentifizierung zu verwenden. Wenn jedoch die SSL-Kommunikation zwischen Servern aktiviert ist, müssen Sie SSL deaktivieren, um die Knotenverwaltung durchzuführen.

> **Hinweis**
>
> Stellen Sie sicher, dass alle zum Herstellen einer Verbindung der BI-Plattform-Server zu ihren Datenquellen (z.B. des CMS zur CMS-Datenbank) erforderlichen Datenbanktreiber vorhanden sind, und dass die richtige Umgebung bereits eingerichtet ist (dass also z.B. die entsprechenden Umgebungsvariablen festgelegt wurden).

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Konfigurieren von Servern für SSL [Seite 174]
Vorbereiten eines UNIX-Rechners für SQL Anywhere [Seite 405]

10.12.1.1 Variablen

Variable	Beschreibung
<INSTALLVERZ>	Das Verzeichnis, in dem SAP BusinessObjects Business Intelligence installiert ist. Unter Windows: `C:\Programme (x86)\SAP BusinessObjects`
<SKRIPTVERZ>	Das Verzeichnis, in dem Knotenverwaltungsskripte gespeichert sind. • Unter Windows: **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts` • Unter Unix: **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/`**<PLATTFORM64>**`/scripts`
<PLATTFORM32>	Der Name Ihres Unix-Betriebssystems. Die folgenden Werte sind zulässig: • `aix_rs6000` • `linux_x86` • `solaris_sparc` • `win32_x86`
<PLATTFORM64>	Der Name Ihres Unix-Betriebssystems. Die folgenden Werte sind zulässig: • `aix_rs6000_64` • `linux_x64` • `solaris_sparcv9` • `win64_x64`

10.12.1.2 Vorbereiten eines UNIX-Rechners für SQL Anywhere

Sie müssen die Datei `odbc.ini` erstellen und ausführen, bevor Sie SQL Anywhere als ODBC-Datenquelle auf einem UNIX-Rechner verwenden können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Hinweis

Diese Vorgehensweise ist nicht erforderlich, wenn Sie die mit der BI-Plattform installierte gebündelte SQL Anywhere verwenden.

1. Erstellen Sie die Datei `odbc.ini` im Verzeichnis **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/`**<PLATFORM64>**.
2. Geben Sie den Namen der Datenbankquelle (DSN), den Datenbanknamen und den Servernamen für SQL Anywhere sowie die IP-Adresse und die Portnummer des Rechners ein, auf dem der Datenbankserver von SQL Anywhere gehostet wird.
3. Speichern Sie `odbc.ini`.
4. Bringen Sie die SQL-Anywhere-Umgebung in Ihre aktuelle Umgebung.

   Wenn Sie beispielsweise Bash als Befehlszeilen-Shell verwenden, geben Sie als Bezugsquelle `sa_config.sh` an.
5. Definieren Sie eine Umgebungsvariable mit dem Namen `ODBCINI`, die auf das Verzeichnis verweist, in dem die Datei `odbc.ini` erstellt wurde.

   Konfigurieren Sie die Umgebungsvariable, damit die untergeordneten Prozesse die Umgebungsvariable `ODBCINI` ermitteln können.

Beispiel

Beispiel für eine `odbc.ini`-Datei:

```
[ODBC Data Sources]
SampleDatabase=SQLAnywhere 12.0

[SampleDatabase]
UID=Administrator
PWD=password
DatabaseName=SampleDatabase
ServerName=SampleDatabase
CommLinks=tcpip(host=192.0.2.0;port=2638)
Driver=/build/bo/sqlanywhere12/lib64/libdbodbc12.so
```

Beispiel für einen `source`-Befehl:

```
source /build/bo/sqlanywhere12/bin64/sa_config.sh
ODBCINI=/build/bo/sap_bobj/enterprise_xi40/linux_x64/odbc.ini;export ODBCINI
```

Weitere Informationen

Variablen [Seite 405]

10.12.2 Hinzufügen eines neuen Knotens

Bei der erstmaligen Installation der BI-Plattform wird vom Installationsprogramm ein einzelner Knoten erstellt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Sie müssen ggf. weitere Knoten hinzufügen, wenn die Server unter verschiedenen Benutzerkonten ausgeführt werden sollen.

Zum Hinzufügen eines neuen Knotens können Sie Central Configuration Manager (CCM) oder ein Knotenverwaltungsskript verwenden. Bei Verwendung einer Firewall stellen Sie sicher, dass die Ports für den Server Intelligence Agent (SIA) und den Central Management Server (CMS) geöffnet sind.

> **Hinweis**
>
> Verwenden Sie das CCM- oder Knotenverwaltungsskript auf dem Rechner, auf dem ein Knoten hinzugefügt werden soll. Es kann kein Knoten auf einem Remote-Rechner hinzugefügt werden.

Eine BI-Plattform-Installation ist eine eindeutige Instanz der BI-Plattform-Dateien, die vom Installationsprogramm auf einem Rechner erstellt werden. Eine Instanz einer BI-Plattform-Installation kann nur innerhalb eines einzigen Clusters verwendet werden. Knoten, die zu verschiedenen Clustern derselben BI-Plattform-Installation gehören, werden nicht unterstützt, da diese Art der Implementierung nicht gepatcht oder aktualisiert werden kann. Nur Unix-Plattformen unterstützen mehrere Installationen der Software auf demselben Rechner, und zwar nur dann, wenn jede Installation unter einem eindeutigen Benutzerkonto ausgeführt und in einem separaten Ordner installiert wird, so dass die Installationen keine Dateien gemeinsam nutzen.

Beachten Sie, dass alle Rechner im Cluster dieselbe Version und denselben Patch-Level aufweisen müssen.

10.12.2.1 Hinzufügen von Knoten zu neuen Rechnern in vorhandenen Implementierungen

Sie können den ersten Knoten auf einem Rechner automatisch erstellen, wenn Sie einer vorhandenen Implementierung mit dem Installationsprogramm einen neuen Rechner hinzufügen.

> **Tipp**
>
> Klicken Sie während der Installation auf **Aufklappen**, und geben Sie den vorhandenen Central Management Server an.

Falls Sie zusätzliche Knoten erstellen möchten, verwenden Sie Central Configuration Manager oder das Skript`serverconfig.sh`.

Weitere Informationen zur Installation finden Sie im *Installationshandbuch für SAP BI*.

10.12.2.2 Hinzufügen von Knoten unter Windows

> **Achtung**
>
> Sichern Sie vor und nach dem Hinzufügen eines Knotens die Serverkonfiguration für den gesamten Cluster.

1. Klicken Sie in Central Configuration Manager (CCM) in der Symbolleiste auf **Knoten hinzufügen**.
2. Geben Sie im *Assistent zum Hinzufügen von Knoten* den Knotennamen und die Portnummer für den neuen Server Intelligence Agent (SIA) ein.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Bestimmen Sie, ob Server auf dem neuen Knoten erstellt werden sollen.
   - **Knoten ohne Server hinzufügen**
   - **Knoten mit CMS hinzufügen**
   - **Knoten mit Standardservern hinzufügen**

     Mit dieser Option werden nur die Server erstellt, die auf dem jeweiligen Rechner installiert sind. Sie schließt nicht alle verfügbaren Server ein.
4. Wählen Sie einen CMS aus.
   - Wenn die Implementierung ausgeführt wird, wählen Sie **Vorhandenen ausgeführten CMS verwenden** aus und klicken auf **Weiter**.

     Wenn Sie dazu aufgefordert werden, geben Sie den Hostnamen und die Portnummer des vorhandenen CMS, die Anmeldedaten des Administrators, den Namen der Datenquelle und die Anmeldedaten der Systemdatenbank sowie den Clusterschlüssel ein.
   - Wenn die Implementierung gestoppt wird, wählen Sie **Neuen temporären CMS starten** aus und klicken auf **Weiter**.

     Wenn Sie dazu aufgefordert werden, geben Sie den Hostnamen und die Portnummer für den temporären CMS, die Anmeldedaten des Administrators, den Namen der Datenquelle, die Datenbankanmeldedaten für die Systemdatenbank und den Clusterschlüssel ein. Es wird ein temporärer CMS gestartet. (Er wird gestoppt, wenn der Prozess abgeschlossen ist.)

     > **Achtung**
     >
     > Die Implementierung sollte während der Ausführung des temporären CMS nicht verwendet werden. Stellen Sie sicher, dass der vorhandene und der neue CMS unterschiedliche Ports verwenden.
5. Überprüfen Sie die Bestätigungsseite, und klicken Sie auf **Fertig stellen**.
   CCM erstellt einen Knoten. Falls Fehler auftreten, konsultieren Sie die Protokolldatei.

Sie können den neuen Knoten jetzt mit CCM starten.

10.12.2.2.1 Hinzufügen eines Knotens auf Windows mithilfe eines Skripts

> **Achtung**
>
> Sichern Sie die Serverkonfiguration für den gesamten Cluster vor und nach dem Hinzufügen eines Knotens.

Sie können mit `AddNode.bat` einen Knoten auf einem Windows-Rechner hinzufügen. Weitere Informationen finden Sie im Abschnitt “Skriptparameter zum Hinzufügen, Neuerstellen und Löschen von Knoten”.

> **Beispiel**
>
> Aufgrund der Einschränkungen der Befehlseingabeaufforderung müssen Sie das Caret-Zeichen (^) zum Steuern von Leerzeichen, das Gleichheitszeichen (=) und das Semikolon (;) in diesen Parametern verwenden, sofern Sie den Tet nicht in Anführungszeichen setzen.

```
<SKRIPTVERZ>\AddNode.bat -name mynode2
  -siaport 6415
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
      -cms mycms:6400
      -username Administrator
      -password My^ Password
      -cmsport 7400
      -dbdriver mysqldatabasesubsystem
      -connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
      -dbkey abc1234
      -noservers
      -createcms
```

Hinweis

Um die Verwendung des Zirkumflexzeichens in langen Zeichenfolgen zu vermeiden, können Sie den Skriptnamen und alle seine Parameter in eine temporäre `response.bat`-Datei schreiben und anschließend die `response.bat`-Datei ohne Parameter ausführen.

Weitere Informationen

Variablen [Seite 405]
Skriptparameter zum Hinzufügen, Neuerstellen und Löschen von Knoten [Seite 423]

10.12.2.3 Hinzufügen von Knoten unter Unix

Achtung

Sichern Sie vor und nach dem Hinzufügen eines Knotens die Serverkonfiguration für den gesamten Cluster.

1. Führen Sie `<INSTALLVERZ>/sap_bobj/serverconfig.sh` aus
2. Wählen Sie **1 – Add node**, und drücken Sie die *Eingabetaste*.
3. Geben Sie den Namen des neuen Knotens ein, und drücken Sie die *Eingabetaste*.
4. Geben Sie die Portnummer des neuen Server Intelligence Agents ein, und drücken Sie die *Eingabetaste*.
5. Wählen Sie aus, ob Server auf dem neuen Knoten erstellt werden sollen.
   - **no servers**

     Es wird ein Knoten erstellt, der keine Server enthält.
   - **cms**

     Es wird ein CMS auf dem Knoten erstellt, jedoch keine anderen Server.
   - **default servers**

     Es werden nur auf diesem Rechner installierte Server erstellt. Es sind nicht alle möglichen Server enhalten.
6. Wählen Sie einen CMS aus.
   - Wenn Ihre Implementierung ausgeführt wird, wählen Sie **existing**, und drücken Sie die *Eingabetaste*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wenn Sie dazu aufgefordert werden, geben Sie den Hostnamen und die Portnummer des vorhandenen CMS, die Anmeldedaten für den Administrator, die Datenbankverbindungsdaten und die Anmeldedaten für die Systemdatenbank sowie den Clusterschlüssel ein.

- Wenn Ihre Implementierung gestoppt ist, wählen Sie **temporary**, und drücken Sie die *Eingabetaste*.

  Wenn Sie dazu aufgefordert werden, geben Sie den Hostnamen und die Portnummer des temporären CMS, die Anmeldedaten für den Administrator, die Datenbankverbindungsdaten und die Anmeldedaten für die Systemdatenbank sowie den Clusterschlüssel ein. Es wird ein temporärer CMS gestartet. (Er wird gestoppt, wenn der Prozess abgeschlossen ist.)

  > **Achtung**
  >
  > Die Implementierung sollte während der Ausführung des temporären CMS nicht verwendet werden. Stellen Sie sicher, dass der vorhandene und der neue CMS unterschiedliche Ports verwenden.

7. Überprüfen Sie die Bestätigungsseite, und drücken Sie die *Eingabetaste*.
   Der CCM erstellt einen Knoten. Falls Fehler auftreten, konsultieren Sie die Protokolldatei.

Sie können nun `<INSTALLVERZ>/sap_bobj/ccm.sh -start <Knotenname>` ausführen, um den neuen Knoten zu starten.

10.12.2.3.1 Hinzufügen eines Knotens unter Unix anhand eines Skripts

> **Achtung**
>
> Sichern Sie die Serverkonfiguration für den gesamten Cluster vor und nach dem Hinzufügen eines Knotens.

Sie können `addnode.sh` zum Hinzufügen eines Knotens auf einem Unix-Rechner verwenden. Weitere Informationen finden Sie im Abschnitt “Skriptparameter zum Hinzufügen, Neuerstellen und Löschen von Knoten”.

> **Beispiel**

```
<SKRIPTVERZ>/addnode.sh -name mynode2
        -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=Administrator;PWD=Password1;HOSTNAME=myDatabase;PORT=3306"
        -dbkey abc1234
  -noservers
  -createcms
```

Weitere Informationen

Variablen [Seite 405]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Skriptparameter zum Hinzufügen, Neuerstellen und Löschen von Knoten [Seite 423]

10.12.3 Neuerstellen von Knoten

Sie können einen Knoten mit Central Configuration Manager (CCM) oder einem Knotenverwaltungsskript neu erstellen, nachdem Sie die Serverkonfiguration für den gesamten Cluster wiederhergestellt haben oder wenn der Rechner mit der Implementierung ausgefallen ist, beschädigt wurde oder ein fehlerhaftes Dateisystem aufweist. Berücksichtigen Sie folgende Richtlinien:

- Ein Knoten muss nicht neu erstellt werden, wenn Sie die Implementierung auf einem Ersatzrechner mit identischen Installationsoptionen und identischem Knotennamen neu installieren. Das Installationsprogramm erstellt den Knoten automatisch neu.
- Ein Knoten sollte nur auf einem Rechner mit einer vorhandenen Implementierung mit identischen Installationsoptionen und identischem Patch-Level neu erstellt werden.
- Sie sollten nur Knoten neu erstellen, die auf keinem Rechner in der Implementierung vorhanden sind. Stellen Sie sicher, dass keine anderen Rechner denselben Knoten hosten.
- Obwohl die Implementierung zulässt, dass Knoten unter verschiedenen Betriebssystemen ausgeführt werden, sollten Sie Knoten nur auf Rechnern neu erstellen, die dasselbe Betriebssystem verwenden.
- Bei Verwendung einer Firewall stellen Sie sicher, dass die Ports für den Server Intelligence Agent (SIA) und den Central Management Server (CMS) geöffnet sind.

➔ Nicht vergessen

Sie können einen Knoten nur auf dem Rechner neu erstellen, auf dem sich der Knoten befindet.

Weitere Informationen

Wiederherstellen des Systems [Seite 497]

10.12.3.1 Neuerstellen eines Knotens unter Windows

1. Klicken Sie in der Symbolleiste des Central Configuration Manager (CCM) auf **Knoten hinzufügen**.
2. Geben Sie im *Assistenten zum Hinzufügen von Knoten* den Knotennamen und die Portnummer für den neu erstellten Server Intelligence Agent (SIA) ein.

   ℹ Hinweis

   Die Namen des Originalknotens und des neu erstellten Knotens müssen identisch sein.

3. Wählen Sie **Knoten neu erstellen**, und klicken Sie auf **Weiter**.
   - Wenn der Knoten in der Systemdatenbank des Central Management Servers (CMS) vorhanden ist, wird er auf dem lokalen Host neu erstellt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Achtung**
>
> Verwenden Sie diese Option nur, wenn der Knoten auf keinen Hosts im Cluster vorhanden ist.

- Wenn der Knoten nicht in der Systemdatenbank des CMS vorhanden ist, wird ein neuer Knoten mit Standardservern hinzugefügt. Zu den Standardservern gehören alle auf dem Host installierten Server.

4. Wählen Sie einen CMS aus.
   - Wenn Ihr CMS ausgeführt wird, wählen Sie **Vorhandenen ausgeführten CMS verwenden**, und klicken Sie auf **Weiter**.

     Wenn Sie dazu aufgefordert werden, geben Sie den Hostnamen und die Portnummer des vorhandenen CMS, die Anmeldedaten des Administrators, den Namen der Datenquelle und die Anmeldedaten der Systemdatenbank sowie den Clusterschlüssel ein.
   - Wenn der CMS gestoppt ist, wählen Sie **Neuen temporären CMS starten**, und klicken Sie auf **Weiter**.

     Wenn Sie dazu aufgefordert werden, geben Sie den Hostnamen des temporären CMS, die Anmeldedaten des Administrators, den Namen der Datenquelle und die Anmeldedaten der Systemdatenbank sowie den Clusterschlüssel ein. Es wird ein temporärer CMS gestartet. (Er wird gestoppt, wenn der Prozess abgeschlossen ist.)

     > **Achtung**
     >
     > Die Implementierung sollte während der Ausführung des temporären CMS nicht verwendet werden.

5. Überprüfen Sie die Bestätigungsseite, und klicken Sie auf **Fertig stellen**.
   Der CCM erstellt den Knoten neu und fügt Informationen über den Knoten zum lokalen Rechner hinzu. Falls Fehler auftreten, überprüfen Sie die Protokolldatei.

Sie können den neu erstellten Knoten nun mithilfe des CCM starten.

10.12.3.1.1 Neuerstellen eines Knotens auf Windows mithilfe eines Skripts

Sie können mit `AddNode.bat` einen Knoten auf einem Windows-Rechner neu erstellen. Weitere Informationen finden Sie im Abschnitt “Skriptparameter zum Hinzufügen, Neuerstellen und Löschen von Knoten”.

> **Beispiel**
>
> Aufgrund der Einschränkungen der Befehlseingabeaufforderung müssen Sie das Caret-Zeichen (^) zum Steuern von Leerzeichen, das Gleichheitszeichen (=) und das Semikolon (;) in diesen Parametern verwenden, sofern Sie den Tet nicht in Anführungszeichen setzen.

```
<SKRIPTVERZ>\AddNode.bat -name mynode2
  -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
        -dbkey abc1234
  -adopt
```

> **Hinweis**
>
> Um die Verwendung des Zirkumflexzeichens in langen Zeichenfolgen zu vermeiden, können Sie den Skriptnamen und alle seine Parameter in eine temporäre `response.bat`-Datei schreiben und anschließend die `response.bat`-Datei ohne Parameter ausführen.

Weitere Informationen

Variablen [Seite 405]
Skriptparameter zum Hinzufügen, Neuerstellen und Löschen von Knoten [Seite 423]

10.12.3.2 Neuerstellen eines Knotens unter Unix

1. Führen Sie `<INSTALLVERZ>/sap_bobj/serverconfig.sh` aus
2. Wählen Sie **1 – Add node**, und drücken Sie die *Eingabetaste*.
3. Geben Sie den Namen des neuen Knotens ein, und drücken Sie die *Eingabetaste*.

   > **Hinweis**
   >
   > Die Namen des Originalknotens und des neu erstellten Knotens müssen identisch sein.

4. Geben Sie die Portnummer des neuen Server Intelligence Agents ein, und drücken Sie die *Eingabetaste*.
5. Wählen Sie **Knoten neu erstellen**, und drücken Sie die *Eingabetaste*.
   - Wenn der Knoten in der Systemdatenbank des Central Management Servers (CMS) vorhanden ist, wird er auf dem lokalen Host neu erstellt.

     > **Achtung**
     >
     > Verwenden Sie diese Option nur, wenn der Knoten auf keinen Hosts im Cluster vorhanden ist.

   - Wenn der Knoten nicht in der Systemdatenbank des CMS vorhanden ist, wird ein neuer Knoten mit Standardservern hinzugefügt. Zu den Standardservern gehören alle auf dem Host installierten Server.
6. Wählen Sie einen CMS aus.
   - Wenn Ihre Implementierung ausgeführt wird, wählen Sie **existing**, und drücken Sie die *Eingabetaste*.

     Wenn Sie dazu aufgefordert werden, geben Sie den Hostnamen und die Portnummer des vorhandenen CMS, die Anmeldedaten für den Administrator, die Datenbankverbindungsdaten und die Anmeldedaten für die Systemdatenbank sowie den Clusterschlüssel ein.
   - Wenn Ihre Implementierung gestoppt ist, wählen Sie **temporary**, und drücken Sie die *Eingabetaste*.

     Wenn Sie dazu aufgefordert werden, geben Sie den Hostnamen des temporären CMS, die Anmeldedaten für den Administrator, die Datenbankverbindungsdaten und die Anmeldedaten für die Systemdatenbank

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

sowie den Clusterschlüssel ein. Es wird ein temporärer CMS gestartet. (Er wird gestoppt, wenn der Prozess abgeschlossen ist.)

> **Achtung**
>
> Die Implementierung sollte während der Ausführung des temporären CMS nicht verwendet werden.

7. Überprüfen Sie die Bestätigungsseite, und drücken Sie die *Eingabetaste*.
   Der CCM erstellt den Knoten neu und fügt Informationen über den Knoten zum lokalen Rechner hinzu. Falls Fehler auftreten, überprüfen Sie die Protokolldatei.

Sie können nun `<INSTALLVERZ>/sap_bobj/ccm.sh -start <Knotenname>` ausführen, um den neu erstellten Knoten zu starten.

10.12.3.2.1 Neuerstellen von Knoten unter Unix mithilfe eines Skripts

Sie können `addnode.sh` zum Regenerieren eines Knotens auf einem Unix-Rechner verwenden. Weitere Informationen finden Sie im Abschnitt “Skriptparameter zum Hinzufügen, Neuerstellen und Löschen von Knoten”.

Beispiel

```
<SCRIPTDIR>/addnode.sh -name mynode2
        -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=Administrator;PWD=Password1;HOSTNAME=database;PORT=3306"
        -dbkey abc1234
        -adopt
```

Weitere Informationen

Variablen [Seite 405]
Skriptparameter zum Hinzufügen, Neuerstellen und Löschen von Knoten [Seite 423]

10.12.4 Löschen von Knoten

Ein gestoppter Knoten lässt sich mit einem ausgeführten Central Configuration Manager (CCM) oder einem Knotenverwaltungsskript löschen. Berücksichtigen Sie folgende Richtlinien:

- Durch das Löschen eines Knotens werden auch die Server auf diesem Knoten dauerhaft gelöscht.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Wenn der Cluster über mehrere Rechner verfügt, löschen Sie die Knoten, bevor Sie einen Rechner aus dem Cluster entfernen und die darauf befindliche Software deinstallieren. Falls Sie vor dem Löschen eines Knotens einen Rechner aus einem Cluster entfernen oder falls das Dateisystem auf einem Rechner nicht mehr funktioniert, müssen Sie den Knoten auf einem anderen Rechner mit denselben Servern im selben Cluster neu erstellen und dann den Knoten löschen.

> **Nicht vergessen**
>
> Sie können einen Knoten nur auf dem Rechner löschen, auf dem sich der Knoten befindet.

Weitere Informationen

Neuerstellen von Knoten [Seite 411]

10.12.4.1 Löschen eines Knotens unter Windows

> **Achtung**
>
> Sichern Sie vor und nach dem Löschen eines Knotens die Serverkonfiguration für das gesamte Cluster.

1. Führen Sie den Central Configuration Manager (CCM) aus.
2. Stoppen Sie im CCM den zu löschenden Knoten.
3. Wählen Sie den Knoten aus, und klicken Sie in der Symbolleiste auf **Knoten löschen**.
4. Wenn Sie dazu aufgefordert werden, geben Sie den Hostnamen, den Port und die Administratoranmeldedaten für den CMS ein.

Der CCM löscht den Knoten und alle Server auf dem Knoten.

10.12.4.1.1 Löschen von Knoten unter Windows mithilfe eines Skripts

> **Achtung**
>
> Sichern Sie vor und nach dem Löschen eines Knotens die Serverkonfiguration für den gesamten Cluster.

Mithilfe von `RemoveNode.bat` können Sie einen Knoten auf einem Windows-Rechner löschen. Weitere Informationen finden Sie im Abschnitt “Skriptparameter zum Hinzufügen, Neuerstellen und Löschen von Knoten”.

> **Beispiel**

```
<SCRIPTDIR>\RemoveNode.bat -name mynode2
        -cms mycms:6400
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
        -username Administrator
        -password Password1
```

Weitere Informationen

Variablen [Seite 405]
Skriptparameter zum Hinzufügen, Neuerstellen und Löschen von Knoten [Seite 423]

10.12.4.2 Löschen eines Knotens auf Unix

Sichern Sie vor und nach dem Löschen eines Knotens die Serverkonfiguration für das gesamte Cluster.

1. Führen Sie `<INSTALLVERZ>/sap_bobj/ccm.sh -stop <Knotenname>` aus, um den Knoten zu stoppen, den Sie löschen möchten.
2. Führen Sie `<INSTALLVERZ>/sap_bobj/serverconfig.sh` aus
3. Wählen Sie **2 – Knoten löschen**, und drücken Sie die *Eingabetaste*.
4. Wählen Sie den Knoten aus, den Sie löschen möchten, und drücken Sie die *Eingabetaste*.
5. Wenn Sie dazu aufgefordert werden, geben Sie den Hostnamen, die Portnummer und die Administratoranmeldedaten für den CMS ein.

Der Knoten und alle Server auf dem Knoten werden gelöscht.

10.12.4.2.1 Löschen eines Knotens unter Unix anhand eines Skripts

Achtung

Sichern Sie vor und nach dem Löschen eines Knotens die Serverkonfiguration für das gesamte Cluster.

Mithilfe von `removenode.sh` können Sie einen Knoten auf einem Unix-Rechner löschen. Weitere Informationen finden Sie im Abschnitt “Skriptparameter zum Hinzufügen, Neuerstellen und Löschen von Knoten”.

Beispiel

```
<SCRIPTDIR>\removenode.sh -name mynode2
        -cms mycms:6400
        -username Administrator
        -password Password1
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Variablen [Seite 405]
Skriptparameter zum Hinzufügen, Neuerstellen und Löschen von Knoten [Seite 423]

10.12.5 Umbenennen eines Knotens

Sie können einen Knoten mithilfe des Central Configuration Manager (CCM) umbenennen. Erstellen Sie zum Umbenennen eines Knotens einen neuen Knoten mit einem neuen Namen, klonen Sie die Server vom ursprünglichen Knoten zum neuen Knoten, und löschen Sie anschließend den ursprünglichen Knoten. Verwenden Sie die folgenden Richtlinien:

- Wenn Sie den Rechner umbenennen, auf dem sich der Knoten befindet, müssen Sie den Knoten nicht umbenennen. Sie können den vorhandenen Knotennamen weiterhin verwenden.
- Wenn Sie eine Firewall verwenden, stellen Sie sicher, dass die Ports des Server Intelligence Agent (SIA) und des Central Management Server (CMS) geöffnet sind.

➔ Nicht vergessen

Sie können einen Knoten nur auf dem Rechner umbenennen, auf dem sich der Knoten befindet.

Weitere Informationen

Hinzufügen eines neuen Knotens [Seite 406]
Klonen von Servern [Seite 376]
Löschen von Knoten [Seite 414]

10.12.5.1 Umbenennen von Knoten unter Windows

⚠ Achtung

Sichern Sie vor und nach dem Umbenennen eines Knotens die Serverkonfiguration für den gesamten Cluster.

1. Starten Sie den Central Configuration Manager (CCM).
2. Klicken Sie in Central Configuration Manager (CCM) in der Symbolleiste auf **Knoten hinzufügen**.
3. Geben Sie im *Assistent zum Hinzufügen von Knoten* den Knotennamen und die Portnummer des neuen Server Intelligence Agent (SIA), die Anmeldedaten des Administrators, die Verbindungsinformationen der Datenbank, die Anmeldedaten für die Systemdatenbank und den Clusterschlüssel ein.
4. Wählen Sie **Knoten ohne Server hinzufügen** aus.
5. Klonen Sie nach dem Erstellen des Knotens alle Server vom ursprünglichen Knoten zum neuen Knoten. Verwenden Sie hierfür die Seite *Serververwaltung* der Central Management Console.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Stellen Sie sicher, dass zwischen den geklonten Servern und den Servern auf dem alten Knoten keine Portkonflikte vorliegen.

6. Starten Sie den neuen Knoten in CCM.
7. Nachdem der neue Knoten fünf Minuten lang ausgeführt wurde, löschen Sie den ursprünglichen Knoten mit CCM.

Weitere Informationen

Hinzufügen eines neuen Knotens [Seite 406]
Klonen von Servern [Seite 376]
Löschen von Knoten [Seite 414]

10.12.5.2 Umbenennen von Knoten unter Unix

> **Achtung**
>
> Sichern Sie vor und nach dem Umbenennen eines Knotens die Serverkonfiguration für den gesamten Cluster.

1. Führen Sie `<INSTALLVERZ>/sap_bobj/serverconfig.sh` aus.
2. Wählen Sie **1 – Add node**, und drücken Sie die *Eingabetaste*.
3. Geben Sie den Namen des neuen Knotens ein, und drücken Sie die *Eingabetaste*.
4. Geben Sie die Portnummer des neuen Server Intelligence Agents ein, und drücken Sie die *Eingabetaste*.
5. Wenn Sie aufgefordert werden, geben Sie die Anmeldedaten des Administrators, die Verbindungsinformationen der Datenbank, die Anmeldedaten für die Systemdatenbank und den Clusterschlüssel ein.
6. Wählen Sie **Ohne Server** aus, und drücken Sie die *Eingabetaste*.
7. Klonen Sie nach dem Erstellen des Knotens alle Server vom ursprünglichen Knoten zum neuen Knoten. Verwenden Sie hierfür die Seite *Serververwaltung* der Central Management Console.

> **Hinweis**
>
> Stellen Sie sicher, dass zwischen den geklonten Servern und den Servern auf dem alten Knoten keine Portkonflikte vorliegen.

8. Führen Sie `<INSTALLVERZ>/sap_bobj/ccm.sh -start <Knotenname>` aus, um den neuen Knoten zu starten.
9. Nachdem der neue Knoten fünf Minuten lang ausgeführt wurde, löschen Sie den ursprünglichen Knoten mit `serverconfig.sh`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Hinzufügen eines neuen Knotens [Seite 406]
Klonen von Servern [Seite 376]
Löschen von Knoten [Seite 414]

10.12.6 Verschieben von Knoten

Zum Verschieben eines gestoppten Knotens von einem Cluster zu einem anderen können Sie Central Configuration Manager (CCM) oder ein Knotenverwaltungsskript verwenden. Berücksichtigen Sie folgende Richtlinien:

- Stellen Sie sicher, dass im Zielcluster kein Knoten mit demselben Namen vorliegt.
- Stellen Sie sicher, dass alle Servertypen, die auf dem Rechner installiert sind, auf dem sich der Quellknoten befindet, auch auf dem Zielcluster installiert sind.
- Wenn Sie einem Produktionscluster einen neuen Rechner hinzufügen möchten, dieser aber erst einsetzbar sein soll, wenn Sie ihn fertig getestet haben, installieren Sie die BI-Plattform auf einem eigenständigen Rechner, testen den Rechner, und verschieben den Knoten dann zu einem Produktionscluster.
- Die BI-Plattform-Versions- und Service-Pack-Ebene für diesen Rechner muss mit dem Rest des Clusters übereinstimmen.

Nicht vergessen

Sie können einen Knoten nur auf dem Rechner verschieben, auf dem sich der Knoten befindet.

10.12.6.1 Verschieben von vorhandenen Knoten unter Windows

In diesem Beispiel ist der zu verschiebende Knoten auf dem Quellsystem installiert. Der Quellsystemcomputer war ursprünglich Teil eines eigenständigen Clusters, wird jedoch zu einem Zielcluster hinzugefügt.

Achtung

Sichern Sie vor und nach dem Verschieben eines Knotens die Serverkonfiguration für das gesamte Cluster.

1. Stoppen Sie den Knoten in Central Configuration Manager (CCM).
2. Klicken Sie mit der rechten Maustaste auf den Knoten, und wählen Sie **Verschieben** aus.
3. Wählen Sie bei entsprechender Eingabeaufforderung den Namen der Datenquelle aus, und geben Sie den Hostnamen, den Port, die Verbindungsinformationen der Datenbank, die Anmeldedaten des Administrators für den Ziel-CMS und den Clusterschlüssel ein.
4. Wählen Sie einen CMS aus.
   - Wenn die Quellimplementierung ausgeführt wird, wählen Sie **Vorhandenen ausgeführten CMS verwenden** aus und klicken auf **Weiter**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wenn Sie dazu aufgefordert werden, geben Sie den Hostnamen und die Portnummer für den vorhandenen CMS des Quellsystems und die Administratoranmeldedaten ein.

- Wenn die Quellimplementierung gestoppt wird, wählen Sie **Neuen temporären CMS starten** aus und klicken auf **Weiter**.

  Geben Sie bei entsprechender Eingabeaufforderung den Hostnamen und die Portnummer für den temporären CMS des Quellsystems, die Anmeldedaten des Administrators, den Namen der Datenquelle, die Datenbankanmeldedaten für die Quellsystemdatenbank und den Clusterschlüssel ein. Es wird ein temporärer CMS gestartet. (Er wird gestoppt, wenn der Prozess abgeschlossen ist.)

  > **Achtung**
  >
  > Die Implementierung sollte während der Ausführung des temporären CMS nicht verwendet werden.

5. Überprüfen Sie die Bestätigungsseite, und klicken Sie auf **Fertig stellen**.
   CCM erstellt einen neuen Knoten im Zielcluster mit demselben Namen und denselben Server wie im Knoten im Quellcluster. Eine Kopie des Knotens verbleibt im Quellcluster. Die Konfigurationsvorlagen für die Server im Knoten können nicht verschoben werden. Falls Fehler auftreten, überprüfen Sie die Protokolldatei.

   > **Achtung**
   >
   > Verwenden Sie den Quellcluster nach Verschieben des Knotens nicht.

6. Starten Sie den verschobenen Knoten in CCM.

10.12.6.1.1 Verschieben eines Knotens unter Windows anhand eines Skripts

> **Achtung**
>
> Sichern Sie vor und nach dem Verschieben eines Knotens die Serverkonfiguration für das gesamte Cluster.

Sie können `MoveNode.bat` zum Verschieben eines Knotens auf einem Windows-Rechner verwenden. Weitere Informationen finden Sie im Abschnitt “Skriptparameter zum Verschieben von Knoten”.

> **Beispiel**
>
> Aufgrund der Einschränkungen der Befehlseingabeaufforderung müssen Sie das Caret-Zeichen (^) zum Steuern von Leerzeichen, das Gleichheitszeichen (=) und das Semikolon (;) in diesen Parametern verwenden, sofern Sie den Tet nicht in Anführungszeichen setzen.

```
<SCRIPTDIR>\MoveNode.bat -cms sourceMachine:6409
        -username Administrator
        -password Password1
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=Source
BOEXI40;UID=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
        -dbkey abc1234
        -destcms destinationMachine:6401
        -destusername Administrator
        -destpassword Password2
        -destdbdriver sybasedatabasesubsystem
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
        -destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
        -destdbkey def5678
```

> **Hinweis**
>
> Um die Verwendung des Zirkumflexzeichens in langen Zeichenfolgen zu vermeiden, können Sie den Skriptnamen und alle seine Parameter in eine temporäre `response.bat`-Datei schreiben und anschließend die `response.bat`-Datei ohne Parameter ausführen.

Weitere Informationen

Variablen [Seite 405]
Skriptparameter zum Verschieben von Knoten [Seite 425]

10.12.6.2 Verschieben eines vorhandenen Knotens unter Unix

In diesem Beispiel ist der zu verschiebende Knoten auf dem Quellsystem installiert. Der Quellsystemcomputer war ursprünglich Teil eines eigenständigen Clusters, wird jedoch zu einem Zielcluster hinzugefügt.

> **Achtung**
>
> Sichern Sie vor und nach dem Verschieben eines Knotens die Serverkonfiguration für das gesamte Cluster.

1. Führen Sie `<INSTALLVERZ>/sap_bobj/ccm.sh -stop <Knotenname>` aus, um den Knoten zu stoppen.
2. Führen Sie `<INSTALLVERZ>/sap_bobj/serverconfig.sh` aus
3. Wählen Sie **4 – Move node** aus, und drücken Sie die *Eingabetaste*.
4. Wählen Sie den zu verschiebenden Knoten, und drücken Sie die *Eingabetaste*.
5. Wenn Sie dazu aufgefordert werden, wählen Sie die Verbindungsdaten für die Systemdatenbank aus, und geben Sie den Hostname, den Port, die Anmeldedaten des Administrators für den Ziel-CMS sowie den Clusterschlüssel ein.
6. Wählen Sie einen CMS aus.
   - Wenn Ihre Quellimplementierung ausgeführt wird, wählen Sie **existing**, und drücken Sie die *Eingabetaste*.

     Wenn Sie dazu aufgefordert werden, geben Sie den Hostnamen und die Portnummer für den vorhandenen CMS des Quellsystems und die Administratoranmeldedaten ein.
   - Wenn Ihre Quellimplementierung gestoppt ist, wählen Sie **temporary**, und drücken Sie die *Eingabetaste*.

     Wenn Sie dazu aufgefordert werden, geben Sie den Hostnamen und den Port des temporären Quellsystem-CMS, die Anmeldedaten des Administrators, die Datenbankverbindungsdaten und die Anmeldedaten der Systemdatenbank sowie den Clusterschlüssel ein. Es wird ein temporärer CMS gestartet. (Er wird gestoppt, wenn der Prozess abgeschlossen ist.)

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Achtung**
>
> Die Implementierung sollte während der Ausführung des temporären CMS nicht verwendet werden. Stellen Sie sicher, dass der vorhandene und der temporäre CMS verschiedene Ports verwenden.

7. Überprüfen Sie die Bestätigungsseite, und drücken Sie die *Eingabetaste*.
   Der CCM erstellt einen neuen Knoten im Zielcluster mit demselben Namen und denselben Servern wie der Knoten im Quellcluster. Eine Kopie des Knotens verbleibt im Quellcluster. Die Konfigurationsvorlagen für die Server im Knoten können nicht verschoben werden. Falls Fehler auftreten, überprüfen Sie die Protokolldatei.

   > **Achtung**
   >
   > Das Quellcluster darf nach dem Verschieben des Knotens nicht mehr verwendet werden.

8. Führen Sie `<INSTALLVERZ>/sap_bobj/ccm.sh -start <Knotenname>` aus, um den verschobenen Knoten zu starten.

10.12.6.2.1 Verschieben eines Knotens auf Unix mithilfe eines Skripts

> **Achtung**
>
> Sichern Sie die Serverkonfiguration für den gesamten Cluster vor und nach dem Verschieben eines Knotens.

Sie können `movenode.sh` verwenden, um einen Knoten auf einem UNIX-Rechner zu verschieben. Weitere Informationen finden Sie im Abschnitt “Skriptparameter zum Verschieben von Knoten”.

Beispiel

```
<SCRIPTDIR>/movenode.sh -cms sourceMachine:6409
        -username Administrator
        -password Password1
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=Source
BOEXI40;UID^=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
        -dbkey abc1234
        -destcms destinationMachine:6401
        -destusername Administrator
        -destpassword Password2
        -destdbdriver sybasedatabasesubsystem
        -destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
        -destdbkey def5678
```

Weitere Informationen

Variablen [Seite 405]
Skriptparameter zum Verschieben von Knoten [Seite 425]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10.12.7 Skriptparameter

10.12.7.1 Skriptparameter zum Hinzufügen, Neuerstellen und Löschen von Knoten

Parameter	Beschreibung	Beispiel:
-adopt	Erstellt den Knoten neu, wenn er bereits im CMS vorhanden ist.	`-adopt`
-cms	Der Name und die Portnummer des Central Management Servers (CMS). **Achtung** Verwenden Sie diesen Parameter nicht, wenn Sie *-usetempcms* verwenden **Hinweis** Sie müssen eine Portnummer angeben, wenn der CMS nicht auf einem 6400-Standardport ausgeführt wird.	`-cms mycms:6409`
-cmsport	• Die Portnummer des CMS beim Start eines temporären CMS. **Einschränkung** Sie müssen auch die Parameter *-usetempcms*, *-dbdriver*, *-connect* und *-dbkey* verwenden. • Die Portnummer des CMS beim Erstellen eines neuen CMS. **Einschränkung** Sie müssen auch die Parameter *-dbdriver*, *-connect* und *-dbkey* verwenden.	`-cmsport 6401`
-connect	Die Verbindungszeichenfolge der CMS-Systemdatenbank (oder der temporären CMS-Systemdatenbank).	`-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=password;HOSTNAME=database;PORT=3306"`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Beschreibung	Beispiel:
	Hinweis Lassen Sie die Attribute *HOSTNAME* und *PORT* weg, wenn Sie sich bei einer DB2-, Oracle-, SQL-Anywhere-, SQL-Server- oder Sybase-Datenbank anmelden.	
-dbdriver	Der Datenbanktreiber des CMS. Zulässige Werte: • `db2databasesubsystem` • `maxdbdatabasesubsystem` • `mysqldatabasesubsystem` • `oracledatabasesubsystem` • `sqldatabasesubsystem` • `sqlserverdatabasesubsystem` • `sybasedatabasesubsystem` • `newdbdatabasesubsystem`	`-dbdriver mysqldatabasesubsystem`
-dbkey	Der Clusterschlüssel.	`-dbkey abc1234`
-name	Der Name des Knotens.	`-name mynode2`
-noservers	Erstellt einen Knoten ohne Server. **Hinweis** Der zusätzliche *-createcms*-Parameter erstellt einen Knoten mit einem CMS, jedoch keinen weiteren Servern. Lassen Sie diese Parameter weg, wenn Sie einen Knoten mit allen Standardservern erstellen möchten.	`-noservers`
-password	Das Kennwort des Administratorkontos.	`-password Password1`
-siaport	Die Portnummer des Server Intelligence Agent für den Knoten.	`-siaport 6409`
-username	Der Benutzername des Administratorkontos.	`-username Administrator`
-usetempcms	**Achtung** Verwenden Sie diesen Parameter nicht, wenn Sie *-cms* verwenden Startet und verwendet den temporären CMS.	`-usetempcms`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Beschreibung	Beispiel:
	Hinweis Verwenden Sie einen temporären CMS, wenn Ihre Implementierung nicht ausgeführt wird.	

Weitere Informationen

Hinzufügen eines Knotens auf Windows mithilfe eines Skripts [Seite 408]
Hinzufügen eines Knotens unter Unix anhand eines Skripts [Seite 410]
Neuerstellen eines Knotens auf Windows mithilfe eines Skripts [Seite 412]
Neuerstellen von Knoten unter Unix mithilfe eines Skripts [Seite 414]
Löschen von Knoten unter Windows mithilfe eines Skripts [Seite 415]
Löschen eines Knotens unter Unix anhand eines Skripts [Seite 416]

10.12.7.2 Skriptparameter zum Verschieben von Knoten

Parameter	Beschreibung	Beispiel:
-cms	Der Name des Quell-Central Management Servers (CMS). **Achtung** Verwenden Sie diesen Parameter nicht, wenn Sie *-usetempcms* verwenden **Hinweis** Sie müssen eine Portnummer angeben, wenn der CMS nicht auf einem 6400-Standardport ausgeführt wird.	`-cms sourceMachine:6409`
-cmsport	• Die Portnummer des CMS beim Start eines temporären CMS.	`-cmsport 6401`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Beschreibung	Beispiel:
	Einschränkung Sie müssen auch die Parameter *-usetempcms*, *-dbdriver*, *-connect* und *-dbkey* verwenden. • Die Portnummer des CMS beim Erstellen eines neuen CMS. **Einschränkung** Sie müssen auch die Parameter *-dbdriver*, *-connect* und *-dbkey* verwenden.	
-connect	Die Verbindungszeichenfolge des Quell-CMS oder der temporären CMS-Systemdatenbank. **Hinweis** Lassen Sie die Attribute *HOSTNAME* und *PORT* weg, wenn Sie sich bei einer DB2-, Oracle-, SQL-Anywhere-, SQL-Server- oder Sybase-Datenbank anmelden.	`-connect "DSN=Source BOEXI40;UID=username;PWD=password;HOSTNAME=database;PORT=3306"`
-dbdriver	Der Datenbanktreiber des Quell-CMS. Zulässige Werte: • `db2databasesubsystem` • `maxdbdatabasesubsystem` • `mysqldatabasesubsystem` • `oracledatabasesubsystem` • `sqldatabasesubsystem` • `sqlserverdatabasesubsystem` • `sybasedatabasesubsystem` • `newdbdatabasesubsystem`	`-dbdriver mysqldatabasesubsystem`
-dbkey	Der Quell-Clusterschlüssel.	`-dbkey abc1234`
-destcms	Der Name des Ziel-CMS. **Hinweis** Sie müssen eine Portnummer angeben, wenn der CMS nicht auf einem 6400-Standardport ausgeführt wird.	`-destcms destinationMachine:6401`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Beschreibung	Beispiel:
-destconnect	Die Verbindungszeichenfolge der CMS-Zieldatenbank. **Hinweis** Lassen Sie die Attribute *HOSTNAME* und *PORT* weg, wenn Sie sich bei einer DB2-, Oracle-, SQL-Anywhere-, SQL-Server- oder Sybase-Datenbank anmelden.	`-destconnect "DSN=Destin BOEXI40;UID=username;PWD=pass-word;HOSTNAME=database;PORT=3306"`
-destdbdriver	Der Datenbanktreiber des Ziel-CMS. Zulässige Werte: • `db2databasesubsystem` • `maxdbdatabasesubsystem` • `mysqldatabasesubsystem` • `oracledatabasesubsystem` • `sqldatabasesubsystem` • `sybasedatabasesubsystem` • `newdbdatabasesubsystem`	`-destdbdriver sybasedatabasesub-system`
-destdbkey	Der Ziel-Clusterschlüssel.	`-destdbkey def5678`
-destpassword	Das Kennwort des Administratorkontos auf dem Ziel-CMS.	`-destpassword Password2`
-destusername	Der Benutzername des Administratorkontos auf dem Ziel-CMS.	`-destusername Administrator`
-password	Das Kennwort des Administratorkontos auf dem Quell-CMS.	`-password Password1`
-username	Der Benutzername des Administratorkontos auf dem Quell-CMS.	`-username Administrator`
-usetempcms	**Achtung** Verwenden Sie diesen Parameter nicht, wenn Sie *-cms* verwenden Startet und verwendet den temporären CMS. **Hinweis** Verwenden Sie einen temporären CMS, wenn Ihre Implementierung nicht ausgeführt wird.	`-usetempcms`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Verschieben eines Knotens unter Windows anhand eines Skripts [Seite 420]
Verschieben eines Knotens auf Unix mithilfe eines Skripts [Seite 422]

10.12.8 Hinzufügen von Windows-Server-Abhängigkeiten

In einer Windows-Umgebung hängen alle Instanzen des Server Intelligence Agent (SIA) von den Ereignisprotokoll- und RPC-Diensten (Remote-Prozeduraufruf) ab.

Wenn ein SIA nicht ordnungsgemäß arbeitet, stellen Sie sicher, dass beide Dienste in der Registerkarte *Abhängigkeit* des SIA angezeigt werden.

10.12.8.1 Hinzufügen von Windows-Server-Abhängigkeiten

1. Verwenden Sie den Central Configuration Manager (CCM), um den Server Intelligence Agent (SIA) zu stoppen.
2. Klicken Sie mit der rechten Maustaste auf den SIA, und wählen Sie **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Abhängigkeit**.
4. Klicken Sie auf **Hinzufügen**.
   Im Dialogfeld *Abhängigkeit hinzufügen* wird eine Liste aller verfügbaren Abhängigkeiten angezeigt.
5. Wählen Sie eine Abhängigkeit, und klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **OK**.
7. Starten Sie den SIA mithilfe des CCM neu.

10.12.9 Ändern von Benutzeranmeldedaten für einen Knoten

Mit Central Configuration Manager (CCM) können Sie die Benutzeranmeldedaten für den Server Intelligence Agent (SIA) angeben oder aktualisieren, wenn sich das Betriebssystemkennwort ändert oder wenn Sie alle Server eines Knotens unter einem anderen Benutzerkonto ausführen möchten.

Alle vom SIA verwalteten Server werden unter demselben Konto ausgeführt. Um einen Server unter einem systemfremden Konto auszuführen, stellen Sie sicher, dass das Konto zur lokalen Administratorgruppe auf dem Serverrechner gehört und über das Recht “Ersetzen eines Tokens auf Prozessebene” verfügt.

Einschränkung

Auf einem Unix-Rechner muss die BI-Plattform mit demselben Konto ausgeführt werden, mit dem das Produkt auch installiert wurde. Um ein anderes Konto zu verwenden, installieren Sie die Implementierung mit einem anderen Konto erneut.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

10.12.9.1 Ändern der Benutzeranmeldedaten für einen Knoten auf Windows

1. Verwenden Sie den Central Configuration Manager (CCM), um den Server Intelligence Agent (SIA) zu stoppen.
2. Klicken Sie mit der rechten Maustaste auf den SIA, und wählen Sie **Eigenschaften**.
3. Deaktivieren Sie das Kontrollkästchen **Systemkonto**.
4. Geben Sie einen Benutzernamen und ein Kennwort ein, und klicken Sie auf **OK**.
5. Starten Sie den SIA mithilfe des CCM neu.

Die SIA- und Serverprozesse melden sich mit dem neuen Benutzerkonto auf dem lokalen Rechner an.

10.13 Umbenennen eines Rechners in einer BI-Plattform-Implementierung

10.13.1 Ändern von Cluster-Namen

Im Folgenden sind optimale Vorgehensweisen für die Umbenennung von Clustern aufgeführt:

> ⚠ Achtung
>
> Implementieren Sie nie mehrere Cluster mit demselben Namen.

Bedingung	Aktion
Der Name des Clusters wird geändert.	Informieren Sie die Benutzer über den neuen Cluster-Namen, und bitten Sie sie, diesen zu verwenden (nach der ersten Verbindung mit dem CMS unter Verwendung der Syntax `<Hostname>:<Port>`). Aktualisieren Sie auf der Webschicht den Cluster-Namen in der Eigenschaftendatei aller Webanwendungsserver.
Sie installieren eine andere BI-Plattform-Version auf einem Rechner, auf dem zuvor ein CMS ausgeführt wurde, oder Sie fügen den Rechner einem anderen Cluster hinzu.	• Stellen Sie sicher, dass der Neue CMS an einem anderen Port ausgeführt wird. • Verwenden Sie unterschiedliche Kennwörter für unterschiedliche Cluster, um zu vermeiden, dass sich Benutzer an einem falschen Cluster anmelden.

10.13.2 Ändern der IP-Adresse

Um Konfigurationsänderungen zu vermeiden, die sich aus Änderungen der IP-Adresse des Rechners ergeben, wählen Sie **Servereigenschaften** auf der Registerkarte **Server** der CMC aus, und stellen Sie sicher, dass alle

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Server an Hostnamen gebunden sind, oder verwenden Sie die Option **Automatisch zuweisen**. Folgen Sie außerdem diesen optimalen Vorgehensweisen:

Bedingung	Aktion
Sie verwenden ODBC mit der CMS-Datenbank oder der Audit-Datenbank.	Stellen Sie sicher, dass der DSN den Hostnamen des CMS-Datenbankservers verwendet.
Sie verwenden einen anderen Datenbankverbindungstyp mit der CMS-Datenbank oder der Audit-Datenbank.	Aktualisieren Sie die Datenbank mit dem CCM so, dass der Hostname des Datenbankservers verwendet wird.
Die CMS-Datenbank oder die Audit-Datenbank befindet sich auf demselben Host auf dem CMS.	Verwenden Sie `localhost` als Rechnernamen.
Sie verwenden die URL für die BI-Plattform-Webanwendungen, auf die Benutzer mit Webbrowsern zugreifen (z.B. die CMC).	Verwenden Sie Hostnamen anstelle von IP-Adressen für die Standard-URL. Um die URL für den Standardviewer zu aktualisieren, wählen Sie für die ausgewählte Anwendung die Option **Verarbeitungseinstellungen**. Wählen Sie beispielsweise für OpenDocument die Registerkarte **Anwendungen** in der CMC, klicken Sie mit der rechten Maustaste auf **OpenDocument** und wählen **Verarbeitungseinstellungen**.
Sie verwenden die URL für BI-Plattform-Clients, die auf Webdiensten basieren (z.B. Crystal Reports für Java oder Live Office).	
Sie verwenden OpenDocument.	

Alternative Richtlinien

> **Hinweis**
>
> Folgen Sie diesen Richtlinien nur, wenn Sie nicht die oben aufgeführten optimalen Verfahrensweise verwenden können.

Tabelle 15: Für Rechner, auf denen Server gehostet werden

Bedingung	Aktion
Der Host enthält BI-Plattform-Server, und die Server müssen an bestimmte IP-Adressen gebunden werden.	Ändern Sie die IP-Adressen auf der Registerkarte **Server** der CMC, starten Sie die Server jedoch erst dann neu, wenn der Rechner komplett aktualisiert wurde. Starten Sie dann den Rechner neu, nicht die einzelnen BI-Plattform-Server.
Eine Datenbankverbindung muss eine IP-Adresse verwenden.	Ändern Sie die IP-Adresse.
Eine Änderung der IP-Adresse ist in einem statischen IP-Netzwerk erforderlich.	Ändern Sie die IP-Adresse des BI-Plattform-Rechners. **Tipp** Melden Sie sich an der CMC an, um zu überprüfen, ob die BI-Plattform betriebsbereit ist.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

➔ Nicht vergessen

Starten Sie den Rechner neu, nachdem Sie eine Aktion durchgeführt haben.

Tabelle 16: Für Rechner, auf denen der Webanwendungsserver gehostet wird

Bedingung	Aktion
Die Standard-Viewer-URL von OpenDocument muss eine IP-Adresse verwenden.	Aktualisieren Sie die IP-Adresse im Feld **Standard-Viewer-URL festlegen** im Abschnitt **Verarbeitungseinstellungen** der Registerkarte **Anwendungen** der CMC.
Die Benutzer greifen auf BI-Plattform-Webanwendungen zu (z.B. die CMC), indem sie in den Browsern eine URL mit einer IP-Adresse angeben.	Teilen Sie die neue IP-Adresse allen Benutzern mit.
Die BI-Plattform-Clients, die auf Webdiensten basieren (z.B. Crystal Reports für Java oder Live Office), müssen IP-Adressen verwenden.	Konfigurieren Sie alle Clients so, dass sie die neue IP-Adresse verwenden.

Weitere Informationen

Auswählen einer neuen oder bereits vorhandenen CMS-Datenbank [Seite 439]

10.13.3 Umbenennen von Rechnern

Sie können Rechner in einer BI-Plattform-Implementierung jederzeit umbenennen, indem Sie alle BI-Plattform-Server auf dem Rechner stoppen und den Rechner dann umbenennen. Folgende optimale Verfahrensweisen gelten für die Umbenennung von Rechnern:

Bedingung	Aktion
Sie melden sich zum ersten Mal an.	Verwenden Sie den CMS-Rechnernamen (und nicht den Clusternamen).
Sie haben eine Implementierung mit mehreren Rechnern.	Stellen Sie sicher, dass während der Umbenennung alle CMS-Server auf allen anderen Rechnern ausgeführt werden.

10.13.3.1 Server-Schicht

ℹ Hinweis

Bevor Sie den CMS-Rechner umbenennen, prüfen Sie die Konfiguration aller Server, die sich auf dem Rechner befinden, den Sie auf der Registerkarte “Serververwaltung” der CMC umbenennen möchten. Wenn die

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft *Hostname* den alten CMS-Hostnamen verwendet, aktualisieren Sie sie auf den neuen CMS-Hostnamen.

Nicht vergessen

Starten Sie den Server erst dann neu, wenn alle Rechnerumbenennungsschritte durchgeführt wurden.

Folgen Sie diesen Anleitungen, um Server-Schichtrechner umzubenennen:

Bedingung	Aktion
Auf dem umbenannten Rechner wird ein CMS gehostet, und die Benutzer haben sich zuvor angemeldet, indem sie den Namen des alten Rechners angegeben haben.	Informieren Sie die Benutzer über den CMS-Rechnernamen, und fordern Sie sie auf, diesen zu verwenden.
Auf dem umbenannten Rechner wird ein CMS gehostet, und die Standardeigenschaftendateien der BI-Plattform-Webanwendung enthalten den alten CMS-Hostnamen in der Eigenschaft `cms.default`.	Aktualisieren Sie den CMS-Rechnernamen in der Eigenschaft `cms.default` in allen benutzerdefinierten Eigenschaftendateien auf allen Webschichtrechnern. Auf Tomcat befinden sich die von Ihnen erstellten Eigenschaftendateien im Verzeichnis **`<INSTALLVERZ>`**`SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\'BOE\BOE\WEB-INF\config\custom`. **Hinweis** Wenn keine benutzerdefinierten Eigenschaftendateien vorhanden sind, erstellen Sie neue. Kopieren Sie die Standard-Eigenschaftendateien in einen benutzerdefinierten Ordner, und entfernen Sie außer der Zeile `cms.default` alle Inhalte aus den benutzerdefinierten Eigenschaftendateien.
Auf dem umbenannten Rechner wird ein CMS gehostet, und SAP BusinessObjects Explorer ist auf einem beliebigen Rechner im Cluster installiert.	Ersetzen Sie den alten CMS-Hostnamen auf allen Rechnern, auf denen Webanwendungsserver gehostet werden, in der Eigenschaft `default.cms.name` in der Datei `default.settings.properties` durch den neuen Hostnamen. Auf Tomcat befindet sich die Datei `default.settings.properties` standardmäßig im Verzeichnis **`<INSTALLVERZ>`**`\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\explorer\WEB-INF\classes\` **Nicht vergessen** Nachdem Sie die Aktion durchgeführt haben, starten Sie die Explorer-Webanwendung oder den Webanwendungsserver neu.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Bedingung	Aktion
Sie verwenden die Einzelanmeldung mit Explorer	Aktualisieren Sie den Wert `cms` in `jsp-sso-provider.jsp` und die Werte `sso.global.cms` und `sso.trusted.auth.x509.cms` in `sso.properties` auf den neuen CMS-Hostnamen.
Sie verwenden Portal Integration Kits oder benutzerdefinierte Anwendungen.	Konfigurieren Sie die Portal Integration Kits oder benutzerdefinierten Anwendungen so, dass der neue CMS-Hostname verwendet wird.
Ihre Implementierung erfüllt alle folgenden Bedingungen: • Ein Cluster hat mehrere Knoten. • Alle CMS-Server werden nur auf dem Rechner ausgeführt, der umbenannt wurde. • Auf mindestens einem Knoten wird der CMS nicht gehostet. • Sie benennen einen Rechner mit mindestens einem Knoten um. • Die IP-Adresse wird während des Umbenennungsprozesses geändert.	Verwenden Sie den CCM, um den Workflow "Knoten neu erstellen" außer auf dem Knoten, auf dem der CMS gehostet wird, auf allen Knoten durchzuführen, und starten Sie dann alle BI-Plattform-Knoten in der Implementierung neu. Weitere Informationen finden Sie im Kapitel "Verwalten von Knoten".

Nicht vergessen

Nachdem Sie eine Aktion durchgeführt haben, starten Sie die Webanwendung oder den Anwendungsserver neu.

Weitere Informationen

Neuerstellen von Knoten [Seite 411]

10.13.3.2 Webschicht

Gehen Sie beim Umbenennen des Rechners, der den Webanwendungsserver der BI-Plattform hostet, wie folgt vor:

Bedingung	Aktion
Sie ändern den Namen des Rechners, der den BI-Plattform-Webanwendungsserver hostet, und die URL des OpenDocument-Standardviewers enthält einen Webanwendungsserver-Hostnamen.	Melden Sie sich an der CMC an, und aktualisieren Sie die Standardviewer-URL in **Anwendungen** > **CMC** > **Verarbeitungseinstellungen**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Bedingung	Aktion
Sie ändern den Namen des Rechners, der den BI-Plattform-Webanwendungsserver hostet, und die Benutzer greifen über eine URL, die einen Webanwendungsserver-Hostnamen enthält, auf BI-Plattform-Webanwendungen zu.	Bitten Sie die Benutzer, über eine URL, die den neuen Webanwendungsserver-Hostnamen enthält, auf die BI-Plattform-Webanwendungen zuzugreifen.
Sie ändern den Namen des Rechners, der den BI-Plattform-Webanwendungsserver hostet, und webdienstbasierte BI-Plattform-Clients verwenden Webanwendungsserver-Hostnamen in der URL.	Konfigurieren Sie alle webdienstbasierten BI-Plattform-Clients neu, sodass diese den neuen Webanwendungsserver-Hostnamen verwenden.

10.13.3.3 Datenbanken

Beachten Sie folgende optimale Verfahrensweisen, wenn Sie den Rechner umbenennen, auf dem die CMS-Systemdatenbank oder die Audit-Datenbank gehostet wird:

Bedingung	Aktion
Sie möchten die Aktualisierung von IP-Adressen vermeiden.	Verwenden Sie im Datenquellennamen (DSN) den Namen des CMS-Datenbank- oder des Audit-Datenbankrechners.
Die CMS-Datenbank oder die Audit-Datenbank befindet sich auf demselben Host wie der CMS.	Verwenden Sie im DSN `localhost`, um bei einer Änderung des Hostnamens Aktualisierungen zu vermeiden.

CMS-Systemdatenbank

Bedingung	Aktion
Sie benennen einen Rechner um, auf dem die CMS-Systemdatenbank gehostet wird, und verwenden ODBC.	Aktualisieren Sie den DSN der CMS-Datenbank auf den neuen Datenbankserver-Hostnamen.
Sie benennen einen Rechner um, auf dem die CMS-Systemdatenbank gehostet wird, und verwenden einen Nicht-ODBC-Datenbankverbindungstyp.	Aktualisieren Sie die CMS-Datenbank mithilfe des CCM auf jedem Knoten im Cluster auf den neuen Datenbankserver-Hostnamen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Überwachungsdatenbank

Bedingung	Aktion
Sie benennen einen Rechner um, auf dem die Audit-Datenbank gehostet wird, und verwenden ODBC.	Aktualisieren Sie den DSN der Audit-Datenbank so, dass der neue Datenbankserver-Hostname verwendet wird.
Sie benennen einen Rechner um, auf dem die Audit-Datenbank gehostet wird, und verwenden einen Nicht-ODBC-Datenbankverbindungstyp.	Aktualisieren Sie den Datenbankserver-Rechnernamen auf der Registerkarte **Auditing** der CMC auf den neuen Datenbankserver-Hostnamen.

10.13.3.4 File Repository Server

Wenn Sie den Rechner umbenennen, auf dem der FRS-Dateispeicher gehostet wird, aktualisieren Sie den *Input-File-Repository*- und den *Output-File-Repository*-Server auf der Seite "Serververwaltung" der CMC, stellen Sie sicher, dass die Eigenschaften *Dateispeicherverzeichnis* und *Temporäres Verzeichnis* den neuen Dateispeicherpfad verwenden, und starten Sie die Server dann neu.

10.14 Verwenden von 32-Bit- und 64-Bit-Bibliotheken von Drittherstellern mit der BI-Plattform

BI-Plattform-Server setzen sich aus einer Kombination von 32-Bit- und 64-Bit-Prozessen zusammen. Manche Server starten zusätzlich untergeordnete 32-Bit- und 64-Bit-Prozesse. Damit die richtige Version der Drittherstellerbibliotheken (32-Bit- oder 64-Bit-Version) mit den Prozessen der BI-Plattform verwendet wird, müssen Sie separate 32-Bit- und 64-Bit-Umgebungsvariablen auf den Rechnern festlegen, auf denen die BI-Plattform gehostet wird. Anschließend ist eine zusätzliche Umgebungsvariable festzulegen, die eine kommagetrennte Liste der Umgebungsvariablen enthält, die über 32-Bit- und 64-Bit-Versionen verfügen. Wenn die BI-Plattform einen Prozess startet, wird die passende Variable ausgewählt, je nachdem, ob es sich um einen 32-Bit- oder 64-Bit-Prozess handelt.

- **<ERSTE_UMG_VAR>** =Der von 64-Bit-BI-Plattform-Prozessen zu verwendende Wert.
- **<ERSTE_UMG_VAR32>**=Der von 32-Bit-Prozessen zu verwendende Wert.
- **<ZWEITE_UMG_VAR>**=Der von 64-Bit-Prozessen zu verwendende Wert.
- **<ZWEITE_UMG_VAR32>**=Der von 32-Bit-Prozessen zu verwendende Wert.
- BOE_USE_32BIT_ENV_FOR=**<ERSTE_UMG_VAR>**,**<ZWEITE_UMG_VAR>**

Wenn Sie beispielsweise die BI-Plattform und 32-Bit- sowie 64-Bit-Oracle-Clients auf einem AIX-Rechner installiert haben und die LIBPATH-Variable festlegen müssen, legen Sie die folgenden Variablen fest:

- ORACLE_HOME=**<Stammverzeichnis der 64-Bit-Version des Oracle-Clients>**
- ORACLE_HOME32=**<Stammverzeichnis der 32-Bit-Version>**
- LIBPATH=**<Bibliothekspfad der 64-Bit-Version>**
- LIBPATH32=**<Bibliothekspfad der 32-Bit-Version>**

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- BOE_USE_32BIT_ENV_FOR=ORACLE_HOME,LIBPATH

> **Hinweis**
>
> Verwenden Sie unter Linux und Solaris zum Trennen von 32-Bit- und 64-Bit-Pfaden nicht BOE_USE_32BIT_ENV_FOR=LD_LIBRARY_PATH Fügen Sie stattdessen sowohl 32-Bit- als auch 64-Bit-Pfade zu LD_LIBRARY_PATH hinzu.

10.15 Verwalten von Server- und Knotenplatzhaltern

10.15.1 Anzeigen von Serverplatzhaltern

Klicken Sie im Verwaltungsbereich *Server* der CMC mit der rechten Maustaste auf einen Server, und wählen Sie **Platzhalter**.
Im Dialogfeld *Platzhalter* wird eine Liste der Platzhalter für alle Server angezeigt, die sich im selben Cluster wie der von Ihnen ausgewählte Server befinden. Wenn Sie den Wert eines Platzhalters ändern möchten, ändern Sie den Platzhalter für den Knoten.

Weitere Informationen

Server- und Knotenplatzhalter [Seite 1012]

10.15.2 Anzeigen und Bearbeiten der Platzhalter eines Knotens

1. Klicken Sie im Verwaltungsbereich *Server* der Central Management Console mit der rechten Maustaste auf den Knoten, für den Sie die Platzhalter ändern möchten, und wählen Sie **Platzhalter**.
2. Wenn Sie Einstellungen für die Platzhalter bearbeiten möchten, nehmen Sie die entsprechenden Änderungen vor, und klicken Sie auf **Speichern**, um fortzufahren.

Weitere Informationen

Server- und Knotenplatzhalter [Seite 1012]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

11 Verwalten von CMS-Datenbanken (Central Management Server)

11.1 Verwalten von Verbindungen zur CMS-Systemdatenbank

Wenn die CMS-Systemdatenbank, beispielsweise aufgrund eines Hardware- oder Softwarefehlers oder eines Netzwerkproblems, nicht verfügbar ist, wechselt der CMS in den Status "Auf Ressourcen wird gewartet". Wenn die BI-Plattform-Implementierung mehrere CMS enthält, werden nachfolgende Anforderungen von anderen Servern an jeden CMS im Cluster gesendet, der über eine aktive Verbindung zur Systemdatenbank verfügt. Während sich ein CMS im Status "Auf Ressourcen wird gewartet" befindet, werden alle aktuellen Anforderungen, für die kein Datenbankzugriff erforderlich ist, weiterhin verarbeitet. Anforderungen, für die Zugriff auf die CMS-Datenbank erforderlich ist, schlagen jedoch fehl.

Im Status "Auf Ressourcen wird gewartet" versucht ein CMS standardmäßig, die Anzahl der in der Eigenschaft " Angeforderte Systemdatenbankverbindungen" angegebenen Verbindungen regelmäßig wiederherzustellen. Sobald mindestens eine Datenbankverbindung hergestellt ist, synchronisiert der CMS alle erforderlichen Daten, wechselt in den Status "Ausgeführt" und nimmt den normalen Betrieb wieder auf.

In einigen Fällen möchten Sie vielleicht verhindern, dass der CMS eine Verbindung zur Datenbank automatisch wiederherstellt. Beispielsweise, wenn Sie die Integrität der Datenbank überprüfen möchten, bevor Datenbankverbindungen wiederhergestellt werden. Deaktivieren Sie dazu auf der Seite *Eigenschaften* des CMS-Servers die Option **Automatisch Wiederverbindung zur Systemdatenbank herstellen**.

Weitere Informationen

Ändern der Eigenschaften eines Servers [Seite 392]

11.1.1 Auswählen von SQL Anywhere als CMS-Datenbank

Führen Sie folgende Schritte aus, um SQL Anywhere als CMS-Datenbank zu verwenden:

1. Stoppen Sie alle Knoten im System.
2. Führen Sie die entsprechende Anwendung aus:
   - Unter Unix führen Sie `./cmsdbsetup.sh` aus.
   - Starten Sie unter Windows den Central Configuration Manager (CCM).
3. Kopieren Sie die Daten aus der CMS-Standarddatenbank, und wählen Sie SQL Anywhere als Zieldatenbank aus. Weitere Informationen finden Sie unter der zugehörigen Verknüpfung "Kopieren von Daten von einer CMS-Systemdatenbank in eine andere".
4. Aktualisieren Sie in Mehrknotenimplementierungen die CMS-Datenquelle auf jedem Knoten (außer auf dem Knoten, auf den Sie die Datenbank kopieren) auf die neue SQL-Anywhere-Datenbank. Weitere Informationen finden Sie unter der zugehörigen Verknüpfung "Auswählen einer neuen oder bereits vorhandenen CMS-Datenbank".

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

5. Stellen Sie sicher, dass die Implementierung betriebsbereit ist (melden Sie sich beispielsweise an der CMC an, und zeigen Sie einen Bericht an).

Weitere Informationen

Kopieren von Daten von einer CMS-Systemdatenbank in eine andere [Seite 444]
Auswählen einer neuen oder bereits vorhandenen CMS-Datenbank [Seite 439]

11.1.2 Auswählen von SAP HANA als CMS-Datenbank

Führen Sie folgende Schritte aus, um SAP HANA als CMS-Datenbank zu verwenden.

1. Installieren Sie die BI-Plattform mit der CMS-Standarddatenbank.
2. Installieren Sie den SAP-HANA-Client.
3. Erstellen Sie eine Verbindung mit SAP HANA.
   - Prüfen Sie unter Unix die Umgebungsvariable `ODBCINI`. Wenn die Variable vorhanden ist und auf eine vorhandene `odbc.ini`-Datei zeigt, fügen Sie dieser Datei folgende Zeilen hinzu:

     ```
     [ODBC Data Sources]
     NewDB=<New_DB_version>

     [NewDB]
     SERVERNODE=<HANA Server IP address>:<HANA server port #>
     ```

     `<New_DB_version>` ist die SAP-HANA-Version, zum Beispiel “NewDB 1.0”, `<HANA Server IP address>` ist die IP-Adresse des SAP-HANA-Servers, und `<HANA server port #>` ist die Portnummer des SAP-HANA-Servers.

     Wenn die Umgebungsvariable `ODBCINI` nicht vorhanden ist, erstellen Sie eine `odbc.ini`-Datei im Verzeichnis **`<INSTALLVERZ>`**`/sap_bobj/enterprise_xi40/`, fügen der Datei die obigen Zeilen hinzu, und stellen Sie die Umgebungsvariable `ODBCINI` wie folgt ein:

     ```
     ODBCINI=<INSTALLDIR>/sap_bobj/enterprise_xi40/odbc.ini
     ```

   - Unter Windows erstellen Sie eine ODBC-Verbindung mit SAP HANA.

     > **Hinweis**
     >
     > Um ODBC-Verbindungsänderungen vorzunehmen, stellen Sie sicher, dass die 64-Bit-Version des ODBC-Datenquellenadministrators ausgeführt wird: **Start** > **Systemsteuerung** > **Verwaltungstools** > **Datenquellen (ODBC)**.

4. Stellen Sie sicher, dass Verbindungen mit dem SAP-HANA-Server hergestellt werden können.
   - Unter Unix können Sie die Verbindung mit dem SAP-HANA-Server testen, indem Sie den folgenden Befehl ausführen. Die Variablen im folgenden Beispiel verweisen auf die SAP-HANA-Installation:

     ```
     <INSTALLDIR>/odbcreg <SERVER>:<HDBINDEXSERVERPORT> <SYSTEMID> <NONADMINUSER>
     <NONADMINPASSWORD>
     ```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Unter Windows können Sie die SAP-HANA-ODBC-Verbindung mit dem ODBC-Datenquellenadministrator testen.

5. Unter Linux kopieren Sie `libodbcHDB.so` aus dem SAP-HANA-Installationsverzeichnis nach `<INSTALLVERZ>/sap_bobj/enterprise_xi40/<PLATTFORM>`
6. Stoppen Sie alle Knoten im System.
7. Führen Sie die entsprechende Anwendung aus:
   - Unter Unix führen Sie `./cmsdbsetup.sh` aus.
   - Starten Sie unter Windows den Central Configuration Manager (CCM).
8. Kopieren Sie die Daten aus der CMS-Standarddatenbank, und wählen Sie SAP HANA als Zieldatenbank aus. Weitere Informationen finden Sie unter der zugehörigen Verknüpfung "Kopieren von Daten von einer CMS-Systemdatenbank in eine andere".
9. Aktualisieren Sie in Mehrknotenimplementierungen die CMS-Datenquelle auf jedem Knoten (außer auf dem Knoten, auf den Sie die Datenbank kopieren) auf die neue SAP-HANA-Datenbank. Weitere Informationen finden Sie unter der zugehörigen Verknüpfung "Auswählen einer neuen oder bereits vorhandenen CMS-Datenbank".
10. Stellen Sie sicher, dass die Implementierung betriebsbereit ist (melden Sie sich beispielsweise an der CMC an, und zeigen Sie einen Bericht an).

Weitere Informationen

Kopieren von Daten von einer CMS-Systemdatenbank in eine andere [Seite 444]
Auswählen einer neuen oder bereits vorhandenen CMS-Datenbank [Seite 439]

11.2 Auswählen einer neuen oder bereits vorhandenen CMS-Datenbank

Sie können den CCM oder `cmsdbsetup.sh` verwenden, um eine neue oder vorhandene CMS-Systemdatenbank für einen Knoten anzugeben. Die folgenden Schritte sind im Allgemeinen nur selten notwendig:

- Wenn Sie das Kennwort der aktuellen CMS-Systemdatenbank geändert haben, können Sie anhand dieser Schritte die Verbindung mit der aktuellen Datenbank trennen und anschließend wiederherstellen. Wenn Sie dazu aufgefordert werden, können Sie dem CMS das neue Kennwort zuweisen.
- Wenn Sie eine leere Datenbank für die BI-Plattform auswählen und initialisieren möchten, können Sie anhand dieser Schritte diese neue Datenquelle auswählen.
- Wenn nach der Wiederherstellung einer CMS-Systemdatenbank aus gesicherten Daten (unter Verwendung der üblichen Datenbankverwaltungsprogramme und -verfahren) die ursprüngliche Datenbankverbindung ungültig wird, muss der CMS erneut mit der wiederhergestellten Datenbank verbunden werden. (Dies kann zum Beispiel vorkommen, wenn Sie die ursprüngliche CMS-Datenbank auf einem neu installierten Datenbankserver wiederherstellen.)

Hinweis

Falls Sie IBM DB2 als CMS-Datenbank verwenden und von einer älteren Version als 9.5 Fixpack 5 auf Version 9.5 Fixpack 5 oder höher (für die 9.5er-Reihe) aktualisieren, oder falls Sie von einer älteren Version als 9.7

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Fixpack 1 auf Version 9.7 Fixpack 1 oder höher (für die 9.7er Reihe) aktualisieren, wird während des nächsten Neustarts des BI-Plattform-Knotens oder des CMS das CMS-Datenbankschema automatisch vom CMS zur Unterstützung eines HADR-kompatiblen Schemas aktualisiert.

Dieser Vorgang kann längere Zeit in Anspruch nehmen, während der die BI-Plattform nicht zur Verwendung zur Verfügung steht. Unterbrechen Sie den Aktualisierungsprozess nicht, um eine Beschädigung der CMS-Datenbank zu vermeiden. Die CMS-Datenbank sollte vor dem Durchführen dieses Vorgangs gesichert werden. Versuchen Sie nicht, IBM HADR mit einer IBM-DB2-CMS-Datenbank in einer älteren Version als 9.5 Fixpack 5 (für die 9.5er Reihe) oder 9.7 Fixpack 1 (für die 9.7er Reihe) zu verwenden.

Hinweis

Konfigurieren Sie eine BI-Plattform-Installation nicht für die Verwendung einer CMS-Systemdatenbank, die zu einem anderen Cluster gehört – es sei denn, Sie führen einen Systemkopier-Workflow aus.

Wenn die Versionen und Patch-Level der BI-Plattform-Installationen und CMS-Datenbanken, die Installationspfade oder die installierten Komponenten unterschiedlich sind, kann das System beschädigt werden.

Um diese Beschädigung zu vermeiden, sollten Sie keine BI-Inhalte aus einem System in ein anderes migrieren, indem die BI-Plattform-Implementierung auf eine CMS-Datenbank eines anderen BI-Plattform-Systems zeigt, insbesondere eines mit einer anderen Version und einem anderen Patch-Level.

11.2.1 So wählen Sie eine neue oder vorhandene CMS-Datenbank unter Windows aus

1. Verwenden Sie den CCM zum Stoppen des Server Intelligence Agents (SIA).
2. Wählen Sie den SIA aus, und klicken Sie auf die Schaltfläche **CMS-Datenquelle angeben**.
3. Wählen Sie **Datenquelleneinstellungen aktualisieren**, und klicken Sie auf**OK**.
4. Wählen Sie einen Datenbanktreiber aus, und klicken Sie auf **OK**.
5. Diese Schritte hängen vom ausgewählten Verbindungstyp ab:
   - Wenn Sie ODBC ausgewählt haben, wird das Windows-Dialogfeld “Datenquelle auswählen” angezeigt. Wählen Sie die ODBC-Datenquelle aus, die Sie als CMS-Datenbank verwenden möchten, und klicken Sie auf **OK**. (Klicken Sie auf **Neu**, um einen neuen DSN zu konfigurieren.) Wenn Sie dazu aufgefordert werden, geben Sie die Anmeldedaten für die Datenbank ein und klicken auf **OK**.
   - Wenn Sie einen systemeigenen Treiber ausgewählt haben, werden Sie aufgefordert, Servernamen der Datenbank, Anmelde-ID sowie Kennwort einzugeben. Geben Sie diese Informationen ein, und klicken Sie auf **OK**.
6. Geben Sie den Clusterschlüssel an.
7. Starten Sie den Server Intelligence Agent neu.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

11.2.2 So wählen Sie eine neue oder vorhandene CMS-Datenbank unter UNIX aus

Verwenden Sie das Skript `cmsdbsetup.sh`. Weitere Informationen finden Sie im Abschnitt “Unix-Skripte” im Kapitel Befehlszeilenverwaltung des *Administratorhandbuchs für SAP BusinessObjects Business Intelligence*.

1. Führen Sie das Skript `cmsdbsetup.sh` aus (standardmäßig unter **<INSTALLVERZ>**/`sap_bobj/`).
2. Wählen Sie die Aktualisierungsoption (Option 6).
3. Geben Sie den Datenbanktyp der neuen CMS-Datenbank ein, sobald Sie dazu aufgefordert werden.
4. Geben Sie die Datenbankinformationen an (z. B.: Hostname, Benutzername, Kennwort und Clusterschlüssel). Eine Benachrichtigungsmeldung wird angezeigt, nachdem die CMS-Datenbank auf den neuen Speicherort eingestellt wurde.
5. Wenn Sie aufgefordert werden, den Server Intelligence Agent (SIA) neu zu erstellen, geben Sie das Administratorkennwort und die Portnummer an, über die der CMS kommunizieren soll.

> **Hinweis**
>
> Diese Informationen werden nur angefordert, wenn Sie eine leere CMS-Datenbank angeben.

Weitere Informationen

Unix-Skripte [Seite 884]

11.3 Neu erstellen der CMS-Systemdatenbank

Mit diesem Verfahren kann die aktuelle CMS-Systemdatenbank neu erstellt (neu initialisiert) werden. Bevor Sie diese Aufgabe durchführen, sollten Sie alle Daten löschen, die sich bereits in der Datenbank befinden. Dies ist zum Beispiel dann sinnvoll, wenn Sie die BI-Plattform in einer Entwicklungsumgebung zum Entwerfen und Testen eigener, benutzerdefinierter Webanwendungen installiert haben. Sie können die CMS-Systemdatenbank in der Entwicklungsumgebung jeweils neu initialisieren, wenn alle Daten aus dem System gelöscht werden müssen.

> **Achtung**
>
> Indem Sie die in diesem Arbeitsablauf aufgeführten Schritte ausführen, löschen Sie alle in der CMS-Datenbank enthaltenen Daten sowie Objekte wie Berichte und Benutzer. Führen Sie diese Schritte nicht in einer Produktionsumgebung aus.

Es ist äußerst wichtig, alle Serverkonfigurationseinstellungen zu sichern, bevor Sie die CMS-Systemdatenbank neu initialisieren. Da die Serverkonfigurationseinstellungen beim Neuerstellen der Datenbank gelöscht werden, benötigen Sie eine Sicherungskopie, um diese Informationen wiederherzustellen.

Wenn Sie die Systemdatenbank neu erstellen, sollten Ihre vorhandenen Lizenzschlüssel in der Datenbank erhalten bleiben. Wenn Sie jedoch Lizenzschlüssel erneut eingeben müssen, melden Sie sich bei der CMC mit dem

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

standardmäßigen Administratorkonto an. Wechseln Sie zum Verwaltungsbereich "Autorisierung", und geben Sie die Daten auf der Registerkarte "Lizenzschlüssel" ein.

> **Hinweis**
>
> Wenn Sie die CMS-Systemdatenbank neu initialisieren, werden alle Daten in der aktuellen CMS-Systemdatenbank gelöscht. Es empfiehlt sich, die aktuelle Datenbank zu sichern, bevor Sie mit dem Verfahren beginnen. Wenden Sie sich gegebenenfalls an den Datenbankadministrator.

Weitere Informationen

Sichern der Servereinstellungen [Seite 494]

11.3.1 So erstellen Sie die CMS-Systemdatenbank unter Windows neu

1. Verwenden Sie den CCM zum Stoppen des Server Intelligence Agents (SIA).

   > **Hinweis**
   >
   > Bei diesem Verfahren kann der CCM nicht auf einem Remoterechner ausgeführt werden, sondern muss auf einem Rechner mit mindestens einem gültigen Knoten ausgeführt werden. Außerdem müssen die CMS-Binärdateien auf diesem Rechner installiert sein.

2. Klicken Sie mit der rechten Maustaste auf den SIA, und wählen Sie **Eigenschaften**.
3. Wählen Sie im Dialogfeld **Eigenschaften** die Registerkarte *Konfiguration* und klicken auf **Festlegen**.
4. Klicken Sie im Dialogfeld **CMS-Datenbankeinrichtung** auf **Aktuelle Datenquelle erneut erstellen**.

   > **Hinweis**
   >
   > Die Server und Objekte von dem Rechner, auf dem der CCM in Schritt 1 ausgeführt wurde, werden ebenfalls neu erstellt. Es werden jedoch nicht alle Objekte neu erstellt, sondern nur die Schlüsselstandardobjekte. Beispielberichte werden z.B. nicht neu erstellt.

5. Klicken Sie auf **OK** und auf **Ja**, wenn Sie zur Bestätigung aufgefordert werden.
6. Geben Sie das Kennwort für die die CMS-Systemdatenbank ein, und klicken Sie auf **OK**.

   > **Hinweis**
   >
   > Stellen Sie sicher, dass Sie ein neues Administratorkennwort festlegen. Das Administratorkonto hat standardmäßig kein Kennwort.

   Sie werden vom CCM darüber benachrichtigt, wenn das Setup der CMS-Systemdatenbank abgeschlossen ist.
7. Klicken Sie auf **OK**.

   Sie kehren zum CCM zurück.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8. Starten Sie den Server Intelligence Agent neu, und aktivieren Sie die Dienste.

   Der CMS wird beim Start des Server Intelligence Agents mitgestartet. Der CMS schreibt erforderliche Systemdaten in die neu geleerte Datenquelle.
9. Wenn die Implementierung über mehrere Rechner verfügt, erstellen Sie die Knoten auf den anderen Rechnern neu.

11.3.2 So erstellen Sie die CMS-Systemdatenbank unter UNIX neu

Verwenden Sie das Skript `cmsdbsetup.sh`. Weitere Informationen finden Sie im Abschnitt “Unix-Skripte” im Kapitel Befehlszeilenverwaltung des *Administratorhandbuchs für SAP BusinessObjects Business Intelligence*.

1. Führen Sie die Datei `cmsdbsetup.sh` (standardmäßig unter **<INSTALLVERZ>**`/sap_bobj/` aus).
2. Wählen Sie die Option "Neu initialisieren" (Option 5) aus, und bestätigen Sie Ihre Auswahl.
   Das Skript `cmsdbsetup.sh` beginnt mit der Neuerstellung der CMS-Systemdatenbank.
3. Stellen Sie das CMS-Systemdatenbankkennwort bereit
4. Nachdem die Datenbank erstellt wurde, beenden Sie das Skript `cmsdbsetup.sh`.
5. Geben Sie die Datenbankinformationen an (z. B.: Hostname, Benutzername und Kennwort).
   Eine Benachrichtigungsmeldung wird angezeigt, nachdem die CMS-Datenbank auf den neuen Speicherort eingestellt wurde.
6. Wenn Sie aufgefordert werden, den Server Intelligence Agent (SIA) neu zu erstellen, geben Sie das Administratorkennwort und die Portnummer an, über die der CMS kommunizieren soll.

   > **Hinweis**
   >
   > Diese Informationen werden nur angefordert, wenn Sie eine leere CMS-Datenbank angeben.
7. Verwenden Sie im Verzeichnis **<INSTALLVERZ>**`/sap_bobj/` den folgenden Befehl, um den Knoten zu starten.

   ```
   ccm.sh -start <Knotenname>
   ```
8. Aktivieren Sie die Dienste mit folgendem Befehl:

   ```
   ccm.sh -enable all -cms <CMSNAME:PORT> -username administrator -password
   <password >
   ```

   > **Hinweis**
   >
   > Da Sie die CMS-Datenbank gerade neu erstellt haben, ist für das Administratorkennwort kein Eintrag vorhanden.

Weitere Informationen

Unix-Skripte [Seite 884]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

11.4 Kopieren von Daten von einer CMS-Systemdatenbank in eine andere

Sie können mit dem Central Configuration Manager (CCM) oder mit `cmsdbsetupsh` Systemdaten von einem Datenbankserver auf einen anderen kopieren. Wenn Sie z. B. die Datenbank durch eine andere ersetzen möchten, da ein Upgrade der Datenbank oder ein Wechsel des Datenbanktyps ansteht, können Sie den Inhalt der vorhandenen Datenbank in die neue Datenbank kopieren, bevor Sie die vorhandene Datenbank außer Betrieb setzen.

Die Zieldatenbank wird initialisiert, bevor die neuen Daten kopiert werden, damit der gesamte Inhalt der Zieldatenbank dauerhaft gelöscht wird (alle BI-Plattform-Tabellen werden dauerhaft gelöscht und dann neu erstellt). Sobald die Daten kopiert wurden, wird die Zieldatenbank als aktuelle Datenbank für den CMS eingerichtet.

Hinweis

Wenn Sie Benutzer, Gruppen, Ordner und Berichte aus einer früheren Hauptversion der BI-Plattform in die aktuelle Hauptversion importieren möchten, verwenden Sie das Upgrade-Management-Tool. Weitere Informationen finden Sie im *Aktualisierungshandbuch für SAP BI*.

Achtung

Versuchen Sie nie, eine CMS-Datenbank aus einem anderen BI-Plattform-Cluster zu verwenden. Bevor Sie diesen Workflow starten, stellen Sie sicher, dass die Quell-CMS-Datenbank mit diesem BI-Plattform-Cluster und nicht mit einem anderen BI-Plattform-Cluster verwendet wurde.

Achtung

Versuchen Sie nie, mithilfe des Workflows zum Kopieren einer CMS-Datenbank ein Upgrade vorzunehmen. Der Workflow zum Kopieren einer CMS-Datenbank dient der Verschiebung einer CMS-Datenbank von einem Datenbankserver auf einen anderen Datenbankserver. Der Workflow dient nicht der Aktualisierung einer CMS-Datenbank. Bevor Sie diesen Workflow starten, stellen Sie sicher, dass die Quell-CMS-Datenbank mit diesem BI-Plattform-Cluster verwendet wurde und dieselbe Version und dasselbe Patch-Level wie die aktuelle BI-Plattform-Installation aufweist.

11.4.1 Vorbereitung für das Kopieren einer CMS-Systemdatenbank

Schalten Sie vor dem Kopieren einer CMS-Systemdatenbank die Quell- und Zielumgebung offline, indem alle Server deaktiviert und anschließend gestoppt werden. Sichern Sie beide CMS-Datenbanken sowie die Root-Verzeichnisse, die von allen Input und Output File Repository Server verwendet werden. Kontaktieren Sie gegebenenfalls den Datenbankadministrator.

Stellen Sie sicher, dass Sie über ein Datenbank-Benutzerkonto mit der Berechtigung zum Lesen aller Daten in der Quelldatenbank und mit den Rechten "Erstellen", "Löschen" und "Aktualisieren" in der Zieldatenbank verfügen. Vergewissern Sie sich weiterhin, dass Sie von dem CMS-Rechner, dessen Datenbank Sie ersetzen, eine

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Verbindung mit beiden Datenbanken (je nach Konfiguration über eine Datenbank-Client-Software oder ODBC) herstellen können.

Wenn Sie eine CMS-Datenbank von ihrem aktuellen Speicherort auf einen anderen Datenbankserver kopieren, ist Ihre aktuelle CMS-Datenbank die Quellumgebung. Deren Inhalt wird in die Zieldatenbank kopiert, die als aktive Datenbank für den aktuellen CMS eingerichtet wird: Genauso sollten Sie vorgehen, wenn Sie die standardmäßige CMS-Datenbank von der vorhandenen Standarddatenbank auf einen dedizierten Datenbankserver, z.B. Microsoft SQL Server, Informix, Oracle, DB2 oder Sybase, verlegen möchten. Melden Sie sich mit einem Administratorkonto beim Rechner an, auf dem der CMS ausgeführt wird, dessen Datenbank Sie verschieben möchten.

> **Hinweis**
>
> Wenn Sie Daten in eine andere Datenbank kopieren, wird die Zieldatenbank initialisiert, bevor die neuen Daten hinein kopiert werden. Dies bedeutet, dass die BI-Plattform-Systemtabellen erstellt werden, wenn sie noch nicht in der Zieldatenbank enthalten sind. Wenn die Zieldatenbank Systemtabellen von der BI-Plattform enthält, werden die Tabellen dauerhaft gelöscht, und es werden neue Systemtabellen erstellt. Die Daten aus der Quelldatenbank werden in die neuen Tabellen kopiert. Andere Tabellen in der Datenbank bleiben davon unberührt.

> **Hinweis**
>
> Wenn Sie eine CMS-Systemdatenbank in eine MaxDB-Zieldatenbank kopieren, müssen Sie sicherstellen, dass der Pfad zum MaxDB-Client zur Umgebungsvariablen **`<PATH>`** hinzugefügt wurde. Beispiel: `;C:\Programme\sdb\MAXDB1\pgm`.

11.4.2 Kopieren einer CMS-Systemdatenbank unter Windows

Bevor Sie den Inhalt der CMS-Datenbank kopieren, sollten Sie sicherstellen, dass Sie sich bei der Zieldatenbank mit einem Konto anmelden können, dem Berechtigungen zum Hinzufügen oder Löschen von Tabellen sowie zum Hinzufügen, Löschen oder Ändern von Daten in diesen Tabellen zugewiesen wurden.

1. Öffnen Sie den Central Configuration Manager (CCM), und stoppen Sie den Server Intelligence Agent (SIA).
2. Klicken Sie mit der rechten Maustaste auf den SIA, und wählen Sie **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Festlegen**.
4. Klicken Sie auf **Kopieren** und anschließend auf **OK**.
5. Wählen Sie den Datenbanktyp der CMS-Quelldatenbank aus, und geben Sie die Datenbankinformationen an (einschließlich Hostname, Benutzername und Kennwort).
6. Wählen Sie den Datenbanktyp der CMS-Zieldatenbank aus, und geben Sie die Datenbankinformationen an (einschließlich Hostname, Benutzername und Kennwort).
7. Klicken Sie nach Beendigung des Kopiervorgangs auf **OK**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

11.4.3 Kopieren von Daten von einer CMS-Systemdatenbank unter UNIX

Bevor Sie den Inhalt der CMS-Datenbank kopieren, sollten Sie sicherstellen, dass Sie sich bei der Zieldatenbank mit einem Konto anmelden können, dem Berechtigungen zum Hinzufügen oder Löschen von Tabellen sowie zum Hinzufügen, Löschen oder Ändern von Daten in diesen Tabellen zugewiesen wurden.

> **Hinweis**
>
> Unter UNIX ist eine direkte Migration von einer Quellumgebung mit einer ODBC-Verbindung mit der CMS-Datenbank nicht möglich. Wenn für die CMS-Quelldatenbank ODBC verwendet wird, muss das System zuerst auf einen unterstützten systemeigenen Treiber aktualisiert werden.

1. Stoppen Sie den CMS, indem Sie folgenden Befehl eingeben:

   ```
   ./ccm.sh -stop <Knotenname>
   ```

2. Führen Sie die Datei `cmsdbsetup.sh` (standardmäßig unter **<INSTALLVERZ>**`/sap_bobj/` aus).
3. Wählen Sie die Option “Kopieren” (Option 4) aus, und bestätigen Sie Ihre Auswahl.
4. Wählen Sie den Datenbanktyp der CMS-Quelldatenbank aus, und geben Sie die Datenbankinformationen an (einschließlich Hostname, Benutzername und Kennwort).
5. Wählen Sie den Datenbanktyp der CMS-Zieldatenbank aus, und geben Sie die Datenbankinformationen an (einschließlich Hostname, Benutzername und Kennwort).
   Die CMS-Datenbank wird auf den Zielrechner kopiert. Sie erhalten eine Meldung, sobald der Kopiervorgang abgeschlossen ist.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12 Verwalten von Web Application Container Servern (WACS)

12.1 WACS

12.1.1 Web Application Container Server (WACS)

Web Application Container Server (WACS) bieten eine Plattform zum Hosten mehrerer Webanwendungen von SAP BusinessObjects Business Intelligence. Beispielsweise kann eine Central Management Console (CMC) auf einem WACS gehostet werden.

WACS vereinfachen die Systemadministration, indem mehrere Arbeitsabläufe entfernt werden, die zuvor zur Konfiguration von Anwendungsservern und zur Bereitstellung von Webanwendungen erforderlich waren, und eine vereinfachte, konsistente Verwaltungsoberfläche bereitgestellt wird.

Webanwendungen werden automatisch auf dem WACS bereitgestellt. WACS untersützt keine manuelle oder WDeploy-Implementierung von BI-Plattform- oder externen Webanwendungen.

12.1.1.1 Brauche ich einen WACS?

Wenn Sie zum Hosten Ihrer SAP-BusinessObjects-Webanwendungen keinen Java-Anwendungsserver verwenden möchten, können Sie sie auf dem WACS hosten.

Wenn Sie einen unterstützten Java-Anwendungsserver zur Implementierung von BI-Plattform-Webanwendungen verwenden möchten oder die BI-Plattform auf einem UNIX-System installieren, muss kein WACS installiert und verwendet werden.

12.1.1.2 Welche Vorteile bieten WACS?

Das Hosten der CMC auf einem WACS bietet Ihnen eine Reihe von Vorteilen:

- Der WACS erfordert nur ein Minimum an Installations-, Wartungs- und Konfigurationsschritten.
- Alle gehosteten Anwendungen werden vorab auf einem WACS implementiert, sodass keine zusätzlichen manuellen Schritte erforderlich sind.
- WACS wird von SAP unterstützt.
- Die Verwendung eines WACS setzt keine Kenntnisse in der Verwaltung und Wartung eines Java-Anwendungsservers voraus.
- Der WACS bietet eine Verwaltungsoberfläche, die mit der anderer BI-Plattform-Server übereinstimmt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12.1.1.3 Allgemeine Aufgaben

Aufgabe	Beschreibung	Thema
Wie steigere ich die Leistung von Webanwendungen oder Webdiensten, die auf dem WACS gehostet werden?	Sie können die Leistung von Webanwendungen oder Webdiensten optimieren, indem Sie den WACS auf mehreren Rechnern installieren.	• *Hinzufügen oder Entfernen zusätzlicher WACS in einer Implementierung* [Seite 450] • *Klonen eines Web Application Container Servers* [Seite 452]
Wie verbessere ich die Verfügbarkeit meiner Webschicht?	Erstellen Sie einen zusätzlichen WACS in der Implementierung, sodass die Verarbeitung von Anforderungen von einem anderen Server übernommen werden kann, falls auf einem Server Hardware- oder Softwarefehler auftreten.	*Hinzufügen oder Entfernen zusätzlicher WACS in einer Implementierung* [Seite 450]
Wie erstelle ich eine Umgebung, in der eine falsch konfigurierte CMC leicht wiederhergestellt werden kann?	Erstellen Sie einen zweiten, gestoppten WACS, und verwenden Sie ihn zum Festlegen einer Konfigurationsvorlage. Falls sich der primäre WACS als falsch konfiguriert herausstellt, verwenden Sie entweder den zweiten WACS, bis Sie den ersten Server konfigurieren, oder wenden die Konfigurationsvorlage auf den ersten Server an.	*Hinzufügen oder Entfernen zusätzlicher WACS in einer Implementierung* [Seite 450]
Wie verbessere ich die Sicherheit der Kommunikation zwischen Clients und WACS?	Konfigurieren Sie HTTPS auf dem WACS.	• *Konfigurieren von HTTPS/SSL* [Seite 455] • *Verwenden von WACS mit Firewalls* [Seite 480]
Wie verbessere ich die Sicherheit der Kommunikation zwischen dem WACS und anderen BI-Plattform-Servern in der Implementierung?	Konfigurieren Sie die SSL-Kommunikation zwischen dem WACS und anderen BI-Plattform-Servern in der Implementierung.	• *Konfigurieren von Servern für SSL* [Seite 174] • *Verwenden von WACS mit Firewalls* [Seite 480]
Kann ich den WACS mit HTTPS und einem Reverseproxy verwenden?	Sie können den WACS mit HTTPS und einem Reverseproxy verwenden, wenn Sie zwei WACS erstellen und beide Server mit HTTPS konfigurieren. Verwenden Sie den ersten WACS für die Kommunikation innerhalb des internen Netzwerks und den anderen WACS für die Kommunikation mit einem externen Netzwerk über einen Reverseproxy.	*Konfigurieren des WACS für die Unterstützung von HTTPS mit einem Reverseproxy* [Seite 479]
Wie kann ich den WACS in die IT-Umgebung integrieren?	Der WACS kann in einer IT-Umgebung mit vorhandenen Webservern, Hardwaremodulen für den Lastausgleich, Reverseproxys und Firewalls implementiert werden.	• *Verwenden des WACS mit anderen Webservern* [Seite 478] • *Verwenden von WACS mit einem Lastausgleichsmodul* [Seite 478]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Aufgabe	Beschreibung	Thema
		• *Verwenden eines WACS mit einem Reverse Proxy* [Seite 479] • *Verwenden von WACS mit Firewalls* [Seite 480]
Wie setze ich den WACS in einer Implementierung mit Lastausgleich ein?	Sie können den WACS in einer Implementierung einsetzen, in denen ein Hardwaremodul für den Lastausgleich verwendet wird. Der WACS selbst kann nicht als Lastausgleichsmodul verwendet werden.	*Verwenden von WACS mit einem Lastausgleichsmodul* [Seite 478]
Kann ich den WACS in einer Umgebung mit einem Reverseproxy verwenden?	Sie können den WACS in einer Implementierung einsetzen, in der ein Reverseproxy verwendet wird. Der WACS selbst kann nicht als Reverseproxy verwendet werden.	*Verwenden eines WACS mit einem Reverse Proxy* [Seite 479]
Wie behebe ich Fehler auf meinen WACS-Servern?	Wenn Sie die Ursachen/Gründe für eine geringe WACS-Leistung herausfinden möchten, können Sie die Protokolldateien und Systemmetriken einsehen.	• *Konfiguration der Ablaufverfolgung auf einem WACS* [Seite 482] • *So zeigen Sie die Servermetrik an* [Seite 482]
Ich kann über einen bestimmten Port keine Seiten aufrufen. Wo liegt das Problem?	Wenn Sie keine Verbindung zu einem WACS herstellen können, kann dies unterschiedliche Gründe haben. Überprüfen Sie Folgendes: • Die HTTP-, HTTP über Proxy- und HTTPS-Ports, die Sie für den WACS angegeben haben, dürfen nicht von anderen Anwendungen belegt sein. • Dem WACS wurde genügend Arbeitsspeicher zugewiesen. • Der WACS muss genügend gleichzeitige Anforderungen bedienen. • Stellen Sie ggf. die Systemstandardwerte für den WACS wieder her.	• *So lösen Sie HTTP-Portkonflikte* [Seite 483] • *Ändern der Arbeitsspeichereinstellungen* [Seite 484] • *Ändern der Anzahl gleichzeitiger Anforderungen* [Seite 484] • *Wiederherstellen der Systemstandardwerte* [Seite 485]
Wie konfiguriere ich die Eigenschaften von Webanwendungen, die auf dem WACS gehostet werden?	Das Verfahren zum Konfigurieren der Eigenschaften für Webanwendungen hängt von der jeweiligen Eigenschaft und der Webanwendung ab. Weitere Informationen finden Sie im Abschnitt " Konfigurieren von Webanwendungseigenschaften" in diesem Kapitel.	*Konfigurieren von Webanwendungseigenschaften* [Seite 481]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Aufgabe	Beschreibung	Thema
Wo finde ich eine Liste der WACS-Eigenschaften?	Im Abschnitt "Servereigenschaften (Anhang)" dieses Handbuchs finden Sie eine Liste der WACS-Eigenschaften.	*Kerndienste-Eigenschaften* [Seite 950]

12.1.2 Hinzufügen oder Entfernen zusätzlicher WACS in einer Implementierung

Das Hinzufügen zusätzlicher WACS zur Implementierung kann folgende Vorteile haben:

- Schnellere Wiederherstellung von einem falsch konfigurierten Server
- Höhere Serververfügbarkeit
- Besserer Lastausgleich
- Bessere Gesamtleistung

Es gibt drei Möglichkeiten, der Implementierung zusätzliche WACS hinzuzufügen:

- Installieren von WACS auf einem Rechner
- Erstellen eines neuen WACS
- Klonen eines WACS

> **Hinweis**
>
> Aufgrund der hohen Ressourcenauslastung wird empfohlen, jeweils nur einen WACS auf demselben Rechner auszuführen. Auf einem Rechner können mehrere WACS bereitgestellt, jedoch nur einer ausgeführt werden, damit bei einem fehlerhaft konfigurierten WACS eine Wiederherstellung möglich ist.

12.1.2.1 Installieren von WACS

Das Installieren von WACS auf unterschiedlichen Rechnern kann Ihrer Implementierung höhere Leistung, besseren Lastausgleich und höhere Serververfügbarkeit bringen. Wenn Ihre Implementierung mehrere WACS auf separaten Rechnern umfasst, wird die Verfügbarkeit der Webanwendungen und Webdienste nicht durch Hardware- oder Softwareausfälle auf einem bestimmten Rechner beeinträchtigt, da die Diensts vom anderen WACS weiterhin bereitgestellt werden.

Sie können einen Web Application Container Server mit dem Installationsprogramm der BI-Plattform installieren. Sie können WACS auf zwei Arten installieren:

- Wählen Sie bei einer vollständigen Installation auf dem Bildschirm *Java-Webanwendungsserver auswählen* die Option **Web Application Container Server installieren und Webanwendungen automatisch implementieren** aus.

  Wenn Sie in einer Neuinstallation einen Java-Anwendungsserver auswählen, wird kein WACS installiert.
- In einer benutzerdefinierten/erweiterten Installation können Sie im Bildschirm *Komponenten auswählen* die Installation eines WACS auswählen, indem Sie **Server** > **Plattformdienste** aufklappen und **Web Application Container Server** auswählen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wenn Sie einen WACS installieren, erstellt das Installationsprogramm automatisch einen Server mit dem Namen `<KNOTEN>.WebApplicationContainerServer`, wobei `<KNOTEN>` für den Namen des Knotens steht. Die Webanwendungen und Webdienste der BI-Plattform werden dann auf diesem Server implementiert. Zur Bereitstellung oder Konfiguration der CMC sind keine manuellen Schritte erforderlich. Das System ist sofort einsatzbereit.

Wenn Sie einen WACS installieren, werden Sie vom Installationsprogramm aufgefordert, eine HTTP-Portnummer für WACS anzugeben. Geben Sie eine nicht verwendete Portnummer an. Der Standardport ist 6405. Wenn Sie beabsichtigen, Benutzern von außerhalb der Firewall eine Verbindung zum WACS zu ermöglichen, muss der HTTP-Port des Servers in der Firewall geöffnet sein.

WACS werden nur auf Windows-Betriebssystemen unterstützt.

> **Hinweis**
>
> Die vom WACS gehosteten Webanwendungen werden automatisch implementiert, wenn Sie den WACS installieren oder wenn Sie Aktualisierungen oder Hotfixes auf den WACS oder vom WACS gehostete Webanwendungen anwenden. Die Implementierung der Webanwendungen dauert einige Minuten. Der WACS befindet sich so lange im "Initialisierungszustand", bis die Implementierung der Webanwendungen abgeschlossen ist. Benutzer können erst auf die auf dem WACS gehosteten Webanwendungen zugreifen, nachdem die Webanwendungen vollständig implementiert wurden. Stoppen Sie den Server erst nach Ende der Erstimplementierung. Sie können den Serverzustand des WACS über den Central Configuration Manager (CCM) einsehen.
>
> Diese Verzögerung tritt nur auf, wenn der WACS nach der Installation erstmalig gestartet oder Aktualisierungen auf ihn angewendet werden. Bei nachfolgenden WACS-Neustarts findet keine Verzögerung statt.
>
> Webanwendungen können nicht manuell auf einem WACS-Server implementiert werden. Sie können Webanwendungen nicht mit WDeploy auf einem WACS implementieren.

12.1.2.2 Hinzufügen eines neuen Web Application Container Servers

> **Hinweis**
>
> Aufgrund der hohen Ressourcenauslastung wird empfohlen, jeweils nur einen WACS auf demselben Rechner auszuführen. Auf einem Rechner können mehrere WACS bereitgestellt, jedoch nur einer ausgeführt werden, damit bei einem fehlerhaft konfigurierten WACS eine Wiederherstellung möglich ist.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Wählen Sie **Verwalten** > **Neu** > **Neuer Server**.
   Das Dialogfeld *Neuen Server erstellen* wird angezeigt.
3. Wählen Sie aus der Liste **Dienstkategorie** den Eintrag **Kerndienste** aus.
4. Wählen Sie in der Liste **Dienst auswählen** die Dienste aus, die vom WACS gehostet werden sollen, und klicken Sie auf **Weiter**.
   - Wenn auf dem WACS Webanwendungen wie die CMC, BI-Launchpad oder OpenDocument gehostet werden sollen, wählen Sie **BOE-Webanwendungsdienst**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Wenn auf dem WACS Webdienste wie Live Office oder Query as a Web Service (QaaWS) gehostet werden sollen, wählen Sie **Web Services SDK und QaaWS** aus.
- Wenn auf dem WACS Business Process BI-Webdienste gehostet werden sollen, wählen Sie **Business Process BI-Webdienst**.

5. Wählen Sie im nächsten Bildschirm *Neuen Server erstellen* alle zusätzlichen Dienste aus, die der WACS hosten soll, und klicken Sie auf **Weiter**.
6. Wählen Sie im nächsten Bildschirm *Neuen Server erstellen* einen Knoten aus, dem der Server hinzugefügt werden soll, geben Sie einen Servernamen und eine Beschreibung für den Server ein, und klicken Sie auf **Erstellen**.

   > **Hinweis**
   >
   > In der Liste **Knoten** werden nur diejenigen Knoten angezeigt, auf denen WACS installiert sind.

7. Doppelklicken Sie im Bildschirm *Server* auf den neu erstellten WACS.
   Der Bildschirm *Eigenschaften* wird angezeigt.
8. Wenn der WACS bei einem Neustart des Systems nicht automatisch gestartet werden soll, stellen Sie im Bereich *Allgemeine Einstellungen* sicher, dass das Kontrollkästchen **Diesen Server beim Start des Server Intelligence Agents automatisch starten** deaktiviert ist.
9. Klicken Sie auf **Speichern und schließen.**

Ein neuer WACS wird erstellt. Die standardmäßigen Einstellungen und Eigenschaften werden auf den Server angewendet.

12.1.2.3 Klonen eines Web Application Container Servers

Alternativ zum Hinzufügen eines neuen WACS zur Implementierung können Sie einen WACS auch auf demselben Rechner oder auf einem anderen Rechner klonen. Beim Hinzufügen eines neuen WACS wird ein Server mit Standardeinstellungen erstellt. Durch das Klonen eines WACS werden die Einstellungen des Quell-WACS auf den neuen WACS angewendet.

Server können nur auf Rechnern geklont werden, auf denen bereits ein WACS installiert ist.

> **Hinweis**
>
> Aufgrund der hohen Ressourcenauslastung wird empfohlen, jeweils nur einen WACS auf demselben Rechner auszuführen. Auf einem Rechner können mehrere WACS bereitgestellt, jedoch nur einer ausgeführt werden, damit bei einem fehlerhaft konfigurierten WACS eine Wiederherstellung möglich ist.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Wählen Sie den zu klonenden WACS aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Server klonen**.

   Im Bildschirm *Server klonen* wird eine Liste der in der Implementierung enthaltenen Knoten angezeigt, auf denen der WACS geklont werden kann. In der Liste **Für Knoten klonen** werden nur diejenigen Knoten angezeigt, auf denen ein WACS installiert ist.
3. Geben Sie im Bildschirm *Server klonen* einen neuen Servernamen ein, wählen Sie den Knoten aus, auf dem der Server geklont werden soll, und klicken Sie auf **OK**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ein neuer WACS wird erstellt. Der neue Server enthält dieselben Dienste wie der Server, von dem er geklont wurde. Der neue Server und die auf ihm gehosteten Dienste weisen abgesehen vom Servernamen dieselben Einstellungen auf wie der Server, von dem geklont wurde.

> **Hinweis**
>
> Wenn Sie einen WACS auf demselben Rechner geklont haben, können Portkonflikte bei dem WACS auftreten, von dem geklont wurde. In diesem Fall müssen die Portnummern der neu geklonten WACS-Instanz geändert werden.

Weitere Informationen

So lösen Sie HTTP-Portkonflikte [Seite 483]

12.1.2.4 Löschen von WACS-Servern aus der Implementierung

Sie können einen WACS nur löschen, wenn auf ihm nicht die CMC für Sie bereitstellt wird. Wenn Sie einen WACS aus Ihrer Implementierung löschen möchten, melden Sie sich von einem anderen WACS oder Java-Anwendungsserver bei einer CMC an. Sie können keinen WACS löschen, von dem derzeit die CMC für Sie bereitgestellt wird.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Stoppen Sie den zu löschenden Server, indem Sie mit der rechten Maustaste auf den Server klicken und dann auf **Server stoppen** klicken.
3. Klicken Sie mit der rechten Maustaste auf den Server, und wählen Sie **Löschen**.
4. Wenn Sie zum Bestätigen aufgefordert werden, klicken Sie auf **OK**.

12.1.3 Hinzufügen oder Entfernen von Diensten auf dem WACS

12.1.3.1 Hinzufügen einer Webanwendung oder eines Webdiensts zu einem WACS

Wenn Sie weitere Webanwendungen oder Webdienste von der BI-Plattform zu einem WACS hinzufügen möchten, müssen Sie den WACS stoppen. Deshalb benötigen Sie mindestens eine zusätzliche CMC, die auf einem WACS in Ihrer Implementierung gehostet wird und die einen BOE-Webanwendungsdienst bereitstellt, während Sie den anderen WACS stoppen und ihm einen Dienst hinzufügen.

Wenn Sie einen Dienst zum WACS hinzufügen, wird der Dienst automatisch auf dem WACS implementiert, wenn der Server neu gestartet wird.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den WACS, dem Sie den Dienst hinzufügen möchten, und lassen Sie die Eigenschaften des Servers anzeigen, um sicherzustellen, dass der hinzuzufügende Dienst noch nicht vorhanden ist.
3. Klicken Sie auf **Abbrechen**, um zum Bildschirm *Server* zurückzukehren.
4. Stoppen Sie den Server, indem Sie mit der rechten Maustaste auf den Server klicken und **Server stoppen** auswählen.

   Wenn Sie versuchen, den WACS zu stoppen, von dem die CMC derzeit für Sie bereitgestellt wird, wird eine Warnmeldung angezeigt. Fahren Sie erst fort, wenn mindestens ein zusätzlicher BOE-Webanwendungsdienst auf einem anderen WACS in der Implementierung ausgeführt wird. Klicken Sie in diesem Fall auf **OK**, melden Sie sich bei einem anderen WACS an, und starten Sie dieses Verfahren neu.
5. Klicken Sie mit der rechten Maustaste auf den Server, und wählen Sie **Dienste auswählen**.
   Das Dialogfeld *Dienste auswählen* wird angezeigt.
6. Wählen Sie den dem Server hinzuzufügenden Dienst aus, fügen Sie ihn dem Server hinzu, indem Sie auf **>** klicken, und klicken Sie auf **OK**.
7. Starten Sie den WACS, indem Sie mit der rechten Maustaste auf den Server klicken und **Server starten** auswählen.

Der Service wird dem WACS hinzugefügt. Die Standardeinstellungen und -eigenschaften für den Dienst werden angewendet.

12.1.3.2 Entfernen einer Webanwendung oder eines Webdiensts von einem WACS

Um eine Webanwendung oder einen Webdienst von einem WACS zu entfernen, melden Sie sich bei einer CMC auf einem anderen WACS oder bei einem Java-Anwendungsserver an. Sie können keinen WACS stoppen, von dem derzeit die CMC für Sie bereitgestellt wird.

Der letzte Dienst auf einem WACS kann nicht gelöscht werden. Wenn Sie einen Webdienst von einem WACS entfernen, muss folglich sichergestellt werden, dass der Server mindestens einen weiteren Dienst hostet.

Wenn Sie den letzten Dienst von einem WACS entfernen möchten, löschen Sie den WACS selbst.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den WACS, von dem Sie den Dienst entfernen möchten, und lassen Sie die Eigenschaften des Servers anzeigen, um sicherzustellen, dass der zu entfernende Dienst vorhanden ist.
3. Klicken Sie auf **Abbrechen**, um zum Bildschirm *Server* zurückzukehren.
4. Stoppen Sie den WACS, indem Sie mit der rechten Maustaste auf den Server klicken und **Server stoppen** auswählen.

   Wenn Sie versuchen, den WACS zu stoppen, von dem die CMC derzeit für Sie bereitgestellt wird, wird eine Warnmeldung angezeigt. Fahren Sie erst fort, wenn mindestens ein zusätzlicher BOE-Webanwendungsdienst auf einem anderen WACS in der Implementierung ausgeführt wird. Klicken Sie in diesem Fall auf **OK**, melden Sie sich bei einem anderen WACS an, und starten Sie dieses Verfahren neu.
5. Klicken Sie mit der rechten Maustaste auf den WACS, und wählen Sie **Dienste auswählen**.
   Das Dialogfeld *Dienste auswählen* wird angezeigt.
6. Wählen Sie den zu entfernenden Dienst aus, und klicken Sie auf **<** und anschließend auf **OK**.
7. Starten Sie den WACS, indem Sie mit der rechten Maustaste auf den Server klicken und **Server starten** auswählen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Der Dienst wird vom WACS entfernt.

12.1.4 Konfigurieren von HTTPS/SSL

Sie können das SSL-Protokoll (Secure Sockets Layer) und HTTP für die gesamte Netzwerkkommunikation zwischen Clients und WACS in Ihrer BI-Plattform-Implementierung verwenden. Durch SSL/HTTPS wird der Netzwerkdatenverkehr verschlüsselt und die Sicherheit optimiert.

Es gibt zwei Arten von SSL:

- SSL wird zwischen BI-Plattform-Servern, einschließlich WACS, und anderen BI-Plattform-Servern in der Implementierung verwendet. Dies wird als CORBA SSL bezeichnet. Informationen zur Verwendung von SSL zwischen den BI-Plattform-Servern in Ihrer Implementierung finden Sie im Abschnitt "Erläuterung der Kommunikation zwischen BI-Plattform-Komponenten" des Kapitels "Arbeiten mit Firewalls" im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.
- HTTP over SSL findet zwischen WACS und Clients (z.B. Browsern) statt, die mit WACS kommunizieren.

> **Hinweis**
>
> Wenn Sie einen WACS in einer Implementierung mit einem Proxy oder Reverse Proxy bereitstellen und SSL zum Sichern der Netzwerkkommunikation in Ihrer Implementierung verwenden möchten, erstellen Sie zwei WACS. Weitere Informationen finden Sie unter *Verwenden von WACS mit einem Reverseproxy*.

Führen Sie zur Konfiguration von HTTPS/SSL auf einem WACS folgende Schritte aus:

- Erstellen oder Abrufen eines PKCS12-Zertifikatspeichers oder JKS-Keystores, der Ihre Zertifikate und privaten Schlüssel enthält. Sie können Microsoft Internet-Informationsdienste (IIS) und die Microsoft Management Console (MMC) zum Generieren einer PKCS12-Datei oder "openssl" bzw. das Java-Befehlszeilentool "keytool" zum Generieren einer Keystore-Datei verwenden.
- Wenn nur bestimmte Clients eine Verbindung zu einem WACS herstellen sollen, muss eine Datei mit einer Zertifikatvertrauensliste erstellt werden.
- Wenn Sie über einen Zertifikatspeicher und, falls erforderlich, über eine Datei mit einer Zertifikatvertrauensliste verfügen, kopieren Sie die Dateien auf den WACS-Rechner.
- Konfigurieren Sie HTTPS auf dem WACS.

Weitere Informationen

Erläuterung der Kommunikation zwischen BI-Plattform-Komponenten [Seite 183]
Verwenden eines WACS mit einem Reverse Proxy [Seite 479]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12.1.4.1 So generieren Sie einen PKCS12-Zertifikatdateispeicher

Es gibt verschiedene Möglichkeiten und unterschiedliche Tools, um PKCS12-Zertifikatdateispeicher oder Java-Keystores zu generieren. Welche Methode Sie verwenden, hängt von den Tools ab, auf die Sie Zugriff haben und mit denen Sie vertraut sind.

In diesem Beispiel wird veranschaulicht, wie Sie mithilfe der Microsoft-Internet-Informationsdienste (IIS) und der Microsoft Management Console (MMC) für Windows Server 2008 eine PKCS12-Datei generieren.

1. Melden Sie sich als Administrator bei dem Rechner an, auf dem der WACS gehostet wird.
2. Fordern Sie in IIS ein Zertifikat von der Zertifizierungsstelle an. Weitere Informationen finden Sie in der IIS-Hilfe.
3. Starten Sie die MMC, indem Sie auf **Start** > **Ausführen** klicken, `mmc.exe` eingeben und auf **OK** klicken.
4. Fügen Sie der MMC das Snap-In "Zertifikate" hinzu:
   a) Klicken Sie im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
      Der Bildschirm *Snap-In hinzufügen/entfernen* wird angezeigt.
   b) Wählen Sie in der Liste *Verfügbare Snap-Ins* die Option **Zertifikate** aus, und klicken Sie auf **Hinzufügen**.
   c) Wählen Sie **Computerkonto**, und klicken Sie auf **Weiter**.
   d) Wählen Sie **Lokaler Computer**, und klicken Sie auf **Fertig stellen**.
   e) Klicken Sie auf **OK**.

   Das Snap-In "Zertifikate" wird der MMC hinzugefügt.
5. Erweitern Sie in der MMC die Option **Zertifikate**, und wählen Sie das gewünschte Zertifikat aus.
6. Wählen Sie im Menü **Aktion** die Option **Alle Aufgaben** > **Exportieren**.
   Der *Zertifikatexport-Assistent* wird gestartet.
7. Klicken Sie auf **Weiter**.
8. Aktivieren Sie **Ja, privaten Schlüssel exportieren**, und klicken Sie auf **Weiter**.
9. Aktivieren Sie **Privater Informationsaustausch – PKCS #12 (.PFX)**, und klicken Sie auf **Weiter**.
10. Geben Sie das Kennwort ein, das Sie beim Erstellen des Zertifikats verwendet haben, und klicken Sie auf **Weiter**. Geben Sie dieses Kennwort im Feld **Zugangskennwort für den privaten Schlüssel** ein, wenn Sie HTTPS für den WACS konfigurieren.

Ein PKCS12-Zertifikatdateispeicher wird erstellt.

12.1.4.2 So generieren Sie eine Zertifikatvertrauensliste

1. Melden Sie sich als Administrator bei dem Rechner an, auf dem der WACS gehostet wird.
2. Starten Sie die Microsoft Management Console (MMC).
3. Fügen Sie das Snap-In für Internet-Informationsdienste hinzu:
   a) Klicken Sie im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
   b) Wählen Sie in der Liste *Verfügbare Snap-Ins* die Option **Internet-Informationsdienstemanager (IIS)**, und klicken Sie auf **Hinzufügen**.
   c) Klicken Sie auf **OK**.
      Das IIS-Snap-In wird der MMC hinzugefügt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Führen Sie die hier beschriebenen Schritte aus, um eine Zertifikatvertrauensliste zu erstellen: *http://www.iis.net/learn/install/installing-iis-7/compatibility-and-feature-requirements-for-windows-vista#NoWizard* .

12.1.4.3 Konfigurieren von HTTPS/SSL

Bevor Sie HTTPS/SSL auf dem WACS konfigurieren, sollten Sie sicherstellen, dass Sie bereits eine PKCS12-Datei oder einen JKS-Keystore erstellt und die Datei auf den Rechner kopiert oder verschoben haben, auf dem der WACS gehostet wird.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den WACS, für den Sie HTTPS aktivieren möchten.
   Der Bildschirm *Eigenschaften* wird angezeigt.
3. Aktivieren Sie im Abschnitt *HTTPS-Konfiguration* das Kontrollkästchen **HTTPS aktivieren**.
4. Geben Sie im Feld **An Hostnamen oder IP-Adresse binden** die IP-Adresse an, für die die Zertifikate ausgegeben wurden und an die der WACS gebunden wird.
   HTTPS-Dienste werden über die angegebene IP-Adresse bereitgestellt.
5. Geben Sie im Feld **HTTPS-Port** eine Portnummer für den WACS an, um den HTTPS-Dienst bereitzustellen. Dieser Port darf nicht anderweitig belegt sein. Wenn Sie beabsichtigen, Benutzern von außerhalb der Firewall eine Verbindung zum WACS zu ermöglichen, muss dieser Port in der Firewall geöffnet sein.
6. Wenn Sie SSL mit einem Reverseproxy konfigurieren, geben Sie Hostnamen und Port des Proxyservers in die Felder **Proxy-Hostname** und **Proxy-Port** ein.
7. Wählen Sie in der Liste **Protokoll** ein Protokoll aus. Folgende Optionen stehen zur Verfügung:
   - **SSL**

     SSL ist das Secure Sockets Layer-Protokoll, das zum Verschlüsseln des Netzwerkdatenverkehrs verwendet wird.
   - **TLS**

     TLS ist das Transport Layer Security-Protokoll, das einer neueren und verbesserten Protokollversion entspricht. Die Unterschiede zwischen SSL und TLS sind geringfügig, umfassen jedoch effektivere Verschlüsselungsalgorithmen in TLS.
8. Geben Sie im Feld **Zertifikatspeichertyp** den Dateityp für das Zertifikat ein. Folgende Optionen stehen zur Verfügung:
   - **PKCS12**

     Wählen Sie "PKCS12", wenn Sie vertrauter im Umgang mit Microsoft-Tools sind.
   - **JKS**

     Wählen Sie "JKS", wenn Sie vertrauter im Umgang mit Java-Tools sind.
9. Geben Sie im Feld **Speicherort der Zertifikatspeicherdatei** den Pfad ein, unter dem Sie den Zertifikatdateispeicher oder die Java-Keystore-Datei kopiert oder verschoben haben.
10. Geben Sie im Feld **Zugangskennwort für den privaten Schlüssel** das Kennwort ein.

    PKCS12-Zertifikatspeicher und JKS-Keystores verfügen über kennwortgeschützte private Schlüssel, die den unbefugten Zugriff verhindern. Geben Sie das Kennwort für den Zugriff auf private Schlüssel ein, damit der WACS auf die privaten Schlüssel zugreifen kann.
11. Es wird empfohlen, einen Zertifikatdateispeicher oder Keystore zu verwenden, der ein einzelnes Zertifikat enthält oder in dem das gewünschte Zertifikat an erster Stelle aufgelistet ist. Wenn Sie einen

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Zertifikatdateispeicher oder Keystore verwenden, der mehr als ein Zertifikat enthält, und dieses Zertifikat nicht das erste Zertifikat im Dateispeicher ist, geben Sie im Feld **Zertifikat-Alias** jedoch den Alias für das Zertifikat an.

12. Wenn der WACS nur HTTPS-Anforderungen von bestimmten Clients akzeptieren soll, aktivieren Sie die Clientauthentifizierung.

    Bei der Clientauthentifizierung werden keine Benutzer authentifiziert. Sie stellt sicher, dass der WACS nur HTTPS-Anforderungen an bestimmte Clients verarbeitet.

    a) Aktivieren Sie **Clientauthentifizierung aktivieren**.

    b) Geben Sie unter **Speicherort der Datei mit der Zertifikatvertrauensliste** den Speicherort der PKCS12-Datei bzw. des JKS-Keystores ein, in dem die Datei mit der Vertrauensliste enthalten ist.

    > **Hinweis**
    >
    > Der Typ der Zertifikatvertrauensliste muss dem Typ des Zertifikatspeichers entsprechen.

    c) Geben Sie im Feld **Zertifikatvertrauensliste – Zugangskennwort für den privaten Schlüssel** das Kennwort ein, über das der Zugriff auf die privaten Schlüssel in der Datei mit der Zertifikatvertrauensliste kontrolliert wird.

    > **Hinweis**
    >
    > Wenn Sie die Clientauthentifizierung aktivieren und kein Browser oder Webdienstkonsument authentifiziert ist, wird die HTTPS-Verbindung zurückgewiesen.

13. Klicken Sie auf **Speichern und schließen**.
14. Wechseln Sie zum Bildschirm *Metriken*, und stellen Sie sicher, dass der HTTPS-Connector in der Liste *Aktive WACS-Connectors* angezeigt wird. Wenn HTTPS nicht angezeigt wird, überprüfen Sie, ob der HTTPS-Connector ordnungsgemäß konfiguriert ist.

12.1.5 Unterstützte Authentifizierungsmethoden

WACS unterstützt die folgenden Authentifizierungsmethoden:

- Enterprise
- LDAP
- AD Kerberos

WACS bietet keine Unterstützung für folgende Authentifizierungsmethoden:

- NT
- AD NTLM
- LDAP mit Einzelanmeldung

12.1.6 Konfigurieren von AD Kerberos für WACS

Um die AD Kerberos-Authentifizierung für WACS zu konfigurieren, muss der Rechner zuerst für die AD-Unterstützung konfiguriert werden. Führen Sie die folgenden Schritte aus:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Aktivieren des Sicherheits-Plugins für Windows AD
- Zuordnen von Benutzern und Gruppen
- Einrichten eines Dienstkontos
- Einrichten der eingeschränkten Delegierung
- Aktivieren der Kerberos-Authentifizierung im Windows AD-Plugin für WACS
- Erstellen von Konfigurationsdateien

Nachdem Sie den Rechner, auf dem der WACS gehostet wird, für die Verwendung der AD Kerberos-Authentifizierung eingerichtet haben, führen Sie zusätzliche Konfigurationsschritte über die Central Management Console (CMC) aus.

Wenn Sie die Einzelanmeldung über AD Kerberos für Web Services SDK und QaaWS konfigurieren, müssen sowohl der WACS als auch der Rechner konfiguriert werden, auf dem der WACS gehostet wird.

Weitere Informationen

Sicherheits-Plugin für Windows AD [Seite 264]
Zuordnen von Windows-AD-Benutzern und -Benutzergruppen [Seite 265]
Einrichten eines Dienstkontos für die AD-Authentifizierung mit Kerberos [Seite 263]
Ausführen des SIA unter dem Dienstkonto der BI-Plattform [Seite 271]
Aktivieren der Kerberos-Authentifizierung im Windows AD-Plugin für WACS [Seite 459]
Erstellen von Konfigurationsdateien [Seite 461]
Konfigurieren von WACS für AD Kerberos [Seite 464]
Konfigurieren der AD Kerberos-Einzelanmeldung [Seite 466]

12.1.6.1 Aktivieren der Kerberos-Authentifizierung im Windows AD-Plugin für WACS

Damit Kerberos unterstützt wird, muss das Windows AD-Sicherheits-Plugin in der CMC für die Verwendung der Kerberos-Authentifizierung konfiguriert werden. Dies umfasst die folgenden Schritte:

- Sicherstellen, dass die Windows AD-Authentifizierung aktiviert ist.
- Einrichten des AD-Administratorkontos.

> **Hinweis**
>
> Für dieses Konto sind außer Lesezugriff auf Active Directory keine weiteren Rechte erforderlich.

- Aktivieren der Kerberos-Authentifizierung und -Einzelanmeldung, falls Einzelanmeldung verwendet werden soll.
- Eingeben des Dienstprinzipalnamens (Service Principal Name, SPN) für das Dienstkonto.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12.1.6.1.1 Voraussetzungen

Bevor Sie das Windows AD-Sicherheits-Plugin für Kerberos konfigurieren, müssen folgende Aufgaben ausgeführt werden:

- *Einrichten eines Dienstkontos für die AD-Authentifizierung mit Kerberos* [Seite 263]
- *Ausführen des SIA unter dem Dienstkonto der BI-Plattform* [Seite 271]
- *Zuordnen von Windows-AD-Benutzern und -Benutzergruppen* [Seite 265]

12.1.6.1.2 Konfigurieren des Windows AD-Sicherheits-Plugins für Kerberos

1. Wechseln Sie zum Verwaltungsbereich **Authentifizierung** der CMC.
2. Doppelklicken Sie auf **Windows AD**.
3. Stellen Sie sicher, dass das Kontrollkästchen **Windows Active Directory (AD) aktivieren** aktiviert ist.
4. Wählen Sie unter **Authentifizierungsoptionen** die Option **Kerberos-Authentifizierung verwenden**.
5. Wenn Sie die Einzelanmeldung bei einer Datenbank konfigurieren möchten, aktivieren Sie das Kontrollkästchen **Cachesicherheitskontext (für SSO bei Datenbank erforderlich)**.
6. Geben Sie im Feld **Dienstprinzipalname** das Konto und die Domäne des Dienstkontos oder die SPN-Zuordnung zum Dienstkonto ein.

   Verwenden Sie das folgende Format, wobei `<svcacct>` dem Namen des zuvor erstellten Dienstkontos oder SPNs und `<DNS.COM>` dem vollständig qualifizierten Domänennamen in Großbuchstaben entspricht. Beispiel: Das Dienstkonto würde "svcacct@DNS.COM" und der SPN "BOBJCentralMS/Name@DOMÄNE.COM" lauten.

   > **Hinweis**
   >
   > - Wenn Sie beabsichtigen, auch anderen Benutzern als denen aus der Standarddomäne die Anmeldung zu ermöglichen, muss der in einem vorherigen Schritt zugeordnete SPN angegeben werden.
   > - Beim Dienstkonto wird Groß- und Kleinschreibung berücksichtigt. Die Groß- bzw. Kleinschreibung des hier angegebenen Kontos muss mit der Einrichtung in der Active Directory-Domäne übereinstimmen.
   > - Das Konto muss mit dem Konto identisch sein, über das Sie die BI-Plattform-Server ausführen, oder mit dem SPN, der diesem Konto zugeordnet ist.

7. Wenn Sie die Einzelanmeldung konfigurieren möchten, aktivieren Sie **Einzelanmeldung für ausgewählten Authentifizierungsmodus aktivieren**.

   > **Hinweis**
   >
   > Wenn Sie sich für die Aktivierung der Einzelanmeldung entschieden haben, muss der WACS konfiguriert werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Konfigurieren der AD Kerberos-Einzelanmeldung [Seite 466]

12.1.6.2 Erstellen von Konfigurationsdateien

Die allgemeine Vorgehensweise zum Konfigurieren von Kerberos auf einem Anwendungsserver umfasst folgende Schritte:

- Erstellen der Kerberos-Konfigurationsdatei
- Erstellen der Konfigurationsdatei für die JAAS-Anmeldung

> **Hinweis**
>
> - Die standardmäßige Active Directory-Domäne muss im DNS-Format in Großbuchstaben vorliegen.
> - Es ist nicht erforderlich, MIT Kerberos für Windows herunterzuladen und zu installieren. Darüber hinaus wird auch kein Keytab mehr für das Dienstkonto benötigt.

12.1.6.2.1 Erstellen von Kerberos-Konfigurationsdateien

Führen Sie die folgenden Schritte aus, um die Kerberos-Konfigurationsdatei zu erstellen.

1. Erstellen Sie die Datei `krb5.ini`, falls diese noch nicht vorhanden ist, und speichern Sie sie für Windows unter `C:\Windows`.

   > **Hinweis**
   >
   > Sie können diese Datei an einem anderen Speicherort speichern. Wenn dies der Fall ist, geben Sie den Speicherort in der CMC auf der Seite *Eigenschaften* für den WACS-Server im Feld **Speicherort der Datei Krb5.ini** an.

2. Fügen Sie der Kerberos-Konfigurationsdatei die folgenden erforderlichen Informationen hinzu.

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
}
```

> **Hinweis**
>
> `DNS.COM` ist der DNS-Name der Domäne, der in Großbuchstaben im FQDN-Format eingegeben werden muss.

> **Hinweis**
>
> `kdc` ist der Hostname des Domänencontrollers.

> **Hinweis**
>
> Sie können dem Abschnitt [realms] mehrere Domäneneinträge hinzufügen, wenn sich Ihre Benutzer von mehreren Domänen aus anmelden. Ein Beispiel dieser Datei mit mehreren Domäneneinträgen finden Sie unter *Beispiel für Krb5.ini-Dateien* [Seite 463].

> **Hinweis**
>
> In einer Konfiguration mit mehreren Domänen kann der Wert `default_realm` unter `[libdefaults]` einer beliebigen Domäne entsprechen. Am besten verwenden Sie die Domäne mit der größten Anzahl von Benutzern, die sich mit ihrem AD-Konto authentifizieren.

12.1.6.2.2 Erstellen von Konfigurationsdateien für die JAAS-Anmeldung

1. Erstellen Sie eine Datei mit dem Namen `bscLogin.conf`, falls noch nicht vorhanden, und speichern Sie sie am Standardspeicherort `C:\Windows`.

   > **Hinweis**
   >
   > Sie können diese Datei an einem anderen Speicherort speichern. Wenn dies der Fall ist, geben Sie den Speicherort in der CMC auf der Seite **Eigenschaften** für den WACS-Server im Feld *Speicherort der Datei bscLogin.conf* an.

2. Fügen Sie der JAAS-Konfigurationsdatei `bscLogin.conf` folgenden Code hinzu:

   ```
   com.businessobjects.security.jgss.initiate {
   com.sun.security.auth.module.Krb5LoginModule required;
   };
   ```

3. Speichern und schließen Sie die Datei.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12.1.6.2.3 Beispiel für Krb5.ini-Dateien

Beispiel einer Krb5.ini-Datei für mehrere Domänen

Nachfolgend ist eine Beispieldatei mit mehreren Domänen aufgeführt:

```
[domain_realm]
        .domain03.com = DOMAIN03.COM
        domain03.com = DOMAIN03.com
        .child1.domain03.com = CHILD1.DOMAIN03.COM
        child1.domain03.com = CHILD1.DOMAIN03.com
        .child2.domain03.com = CHILD2.DOMAIN03.COM
        child2.domain03.com = CHILD2.DOMAIN03.com
        .domain04.com = DOMAIN04.COM
        domain04.com = DOMAIN04.com
[libdefaults]
        default_realm = DOMAIN03.COM
        dns_lookup_kdc = true
        dns_lookup_realm = true
[realms]
        DOMAIN03.COM = {
         admin_server = testvmw2k07
         kdc = testvmw2k07
         default_domain = domain03.com
        }
     CHILD1.DOMAIN03.COM = {
            admin_server = testvmw2k08
            kdc = testvmw2k08
            default_domain = child1.domain03.com
        }
        CHILD2.DOMAIN03.COM = {
            admin_server = testvmw2k09
            kdc = testvmw2k09
            default_domain = child2.domain03.com
        }
        DOMAIN04.COM = {
            admin_server = testvmw2k011
            kdc = testvmw2k011
            default_domain = domain04.com
        }
```

Beispiel einer Krb5.ini-Datei für eine einzelne Domäne

Nachfolgend ist ein Beispiel einer krb5.ini-Datei mit einer einzelnen Domäne aufgeführt.

```
[libdefaults]
        default_realm = ABCD.MFROOT.ORG
        dns_lookup_kdc = true
        dns_lookup_realm = true
[realms]
        ABCD.MFROOT.ORG = {
            kdc = ABCDIR20.ABCD.MFROOT.ORG
            kdc = ABCDIR21.ABCD.MFROOT.ORG
            kdc = ABCDIR22.ABCD.MFROOT.ORG
            kdc = ABCDIR23.ABCD.MFROOT.ORG
            default_domain = ABCD.MFROOT.ORG
        }
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12.1.6.3 Konfigurieren von WACS für AD Kerberos

Nachdem Sie den Rechner, auf dem der WACS gehostet wird, für die AD Kerberos-Authentifizierung konfiguriert haben, konfigurieren Sie den WACS selbst über die Central Management Console (CMC).

12.1.6.3.1 Konfigurieren von WACS für AD Kerberos

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den WACS, für den Sie AD konfigurieren möchten.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
3. Geben Sie im Feld **Speicherort der Datei Krb5.ini** den Pfad zur Konfigurationsdatei `krb5.ini` an.
4. Geben Sie im Feld **Speicherort der Datei bscLogin.conf** den Pfad zur Konfigurationsdatei `bscLogin.conf` an.
5. Klicken Sie auf **Speichern und schließen**.
6. Starten Sie den WACS neu.

12.1.6.4 Fehlerbehebung bei Kerberos

Die folgenden Schritte können hilfreich sein, falls bei der Konfiguration von Kerberos Probleme auftreten:

- Protokollierung aktivieren
- Testen der Kerberos-Konfiguration

12.1.6.4.1 Aktivieren der Kerberos-Protokollierung

1. Starten Sie Central Configuration Manager (CCM), und klicken Sie auf **Server verwalten**.
2. Geben Sie die Anmeldedaten an.
3. Stoppen Sie den WACS im Bildschirm *Server verwalten*.
4. Klicken Sie auf **Webschicht-Konfiguration**.

   > **Hinweis**
   >
   > Das Symbol **Webschicht-Konfiguration** ist nur aktiviert, wenn Sie einen gestoppten WACS auswählen.

   Das Dialogfeld *Webschicht-Konfiguration* wird angezeigt.
5. Kopieren Sie unter **Befehlszeilenparameter** den folgenden Text an das Ende der Parameter:

   ```
   "-Dcrystal.enterprise.trace.configuration=verbose
    -Djcsi.Kerberos.debug=true"
   ```

6. Klicken Sie auf **OK**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7. Starten Sie den WACS im Bildschirm *Server verwalten*.

12.1.6.4.2 So testen Sie die Kerberos-Konfiguration

Führen Sie zum Testen der Kerberos-Konfiguration den folgenden Befehl aus, wobei `servact` für das Dienstkonto und die Domäne steht, unter der der CMS ausgeführt wird, und `password` für das Kennwort, das dem Dienstkonto zugeordnet ist.

```
<INSTALLDIR>\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM Password
```

Beispiel:

```
 C:\Program Files\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM
Password
```

Wenn weiterhin Probleme auftreten, stellen Sie sicher, dass die Groß- und Kleinschreibung der Domäne und des Dienstprinzipalnamens genau mit den Einstellungen in Active Directory übereinstimmen.

12.1.6.4.3 Zugeordneter AD-Benutzer kann sich nicht bei der BI-Plattform auf dem WACS anmelden

Die folgenden beiden Probleme können auftreten, obwohl die Benutzer der BI-Plattform zugeordnet wurden:

12.1.6.4.3.1 Anmeldefehler aufgrund unterschiedlicher AD UPN- und SAM-Namen

Die Active-Directory-ID eines Benutzers wurde der BI-Plattform erfolgreich zugeordnet. Trotzdem ist der Benutzer nicht in der Lage, mit AD-Authentifizierung und Kerberos in folgendem Format eine Anmeldung bei der CMC auszuführen: `DOMÄNE\ABC123`

Dieses Problem kann auftreten, wenn der Benutzer in Active Directory mit einem UPN und SAM-Namen eingerichtet wurde, die nicht identisch sind, entweder in Bezug auf die Groß-/Kleinschreibung oder aus einem anderen Grund. Im Folgenden zwei Beispiele, die ein Problem verursachen können:

- Der UPN lautet "abc123@firma.com" und der SAM-Name "DOMAIN\ABC123".
- Der UPN lautet "jschmidt@firma" und der SAM-Name "DOMAIN\janschmidt"

Dieses Problem kann auf zwei Weisen behoben werden:

- Benutzer melden sich unter Verwendung des UPN-Namens und nicht mit dem SAM-Namen an.
- Stellen Sie sicher, dass der SAM-Kontoname und der UPN-Name identisch sind.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12.1.6.4.3.2 Fehler vor der Authentifizierung

Ein Benutzer, der sich zuvor anmelden konnte, kann sich nicht mehr anmelden. Der Benutzer erhält folgende Fehlermeldung: "Kontoinformationen nicht erkannt." In WACS-Protokollen finden Sie folgenden Fehler: `"Pre-authentication information was invalid (24)"` (Vorbestätigungsinformationen waren ungültig).

Dieser Fehler kann darin begründet liegen, dass eine Änderung, die in AD am UPN vorgenommen wurde, nicht an die Kerberos-Benutzerdatenbank weitergeleitet wurde. Es ist also möglich, dass die Kerberos-Benutzerdatenbank und die AD-Informationen nicht synchronisiert sind.

Um dieses Problem zu beheben, setzen Sie das Benutzerkennwort in AD zurück. Dadurch wird sichergestellt, dass die Änderungen ordnungsgemäß weitergeleitet werden.

12.1.7 Konfigurieren der AD Kerberos-Einzelanmeldung

Wenn Sie die AD-Kerberos-Einzelanmeldung für BI-Launchpad oder Web Services SDK und QaaWS konfigurieren, müssen Sie sicherstellen, dass Sie sowohl den WACS als auch den Rechner, der den WACS hostet, für die AD-Kerberos-Authentifizierung konfiguriert haben.

Zum Konfigurieren des WACS für die AD Kerberos-Einzelanmeldung müssen Sie zuerst den Rechner konfigurieren, der WACS hostet, und danach den WACS.

> **Hinweis**
>
> Wenn Sie die Einzelanmeldung in einer Reverse-Proxy-Umgebung verwenden möchten, lesen Sie die Sicherheitsinformationen in diesem Handbuch.

Weitere Informationen

Überblick zum Thema Sicherheit [Seite 153]
Konfigurieren von AD Kerberos für WACS [Seite 458]
Konfiguration Ihres Rechners für AD Kerberos-Einzelanmeldung [Seite 466]
Konfigurieren des WACS für die AD Kerberos-Einzelanmeldung [Seite 467]

12.1.7.1 Konfiguration Ihres Rechners für AD Kerberos-Einzelanmeldung

Vor der Konfiguration der AD Kerberos-Einzelanmeldung für Web Services SDK und QaaWS ist zunächst der Rechner zu konfigurieren, der den WACS hostet:

- *Konfigurieren der eingeschränkten Delegierung für Vintela-SSO* [Seite 285]
- *Einrichten des Dienstkontos für Vintela-SSO* [Seite 283]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- *Einrichten mehrerer SPNs* [Seite 467]
- *Erhöhen des Grenzwerts für die Headergröße des WACS* [Seite 467]

In den folgenden Abschnitten wird beschrieben, wie Sie die einzelnen Schritte ausführen.

12.1.7.1.1 Einrichten mehrerer SPNs

Die Verwendung mehrerer SPNs wird nicht unterstützt.

12.1.7.1.2 Erhöhen des Grenzwerts für die Headergröße des WACS

Active Directory erstellt ein Kerberos-Token, das bei der Authentifizierung verwendet wird. Dieses Token wird im HTTP-Header gespeichert. Der WACS verfügt über eine standardmäßige HTTP-Headergröße, die für die meisten Benutzer ausreichend ist. Diese Headergröße ist konfigurierbar.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den WACS, dessen HTTP-Headergröße Sie ändern möchten.
   Der Bildschirm *Eigenschaften* wird angezeigt.
3. Geben Sie im Bereich *HTTP-Konfiguration*, *Konfiguration von "HTTP über Proxy"* oder *HTTPS-Konfiguration* einen Wert in das Feld **Maximale Größe des HTTP-Headers (Byte)** ein.
4. Klicken Sie auf **Speichern und schließen**.
5. Starten Sie den Server neu.

12.1.7.2 Konfigurieren des WACS für die AD Kerberos-Einzelanmeldung

Sie können den Web Application Container Server so konfigurieren, dass er die AD Kerberos-Einzelanmeldung verwendet. Die AD Kerberos-Einzelanmeldung wird unterstützt. AD NTLM wird nicht unterstützt.

Bevor Sie den WACS konfigurieren, müssen Sie die AD Kerberos-Einzelanmeldung für den Rechner konfigurieren, der den WACS hostet.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den WACS, den Sie konfigurieren möchten.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
3. Aktivieren Sie **Kerberos Active Directory Einzelanmeldung aktivieren**
4. Geben Sie Werte für Eigenschaften von "Standard-AD-Domäne", "Dienstprinzipalname" und "Keytab-Datei" ein, und klicken Sie auf **Speichern und schließen**.
5. Starten Sie den WACS neu.

Die Active Directory-Einzelanmeldung ist nun einsatzbereit.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12.1.7.3 Konfigurieren von Kerberos und Einzelanmeldung bei der Datenbank

Die Einzelanmeldung bei Datenbanken wird für Implementierungen unterstützt, die alle folgenden Voraussetzungen erfüllen:

- Die Implementierung der BI-Plattform befindet sich auf dem WACS.
- Der WACS wurde mit AD mit Kerberos konfiguriert.
- Bei der Datenbank, für die Einzelanmeldung erforderlich ist, handelt es sich um eine unterstützte Version von SQL Server oder Oracle.
- Den Benutzergruppen, die Zugriff auf die Datenbank benötigen, müssen Berechtigungen innerhalb von SQL Server oder Oracle gewährt werden.
- Das Kontrollkästchen "Cachesicherheitskontext (für SSO bei Datenbank erforderlich)" auf der Seite "AD-Authentifizierung" der CMC ist aktiviert.

Der letzte Schritt besteht darin, die Datei `krb5.ini` zu ändern, damit die Datenbank-Einzelanmeldung unterstützt wird.

> **Hinweis**
>
> Diese Anweisungen erläutern die Konfiguration der Datenbank-Einzelanmeldung. Wenn Sie die End-to-End-Einzelanmeldung bei Datenbanken konfigurieren möchten, müssen auch die erforderlichen Konfigurationsschritte für die Vintela-Einzelanmeldung vorgenommen werden. Ausführliche Informationen finden Sie unter *Konfigurieren der AD Kerberos-Einzelanmeldung* [Seite 466].

12.1.7.3.1 Aktivieren der Einzelanmeldung bei der Datenbank

1. Öffnen Sie die Datei `krb5.ini`, die für die Implementierung der BI-Plattform verwendet wird.

   Der Standardspeicherort für diese Datei ist das C:\Windows-Verzeichnis auf Ihrem Webanwendungsserver.
2. Wechseln Sie zum Abschnitt `[libdefaults]` der Datei.
3. Geben Sie die folgende Zeichenfolge vor dem Abschnitt `[realms]` der Datei ein:

   ```
   forwardable = true
   ```
4. Speichern und schließen Sie die Datei.
5. Starten Sie den WACS neu.

12.1.8 Konfigurieren von RESTful-Webdiensten

Das RESTful-Webdienste-SDK für die BI-Plattform ermöglicht Ihnen den Zugriff auf die BI-Plattform anhand des HTTP-Protokolls. Damit können Benutzer zum BI-Plattform-Repository navigieren und Objekte anhand einer beliebigen Programmiersprache, die HTTP-Anforderungen unterstützt, zeitgesteuert verarbeiten. RESTful-Webdienste werden als Teil von WACS installiert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

In diesem Abschnitt wird erläutert, wie RESTful-Webdienste verwaltet werden. Weitere Informationen zu RESTful-Webdiensten finden Sie im *Business Intelligence Platform RESTful Web Service Developer Guide*.

12.1.8.1 Anwendungen

12.1.8.1.1 Konfigurieren der Basis-URL für RESTful-Webdienste

Wenn die BI-Plattform-Implementierung einen Proxy-Server verwendet oder mehrere Instanzen des Web Application Container Server (WACS) enthält, müssen Sie die Basis-URL möglicherweise für die Verwendung mit RESTful-Webdiensten konfigurieren. Bevor Sie die Basis-URL konfigurieren, benötigen Sie den Servernamen und die Portnummer, der bzw. die RESTful-Webdienst-Anforderungen überwacht.

Die Basis-URL wird als Teil jeder RESTful-Webdienst-Anforderung verwendet. Entwickler ermitteln die Basis-URL programmatisch und verwenden sie, um RESTful-Webdienst-Anforderungen an den korrekten Server und Port zu lenken. Die Basis-URL wird außerdem in RESTful-Webdienst-Antworten verwendet, um Hyperlinks zu anderen RESTful-Ressourcen zu definieren.

> **Hinweis**
>
> In Standardinstallationen der BI-Plattform ist die Basis-URL als `http://<Servername>:6405/biprws` definiert. Ersetzen Sie `<Servername>` durch den Namen des Servers, der RESTful-Webdienste hostet.

1. Melden Sie sich an der Central Management Console (CMC) als Administrator an.
2. Klicken Sie in der CMC auf die Option **Anwendungen**.
   Es wird eine Liste mit Anwendungen angezeigt.
3. Klicken Sie mit der rechten Maustaste auf **RESTful-Webdienst** > **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
4. Geben Sie im Textfeld **Zugriffs-URL** den Namen der Basis-URL für RESTful-Webdienste ein.
   Geben Sie beispielsweise `http://<Servername>:<Portnummer>/biprws` ein. Ersetzen Sie `<Servername>` und `<Portnummer>` mit dem Namen des Servers und dem Port, der RESTful-Webdienst-Anforderungen überwacht.
5. Klicken Sie auf **Speichern und schließen**.

12.1.8.2 WACS-Eigenschaften

12.1.8.2.1 Konfigurieren von Befehlszeilenparametern von Methoden und Köpfen

Als Administrator können Sie die von RESTful-Webdiensten verwendeten Methoden und Köpfe einschränken, indem Sie die entsprechenden Optionen unter *Befehlszeilenparameter* in den Eigenschaften des Web Application Container Service (WACS) hinzufügen. Änderungen an den Parametern erfordern, dass der WACS-Dienst neu gestartet wird.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Melden Sie sich als Benutzer "Administrator" an der Central Management Console an.
2. Klicken Sie auf **Server** und anschließend auf **Serverliste**.
3. Klicken Sie mit der rechten Maustaste auf den Web Application Container Server (WACS), beispielsweise auf `MySIA.WebApplicationContainerServer`, und klicken Sie dann auf **Eigenschaften**.
   Die Registerkarte **Eigenschaften** für den WACS-Server wird angezeigt.
4. Geben Sie im Bereich *Befehlszeilenparameter* die zulässigen Methoden und Köpfe ein.

   Jede Optionsgruppe ist in doppelte Anführungszeichen eingeschlossen. Verwenden Sie andere Methoden als `GET`, `HEAD` und `POST`. Trennen Sie, wie im folgenden Beispiel veranschaulicht, die Optionswerte, z.B. `PUT` und `DELETE`, durch Kommas.

   ```
   "-Dcom.sap.bip.rs.cors.extra.methods= PUT, DELETE"
   "-Dcom.sap.bip.rs.cors.extra.headers= X-SAP-LogonToken, X-SAP-PVL, WWW-
   Authenticate"
   ```

   Hinweis

   Der Standardwert, mit dem alle Methoden und Köpfe zugelassen werden, ist `*` (Sternchen). Wenn Sie die Befehlszeilenparameter vollständig auslassen, erzielen Sie die gleiche Wirkung.
5. Klicken Sie auf **Speichern und schließen**.
6. Starten Sie den Dienst neu, indem Sie mit der rechten Maustaste auf den WACS-Servernamen, z.B. `MySIA.WebApplicationContainerServer`, klicken und dann auf **Server neu starten** klicken.

12.1.8.2.2 Systemkonfiguration

12.1.8.2.2.1 Aktivieren des Fehlermeldungsstapels

Als Administrator können Sie die von RESTful-Webdiensten zurückgegebenen Fehlermeldungen so konfigurieren, dass der Fehlerstapel enthalten ist. Der Fehlerstapel umfasst spezielle Debugging-Informationen, die verwendet werden können, um zu ermitteln, an welchen Stellen Fehler aufgetreten sind.

Hinweis

In Produktionsszenarios sollte der Fehlerstapel eventuell nicht aktiviert werden, da er Informationen über die BI-Plattform zur Verfügung stellen könnte, die Endbenutzern gegenüber nicht offengelegt werden sollten. Es wird empfohlen, den Fehlerstapel in Produktionsszenarios für das Debugging zu aktivieren und anschließend wieder zu deaktivieren.

1. Melden Sie sich an der Central Management Console als Administrator an.
2. Klicken Sie auf **Server** und anschließend auf **Serverliste**.
3. Klicken Sie mit der rechten Maustaste auf den Web Application Container Server (WACS), beispielsweise auf `MySIA.WebApplicationContainerServer`, und dann auf **Eigenschaften**.
   Die Registerkarte **Eigenschaften** für den WACS-Server wird angezeigt.
4. Wählen Sie im Bereich **RESTful-Webdienst** die Option **Fehlerstapel anzeigen**.
5. Klicken Sie auf **Speichern und schließen**.

Die Fehlerstapelinformationen sind in den Fehlermeldungen des RESTful-Webdiensts eingebunden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12.1.8.2.2.2 Festlegen der je Seite angezeigten Standardanzahl an Einträgen

Wenn eine Antwort eines RESTful-Webdiensts einen Feed mit einer großen Anzahl an Einträgen enthält, kann die Antwort in Seiten unterteilt werden. Sie können die Standardanzahl an Einträgen, die auf jeder Seite angezeigt werden, konfigurieren. Wenn Entwickler RESTful-Webdienst-Anforderungen stellen, können sie angeben, wie viele Einträge auf jeder Seite angezeigt werden sollen. Wenn sie diesen Wert jedoch nicht angeben, wird die Standardseitengröße verwendet.

1. Melden Sie sich an der Central Management Console als Administrator an.
2. Klicken Sie auf **Server** und anschließend auf **Serverliste**.
3. Klicken Sie mit der rechten Maustaste auf den Web Application Container Server (WACS), beispielsweise auf `MySIA.WebApplicationContainerServer`, und dann auf **Eigenschaften**.
   Die Registerkarte **Eigenschaften** für den WACS-Server wird angezeigt.
4. Geben Sie im Bereich **RESTful-Webdienst** die Standardseitengröße im Textbereich **Standard-Objektanzahl pro Seite** ein.
5. Klicken Sie auf **Speichern und schließen**.

12.1.8.2.2.3 Festlegen des Zeitüberschreitungswerts eines Anmeldetokens

Anmeldetoken verfallen, wenn sie nicht innerhalb einer bestimmten Zeit verwendet wurden. Sie können die Dauer festlegen, für die ein nicht verwendetes Anmeldetoken gültig bleibt.

> **Hinweis**
>
> Standardmäßig beträgt der Zeitüberschreitungswert des Anmeldetokens eine Stunde.

1. Melden Sie sich an der Central Management Console als Administrator an.
2. Klicken Sie auf **Server** und anschließend auf **Serverliste**.
3. Klicken Sie mit der rechten Maustaste auf den Web Application Container Server (WACS), beispielsweise auf `MySIA.WebApplicationContainerServer`, und dann auf **Eigenschaften**.
   Die Registerkarte **Eigenschaften** für den WACS-Server wird angezeigt.
4. Geben Sie im Bereich **RESTful-Webdienst** im Textbereich **Zeitüberschreitung für Enterprise-Sitzungstoken (Minuten)** die Anzahl an Minuten ein, für die ein Anmeldetoken gültig sein soll.
5. Klicken Sie auf **Speichern und schließen**.

12.1.8.2.2.4 Konfigurieren von Sitzungspool-Einstellungen

Durch Verwendung eines Sitzungspools können Sie die Serverperformance verbessern. Der Sitzungspool speichert aktive RESTful-Webdienst-Sitzungen zwischen, so dass sie erneut verwendet werden können, wenn ein Benutzer eine weitere Anforderung sendet, die dasselbe Anmeldetoken im HTTP-Request-Header nutzt. Die

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Sitzungspoolgröße definiert die Anzahl der gleichzeitig zu speichernden zwischengespeicherten Sitzungen, und der Sitzungs-Zeitüberschreitungswert steuert die Dauer, für die eine Sitzung zwischengespeichert wird.

Sie können die Sitzungspoolgröße und den Sitzungs-Zeitüberschreitungswert festlegen:

1. Melden Sie sich an der Central Management Console (CMC) als Administrator an.
2. Klicken Sie auf **Server** und anschließend auf **Serverliste**.
3. Klicken Sie mit der rechten Maustaste auf den Web Application Container Server (WACS), beispielsweise auf `MySIA.WebApplicationContainerServer`, und dann auf **Eigenschaften**.
   Die Registerkarte **Eigenschaften** für den WACS-Server wird angezeigt.
4. Geben Sie im Textfeld **Sitzungspoolgröße** des Bereichs **RESTful-Webdienst** die maximale Anzahl an Sitzungen ein, die zwischengespeichert werden sollen.
5. Geben Sie den Sitzungspool-Zeitüberschreitungswert in das Textfeld **Sitzungspool-Zeitüberschreitung (Minuten)** des Bereichs **RESTful-Webdienst** ein.
6. Klicken Sie auf **Speichern und schließen**.
7. Klicken Sie mit der rechten Maustaste auf den WACS, beispielsweise auf `MySIA.WebApplicationContainerServer`, und dann auf **Server neu starten**.

12.1.8.2.2.5 Aktivieren der HTTP-Standardauthentifizierung

Die HTTP-Standardauthentifizierung ermöglicht es den Benutzern, RESTful-Webdienst-Anforderungen zu erstellen, ohne ein Anmeldetoken bereitzustellen zu müssen. Wenn die HTTP-Standardauthentifizierung aktiviert ist, werden die Benutzer aufgefordert, ihren Benutzernamen und ihr Kennwort anzugeben, wenn sie zum ersten Mal eine RESTful-Webdienst-Anforderung stellen.

> **Hinweis**
>
> Benutzernamen und Kennwörter werden mit der HTTP-Standardauthentifizierung nicht sicher übertragen, es sei denn, sie wird in Verbindung mit HTTPS verwendet.

Wenn Sie die HTTP-Standardauthentifizierung aktivieren, legen Sie den Standardtyp der HTTP-Standardauthentifizierung auf SAP, Enterprise, LDAP oder WinAD fest. Der HTTP-Standardauthentifizierungstyp kann von den Benutzern bei der Anmeldung überschrieben werden.

Für die Anmeldung an der BI-Plattform mit der HTTP-Standardauthentifizierung ist eine Lizenz erforderlich. Wenn die Sitzungspool-Zwischenspeicherung eingesetzt wird, verwendet die Anforderung die zur zwischengespeicherten Sitzung zugehörige Lizenz. Wenn die Sitzungspool-Zwischenspeicherung nicht verwendet wird, wird eine Lizenz benutzt, während die Anforderung verarbeitet wird, und wird freigegeben, nachdem die Anforderung beendet wurde.

1. Melden Sie sich an der Central Management Console (CMC) als Administrator an.
2. Klicken Sie auf **Server** > **Serverliste**.
3. Klicken Sie mit der rechten Maustaste auf den Web Application Container Server (WACS), beispielsweise auf `MySIA.WebApplicationContainerServer`, und dann auf **Eigenschaften**.
   Die Registerkarte **Eigenschaften** für den WACS-Server wird angezeigt.
4. Wählen Sie im Bereich *RESTful-Webdienst* die Option **HTTP-Standardauthentifizierung aktivieren**.
5. (Optional) Wählen Sie in der Liste **Standardmäßiges Authentifizierungsschema für HTTP Basic** den Standardtyp der HTTP-Standardauthentifizierung aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6. Klicken Sie auf **Speichern und schließen**.

Wenn sich die Endbenutzer unter Verwendung der HTTP-Standardauthentifizierung anmelden, können sie den Typ der zu verwendenden Authentifizierung angeben. In einem Webbrowser gibt der Benutzer `<Authtyp>\<Benutzername>` in die Benutzernamen-Eingabeaufforderung und `<Kennwort>` in die Kennwort-Eingabeaufforderung ein.

Um die HTTP-Standardauthentifizierung programmatisch bei der Anmeldung zu verwenden, fügen die Benutzer das Attribut `Autorisierung` zum HTTP-Request-Header hinzu und legen den Wert auf `Basic <Authtyp>\<Benutzername>:<Kennwort>` fest.

Ersetzen Sie `<Authtyp>` mit dem Authentifizierungstyp, `<Benutzername>` mit dem Benutzernamen und `<Kennwort>` mit dem Kennwort. Wie in RFC 2617 definiert, müssen Authentifizierungstyp, Benutzername und Kennwort Base64-verschlüsselt sein. Benutzernamen, die das Zeichen `:` enthalten, dürfen mit der HTTP-Standardauthentifizierung nicht verwendet werden.

Weitere Informationen

Konfigurieren von Sitzungspool-Einstellungen [Seite 471]

12.1.8.2.3 Cross-Origin Resource Sharing

12.1.8.2.3.1 Konfigurieren der Ressourcenfreigabe über Ursprungs-URLs hinweg

Die Einstellung **Ressourcenfreigabe-Konfiguration über Ursprungs-URLs hinweg** (CORS) ermöglicht Ihnen, eine Liste von Domänennamen hinzuzufügen, damit die Benutzer Daten aus mehreren Quellen auf JavaScript-Webseiten abrufen können. Dies ist zur Vermeidung der Sicherheitsrichtlinie erforderlich, mit deren Hilfe die Sprachen JavaScript und Ajax den domänenübergreifenden Zugriff verhindern. Um die Sicherheit nicht zu beeinträchtigen, werden nur die Websites, auf die zugegriffen werden darf, den WACS-Servereigenschaften **Ursprungs-URLs zulassen** in der CMC hinzugefügt.

Außerdem steht eine Einstellung **Max. Alter (Minuten)** zur Anpassung der Cacheablaufzeit zur Verfügung. Sie legt als maximale Anzahl von Minuten die Zeit fest, während der Browser HTTP-Anforderungen beibehalten können.

> **Hinweis**
>
> Der Zugriff auf alle Domänen wird standardmäßig mit * (Sternchen) zugelassen.

1. Melden Sie sich an der Central Management Console als Administrator an.
2. Klicken Sie auf **Server** > **Serverliste**.
3. Klicken Sie mit der rechten Maustaste auf den Web Application Container Server (WACS), beispielsweise auf `MySIA.WebApplicationContainerServer`, und klicken Sie dann auf **Eigenschaften**.
   Die Registerkarte **Eigenschaften** für den WACS-Server wird angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Wechseln Sie im Bereich **RESTful-Webdienst** zum Textfeld **Ressourcenfreigabe-Konfiguration über Ursprungs-URLs hinweg** neben **Ursprungs-URLs zulassen**, und ersetzen Sie das * (Sternchen) durch Ihre Liste von Domänennamen, die Sie jeweils durch ein Komma trennen. Beispiel: `http://origin1.server:8080, http://origin2.server:8080`
5. Geben Sie im Textfeld **Max. Alter (Minuten)** die maximale Zeit in Minuten ein, während der Browser HTTP-Anforderungen zwischenspeichern sollen.
6. Klicken Sie auf **Speichern und schließen**.

12.1.8.2.4 Authentifizierung

12.1.8.2.4.1 Konfigurieren von web.xml zum Aktivieren der WinAD-SSO

Um die RESTful-Webdienste so zu konfigurieren, dass die Windows-Active-Directory-Einzelanmeldung (WinAD-SSO) erkannt wird, muss die Konfigurationsdatei `web.xml` bearbeitet werden, die sich auf dem BI-Plattformserver befindet. Weitere Informationen finden Sie unter “Using the SDK > Authentication > To get a logon token using an Active Directory Single Sign-On (AD SSO) account” im *Business Intelligence Platform RESTful Web Service Developer Guide*.

Damit der BI-Plattformserver die WinAD-SSO-Anmeldedaten erkennt, entfernen Sie die Kommentare im Abschnitt `Kerberos Proxy Filter` von `web.xml`, und aktualisieren Sie die Werte von `idm.realm`, `idm.princ` und `idm.keytab`, die die verwendete Active-Directory-Umgebung widerspiegeln.

1. Suchen Sie die `web.xml`-Konfiguration unter `<boe root>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\RestWebService\biprws\WEB-INF\`. Der folgende Dateipfad ist ein Beispiel.

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\java\
pjs\services\RestWebService\biprws\WEB-INF\web.xml
```

2. Entfernen Sie in der Datei `web.xml` den Kommentar im Abschnitt "Kerberos Proxy Filter", indem Sie ein Kommentarendtag, `-->`, vor dem Tag `<filter>` hinzufügen, und entfernen Sie das schließende Kommentartag `-->`

```
  <!-- Kerberos Proxy Filter
    - Uncomment this filter and the corresponding filter-mapping to enable
Kerberos SSO
    - for Windows AD (secWinAD) authentication.
    - The following options must be specified (the rest are optional):
    -   idm.realm
    -   idm.princ
    -   idm.keytab (unless using password, see below)
  -->

  <filter>
    <filter-name>WrappedResponseAuthFilter</filter-name>
      .
      .
      .
  </filter>

  <filter-mapping>
    <filter-name>WrappedResponseAuthFilter</filter-name>
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
    <url-pattern>/logon/adsso</url-pattern>
  </filter-mapping>

</web-app>
```

3. Aktualisieren Sie `<param-value>` für jede Einstellung von `idm.realm`, `idm.princ` und `idm.keytab` mit den in der Active-Directory-Umgebung verwendeten Werten.

```
    <init-param>
      <param-name>idm.realm</param-name>
      <param-value>ADDOM.COM</param-value>
      <description>
          Required: Set this value to the Kerberos realm to use.
      </description>
    </init-param>

    <init-param>
      <param-name>idm.princ</param-name>
      <param-value>BOE120SIAVMBOESRVR/bo.service.addom.com</param-value>

      <description>
          Set this value to the Kerberos service principal to use.
          This will be a name of the form HTTP/fully-qualified-host.
          For example, HTTP/example.vintela.com
          If not set, defaults to the server's hostname and the
          idm.realm  property above.
      </description>
    </init-param>

    <init-param>
      <param-name>idm.kdc</param-name>
      <param-value></param-value>
      <description>
          The KDC against which secondary credentials must be validated
          This can be used for BASIC fallback or credential delegation.
          By default the KDC will be discovered automatically and this
          parameter must only be used if automatic discovery fails, or
          if a different KDC to the one discovered must automatically be used.
      </description>
    </init-param>

    <init-param>
      <param-name>idm.keytab</param-name>
      <param-value>C:/winnt/BOE120SIAVMBOESRVR.keytab</param-value>
      <description>
          The file containing the keytab that Kerberos will use for
          user-to-service authentication. If unspecified, SSO will default
          to using an in-memory keytab with a password specified in the
          com.wedgetail.idm.sso.password environment variable.
      </description>
    </init-param>
```

Hinweis

Der Wert `idm.keytab` verweist auf einen Dateipfad auf dem BI-Plattformserver. Die Werte für `idm.realm` und `idm.prince` können über die Central Management Console angezeigt werden. Doppelklicken Sie auf der Registerkarte **Authentifizierung** in der CMC auf **Windows AD**. Der Wert für `idm.realm` wird mit dem Parameter *Standard-AD-Domäne* unter *Eigenschaften der AD-Konfiguration* festgelegt. Der Wert von `idm.prince` wird mit dem Parameter *Dienstprinzipalname* unter *Authentifizierungsoptionen* festgelegt.

4. Starten Sie den WACS-Dienst neu, sodass die an `web.xml` vorgenommenen Änderungen erkannt werden.
5. Prüfen Sie mithilfe eines Clientrechners, ob ein AD-SSO-Anmeldetoken unter Verwendung der RESTful-Webdienst-API (z.B. `http://<boe host>:6405/biprws/logon/adsso`) abgerufen werden kann.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6. Testen Sie das Token mithilfe einer `GET`-Abfrage mit *X-SAP-LogonToken* im Kopf und der `/infostore`-API.

12.1.8.2.4.2 Aktivieren und Konfigurieren der vertrauenswürdigen Authentifizierung

Die vertrauenswürdige Authentifizierung wird über die Central Management Console (CMC) in mehreren Bereichen aktiviert und konfiguriert. Dazu gehören die Bereiche **Authentifizierung > Enterprise**, in dem die vertrauenswürdige Authentifizierung aktiviert und eine Datei mit dem gemeinsamen geheimen Schlüssel generiert wird, **Benutzer und Gruppen > Benutzerliste**, in dem ein Konto für einen vertrauenswürdigen Benutzer erstellt wird, und **Server > Serverliste > WACS > Eigenschaften**, in dem die Option *Abrufmethode* für */logon/trusted*-API-Anmeldetokenanforderungen ausgewählt wird.

1. Melden Sie sich an der Central Management Console als Administrator an.
2. Wechseln Sie zu **Authentifizierung** > **Enterprise**, und klicken Sie dann auf **Vertrauenswürdige Authentifizierung ist aktiviert**.
3. Klicken Sie auf **Neuer gemeinsamer geheimer Schlüssel** und dann auf **Gemeinsamen geheimen Schlüssel herunterladen**.
4. Klicken Sie auf **Speichern**, und legen Sie die Datei `TrustedPrincipal.conf` im Standardspeicherort, d.h. `<EnterpriseVerz>\<Plattform>`, ab.
   Beispiel-Speicherort:

   ```
   "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjectsEnterprise XI
   4.0\win64_x64\"
   ```

   > **Hinweis**
   >
   > Sie können den Standardspeicherort der Datei `TrustedPrincipal.conf` für gemeinsame geheime Schlüssel ändern, indem Sie in der CMC unter **Server > Serverliste > WACS > Eigenschaften > Befehlszeilenparameter** einen Befehlszeileneintrag hinzufügen und dann den WACS-Dienst neu starten. Beispiel: Ein Befehlszeileneintrag mit `-Dbobj.trustedauth.home=` und dem Ordner `SharedSecrets` am Stamm des Laufwerks `C:\` des BI-Plattformservers wird wie folgt angezeigt:
   >
   > ```
   > "-Dbobj.trustedauth.home=C:\SharedSecrets"
   > ```

   > **Hinweis**
   >
   > Sie können den Standardwert Null (0) der Option **Gültigkeitsdauer des gemeinsamen geheimen Schlüssels (Tage)** beibehalten. Der Schlüssel läuft dann nicht ab. Der Standardwert Null (0) der Option **Anforderung für vertrauenswürdige Anmeldung läuft nach N Millisekunde(n) ab** kann übernommen werden. Für vertrauenswürdige Anmeldeanforderungen gilt dann kein Zeitlimit.

5. Klicken Sie auf **Aktualisieren**, um die Änderung zu speichern.
6. Fügen Sie einen neuen Benutzer und ein neues Kennwort, z.B. `bob` und `Kennwort`, unter **Benutzer und Gruppen** > **Benutzerliste** mithilfe von **Verwalten > Neu > Neuer Benutzer** hinzu. Deaktivieren Sie **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**, und klicken Sie dann auf **Erstellen und schließen**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Sie können auch einen neuen Benutzer erstellen, indem Sie auf das Symbol *Neuen Benutzer erstellen* klicken oder mit der rechten Maustaste auf einem offenen Bereich des Fensters klicken, in dem Benutzernamen aufgelistet sind, und dann **Neu** > **Neuer Benutzer** auswählen.

7. Wechseln Sie zu **Server** > **Kerndienste** > **WACS** > **Eigenschaften**, blättern Sie nach unten zum Abschnitt *Konfiguration der vertrauenswürdigen Authentifizierung*, und wählen Sie im Menü *Abrufmethode* entweder **HTTP_HEADER**, **QUERY_STRING** oder **COOKIE** aus.

   > **Hinweis**
   >
   > Sie können optional die Standardbeschriftung der Option *Benutzernamensparameter* von `X-SAP-TRUSTED-USER` in eine andere geeignete ändern (z.B. `Benutzername`, `Kassierer` oder `Pfleger`), die von den RESTful-Webdienst-Entwicklern verwendet werden kann.

8. Starten Sie den Dienst neu, indem Sie mit der rechten Maustaste auf den WACS-Servernamen, z.B. `MySIA.WebApplicationContainerServer`, klicken und dann auf **Server neu starten** klicken.

   > **Hinweis**
   >
   > Wenn Sie die Option unter *Abrufmethode*, wie in Schritt 7 veranschaulicht, zu einem späteren Zeitpunkt ändern, muss der WACS nicht neu gestartet werden.

9.

12.1.8.2.4.3 Konfigurieren des Befehlszeilenparameters zum Verlagern der Konfigurationsdatei `TrustedPrincipal.conf` für gemeinsame geheime Parameter

Die RESTful-Webdienste bieten einen Befehlszeilenparameter, mit dem ein anderer Speicherort für die Datei `TrustedPrincipal.conf` für die vertrauenswürdige Authentifizierung gewählt werden kann.

Aktualisieren Sie die Befehlszeile des Web Application Container Servers (WACS) wie folgt mit einem benutzerdefinierten Pfad für die Datei `TrustedPrincipal.conf`:

1. Melden Sie sich als Benutzer "Administrator" an der Central Management Console an.
2. Klicken Sie auf **Server** und anschließend auf **Serverliste**.
3. Klicken Sie mit der rechten Maustaste auf den WACS-Dienst, z.B. `MySIA.WebApplicationContainerServer`, und klicken Sie dann auf **Eigenschaften**.
   Die Registerkarte **Eigenschaften** für den WACS-Server wird angezeigt.
4. Geben Sie im Bereich *Befehlszeilenparameter* den Pfad zu dem Verzeichnis ein, das die Datei `TrustedPrincipal.conf` enthält.

   Die Zeichenfolge ist, wie im folgenden Beispiel veranschaulicht, in doppelte Anführungszeichen eingeschlossen.

   ```
   "-Dbobj.trustedauth.home=C:\SharedSecrets"
   ```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Der Standardspeicherort der Datei `TrustedPrincipal.conf` lautet `<EnterpriseVerz>\<Plattform>`. Beispiel-Speicherort:
>
> ```
> C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64
> "
> ```

5. Klicken Sie auf **Speichern und schließen**.
6. Starten Sie den Dienst neu, indem Sie mit der rechten Maustaste auf den WACS-Servernamen, z.B. `MySIA.WebApplicationContainerServer`, klicken und dann auf **Server neu starten** klicken.

12.1.9 WACS und Ihre IT-Umgebung

In diesem Abschnitt wird beschrieben, wie Sie den WACS in einer komplexen Umgebung konfigurieren.

12.1.9.1 Verwenden des WACS mit anderen Webservern

Wenn ein Web Application Container Server (WACS) installiert wird, fungiert er als Anwendungsserver und Webserver, ohne dass zusätzliche Konfigurationsschritte erforderlich sind. Sie können unterstützte Webserver wie Internet-Informationsdienste (IIS) und Apache konfigurieren, um die URL-Weiterleitung an den WACS-Server auszuführen.

> **Hinweis**
>
> Die Weiterleitung von Anforderungen von IIS mithilfe eines ISAPI-Filters an den WACS wird nicht unterstützt.

Der WACS unterstützt kein Implementierungsszenario, in dem ein Webserver statischen Inhalt und ein WACS dynamischen Inhalt hostet. Statische und dynamische Inhalte müssen immer auf dem WACS gespeichert sein.

12.1.9.2 Verwenden von WACS mit einem Lastausgleichsmodul

Um den WACS in einer Implementierung mit einem Hardwaremodul für den Lastausgleich zu verwenden, konfigurieren Sie das Lastausgleichsmodul für die Verwendung von IP-Routing oder aktiven Cookies. Nachdem eine Benutzersitzung auf einem WACS eingerichtet wurde, können alle folgenden vom selben Benutzer abgesetzten Anforderungen an denselben WACS gesendet werden.

Der WACS wird nicht mit einem Hardwaremodul zum Lastausgleich unterstützt, das passive Cookies verwendet.

Wenn Ihr Hardwaremodul für den Lastausgleich SSL-verschlüsselte HTTPS-Anforderungen an den WACS weiterleitet, müssen HTTPS auf dem WACS konfiguriert und SSL-Zertifikate auf jedem WACS installiert werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wenn der HTTPS-Datenverkehr durch das Hardwaremodul für den Lastausgleich entschlüsselt und entschlüsselte HTTP-Anforderungen an Ihren WACS weitergeleitet werden, ist keine zusätzliche WACS-Konfiguration erforderlich.

Weitere Informationen

Konfigurieren von HTTPS/SSL [Seite 455]

12.1.9.3 Verwenden eines WACS mit einem Reverse Proxy

Ein WACS kann in einer Implementierung mit Forward- oder Reverseproxyserver eingesetzt werden. Der WACS selbst kann nicht als Proxyserver verwendet werden.

12.1.9.3.1 Konfigurieren des WACS für die Unterstützung von HTTP mit einem Reverseproxy

Um einen WACS in einer Implementierung mit einem Reverseproxy zu verwenden, konfigurieren Sie den WACS in der Weise, dass der HTTP-Port für die Kommunikation innerhalb einer Firewall (z.B. in einem sicheren Netzwerk) und der "HTTP über Proxy"-Port für die Kommunikation von außerhalb der Firewall (z.B. dem Internet) verwendet wird.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den WACS, den Sie konfigurieren möchten.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
3. Im Abschnitt *Konfiguration von "HTTP über Proxy"*:
   a) Aktivieren Sie **"HTTP über Proxy" aktivieren**.
   b) Geben Sie den HTTP-Port des WACS an, der für die Kommunikation über den Proxy verwendet wird.
   c) Geben Sie Proxy-Hostnamen und Proxy-Port des Proxyservers an.
4. Klicken Sie auf **Speichern und schließen**.

12.1.9.3.2 Konfigurieren des WACS für die Unterstützung von HTTPS mit einem Reverseproxy

Einige Lastausgleichsmodule und Reverseproxyserver können so konfiguriert werden, dass der HTTPS-Datenverkehr entschlüsselt und der entschlüsselte Verkehr an Ihre Anwendungsserver weitergeleitet wird. In diesem Fall können Sie WACS für die Verwendung von HTTP oder HTTP über Proxy konfigurieren.

Wenn HTTPS-Datenverkehr von Ihrem Lastausgleichsmodul oder Reverseproxy weitergeleitet wird und Sie HTTPS mit einem Reverseproxy konfigurieren möchten, erstellen Sie zwei WACS. Konfigurieren Sie einen WACS

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

für HTTPS für externen Datenverkehr über den Reverseproxy und den anderen WACS für die Kommunikation mit Clients im internen Netzwerk über HTTPS.

12.1.9.4 Verwenden von WACS mit Firewalls

Die Implementierung eines WACS in einer IT-Umgebung mit Firewalls wird unterstützt.

Der WACS wird standardmäßig an alle IP-Adressen auf dem Rechner gebunden, auf dem er installiert ist. Wenn Sie eine Firewall zwischen Clients und Ihrem WACS einsetzen möchten, muss erzwungen werden, dass der WACS für HTTP oder HTTP über Proxy an eine bestimmte IP-Adresse gebunden wird. Zu diesem Zweck deaktivieren Sie **An alle IP-Adressen binden** und geben einen Hostnamen oder eine IP-Adresse ein, an den bzw. die gebunden werden soll.

Falls Sie planen, eine Firewall zwischen dem WACS-Server und anderen BI-Plattform-Servern in Ihrer Implementierung zu verwenden, lesen Sie den Abschnitt "Erläuterung der Kommunikation zwischen BI-Plattform-Komponenten" im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.

Weitere Informationen

Erläuterung der Kommunikation zwischen BI-Plattform-Komponenten [Seite 183]

12.1.9.5 Konfigurieren des WACS auf einem mehrfach vernetzten Rechner

Ein mehrfach vernetzter Rechner ist ein Rechner mit mehreren Netzwerkadressen. Der HTTP-Port von Instanzen der Web Application Container Server wird standardmäßig an alle IP-Adressen gebunden. Wenn Sie den WACS an eine bestimmte Netzwerkschnittstellenkarte (NIC) binden, z.B. den HTTP-Port des WACS an eine NIC und den Anforderungs-Port an eine andere NIC:

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den WACS, den Sie konfigurieren möchten.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
3. Deaktivieren Sie im Abschnitt *HTTP-Konfiguration über Proxy* des Bereichs *Webanwendungs-Containerdienst* die Option **An alle IP-Adressen binden**, und geben Sie eine IP-Adresse für den WACS ein, an die der Server gebunden werden soll.
4. Deaktivieren Sie im Abschnitt *HTTP-Konfiguration* die Option **An alle IP-Adressen binden**, und geben Sie eine IP-Adresse oder einen Hostnamen für den WACS ein, an die der Server gebunden werden soll.
5. Deaktivieren Sie unter *Allgemeine Einstellungen* die Option **Automatisch zuweisen**, und geben Sie dann den Hostnamen oder die IP-Adresse der NIC ein, die für die Kommunikation zwischen dem WACS und den anderen BI-Servern in der Implementierung verwendet wird.
6. Klicken Sie auf **Speichern und schließen**.
7. Starten Sie den WACS neu.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12.1.10 Konfigurieren von Webanwendungseigenschaften

Die Eigenschaften von Webanwendungen, die auf einem WACS gehostet sind, können wie folgt konfiguriert werden:

- Eigenschaften, die oft geändert werden, stehen als konfigurierbare Diensteigenschaften für den WACS zur Verfügung. Öffnen Sie zum Bearbeiten dieser Eigenschaften die Seite *Eigenschaften* des WACS in der Central Management Console (CMC), ändern Sie den Wert für die jeweilige Eigenschaft, und klicken Sie auf **Speichern**.
- Zum Ändern der Zeitüberschreitung von Sitzungen für Webanwendungen, die auf dem WACS gehostet werden, bestimmen Sie zuerst, ob die Webanwendung über Eigenschaften verfügt, die sich in der CMC konfigurieren lassen.

  Wenn es für die Webanwendung Eigenschaften gibt, die in der CMC konfiguriert werden können, ändern Sie die Datei `web_xml.ino` für die Webanwendung. Die Datei lautet **`<Webanwendungsname>`**`_web_xml.ino`, wobei **`<Webanwendungsname>`** durch den Namen der Webanwendung zu ersetzen ist, die sich unter **`<Enterprise-Verzeichnis>`**`/java/pjs/services/`**`<Webanwendungsname>`** befindet.

  Wenn es für die Webanwendung keine Eigenschaften gibt, die in der CMC konfiguriert werden können, ändern Sie die Datei `web.xml` für die Webanwendung. Diese Datei befindet sich im **`<Enterprise-Verzeichnis>`**`/warfile/webapps/`**`<Webanwendungsname>`**, wobei **`<Webanwendungsname>`** durch den Namen der Webanwendung zu ersetzen ist.
- Zum Ändern von Eigenschaften, die sich nicht auf die Zeitüberschreitung von Sitzungen beziehen, oder die auf dem Bildschirm *Eigenschaften* für den WACS in der CMC zur Verfügung stehen, ändern Sie die Datei `.properties` für die Webanwendung. Weitere Informationen finden Sie im Abschnitt "Verwalten von Anwendungen über BOE.war-Eigenschaften" im *Administratorhandbuch für SAP BI*.

> **Hinweis**
>
> Ändern Sie nicht die Dateien `web.xml`, `web_xml.ino`, oder `.properties` unter **`<Enterprise-Verzeichnis>`**`/java/pjs/container/work/`**`<Serveranzeigename>`**, da Ihre Änderung bei jedem Start oder Neustart des WACS überschrieben wird.

> **Hinweis**
>
> Nachdem Sie die Eigenschaften für einen WACS geändert haben, müssen Sie den Server immer neu starten.

Weitere Informationen

Ändern der Eigenschaften eines Servers [Seite 392]
BOE-WAR-Datei [Seite 636]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12.1.11 Fehlerbehebung

12.1.11.1 Konfiguration der Ablaufverfolgung auf einem WACS

Informationen zur Konfiguration der Ablaufverfolgung für WACS finden Sie unter *Protokollieren der Ablaufverfolgung für Komponenten* [Seite 861]

12.1.11.2 So zeigen Sie die Servermetrik an

Sie können die Servermetriken eines WACS über die Central Management Console (CMC) anzeigen lassen.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Klicken Sie mit der rechten Maustaste auf den WACS, und klicken Sie auf **Metriken**.

Weitere Informationen

Web Application Container Server-Metriken [Seite 1002]

12.1.11.3 So lassen Sie den Status eines WACS anzeigen

Um den Status eines WACS anzeigen zu lassen, wechseln Sie zum Bereich *Server* der CMC. Die **Serverliste** umfasst die Spalte **Status**, in der der Status für jeden Server in der Liste angegeben ist.

Der WACS verfügt über einen Serverstatus mit dem Namen "Gestartet mit Fehlern". Dieser Status bedeutet, dass der WACS ausgeführt wird, jedoch eine oder mehrere der folgenden Fehlerbedingungen aufweist:

- Ein HTTP-, HTTP-über-Proxy- oder HTTPS-Connector ist falsch konfiguriert.
- Ein auf WACS ausgeführter Dienst, wie z.B. der Tracelog-Dienst wird nicht ordnungsgemäß ausgeführt.
- Eine Webanwendung konnte in WACS nicht implementiert werden.

Auf der WACS-Seite *Eigenschaften* finden Sie Informationen dazu, welche Dienste fehlgeschlagen sind.

12.1.11.4 Auflösen von Portkonflikten

Wenn Sie keine Seiten abrufen können, sobald Sie versuchen, über einen bestimmten Port auf die CMC zuzugreifen, sollten Sie sicherstellen, dass keine andere Anwendung die für den WACS festgelegten HTTP-, HTTP über Proxy- oder HTTPS-Ports übernommen hat.

Sie können auf zwei Arten feststellen, ob Portkonflikte beim WACS vorliegen. Wenn Ihre Implementierung über mehr als einen WACS verfügt, melden Sie sich bei der CMC an und aktivieren die Metriken "Liste der derzeit ausgeführten WACS-Konnektoren" und "WACS-Konnektor(en) bei Start fehlgeschlagen". Wenn ein HTTP-, HTTP-

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

über-Proxy- oder HTTP-Konnektor nicht in der "Liste der derzeit ausgeführten WACS-Konnektoren" angezeigt wird, kann er aufgrund eines Portkonflikts nicht gestartet werden.

Wenn Ihre Implementierung nur einen WACS umfasst oder Sie nicht in der Lage sind, über einen WACS auf die CMC zuzugreifen, verwenden Sie ein Dienstprogramm wie "netstat", um zu überprüfen, ob ein WACS-Port von einer anderen Anwendung belegt wurde.

12.1.11.4.1 So lösen Sie HTTP-Portkonflikte

1. Starten Sie den Central Configuration Manager (CCM), und klicken Sie auf das Symbol **Server verwalten**.
2. Geben Sie die Anmeldedaten an.
3. Stoppen Sie den WACS im Bildschirm *Server verwalten*.
4. Klicken Sie auf das Symbol **Webschicht-Konfiguration**.

   > **Hinweis**
   >
   > Das Symbol **Webschicht-Konfiguration** ist nur aktiviert, wenn Sie einen gestoppten WACS auswählen.

   Das Dialogfeld *Webschicht-Konfiguration* wird angezeigt.
5. Geben Sie im Feld **HTTP-Port** einen freien HTTP-Port an, der vom Web Application Container Server verwendet werden soll, und klicken Sie auf **OK**.
6. Starten Sie den WACS im Bildschirm *Server verwalten*.

12.1.11.4.2 So lösen Sie "HTTP über Proxy"- oder HTTPS-Portkonflikte

Wenn Sie nicht über den "HTTP über Proxy"- oder HTTPS-Port auf einen WACS zugreifen können, die Verbindung zur Central Management Console (CMC) über den HTTP-Port aber zustande kommt, ändern Sie die Portnummern über die CMC.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Um den zu konfigurierenden WACS zu stoppen, klicken Sie mit der rechten Maustaste auf den Server und klicken auf **Server stoppen**.
3. Doppelklicken Sie auf den WACS, den Sie konfigurieren möchten.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
4. Geben Sie im Abschnitt *Konfiguration von "HTTP über Proxy"* einen neuen HTTP-Port ein.
5. Um den HTTPS-Port zu ändern, geben Sie im Abschnitt *HTTPS-Konfiguration* im Feld **HTTPS-Port** einen neuen Wert ein.
6. Klicken Sie auf **Speichern und schließen**.
7. Um den WACS zu starten, klicken Sie mit der rechten Maustaste auf den Server und klicken auf **Server starten**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12.1.11.5 Ändern der Arbeitsspeichereinstellungen

Um die Serverleistung eines WACS zu verbessern, können Sie die dem Server zugewiesene Arbeitsspeicherkapazität über den Central Configuration Manager (CCM) ändern.

1. Starten Sie den CCM, und klicken Sie auf das Symbol **Server verwalten**.
2. Geben Sie die Anmeldedaten für den CMC an.
3. Stoppen Sie den WACS im Bildschirm *Server verwalten*.
4. Klicken Sie auf das Symbol **Webschicht-Konfiguration**.

   > **Hinweis**
   >
   > Das Symbol **Webschicht-Konfiguration** ist nur aktiviert, wenn Sie einen gestoppten WACS auswählen.

   Das Dialogfeld *Webschicht-Konfiguration* wird angezeigt.
5. Geben Sie unter *Befehlszeilenparameter* einen neuen Wert für den Arbeitsspeicher ein, indem Sie die Befehlszeile bearbeiten:
   a) Suchen Sie die Option *-Xmx*. Für diese Option ist normalerweise ein Wert angegeben.
      Beispiel: "-Xmx1g". Durch diese Einstellung wird dem Server 1 GB Arbeitsspeicher zugewiesen.
   b) Geben Sie einen neuen Wert für den Parameter an.
      - Um einen Wert in MB anzugeben, verwenden Sie "m". Beispiel: Durch "`-Xmx640m`" werden dem WACS-Arbeitsspeicher 640 MB zugewiesen.
      - Um einen Wert in GB anzugeben, verwenden Sie "g". Beispiel: Durch "`-Xmx2g`" werden dem WACS-Arbeitsspeicher 2 GB zugewiesen.
   c) Klicken Sie auf **OK**.
6. Starten Sie den WACS im Bildschirm *Server verwalten*.

12.1.11.6 Ändern der Anzahl gleichzeitiger Anforderungen

Die Standardanzahl der gleichzeitigen HTTP-Anforderungen, die vom WACS verarbeitet werden können, beträgt 150. Dieser Wert ist für die meisten Implementierungsszenarios ausreichend. Um die WACS-Leistung zu verbessern, können Sie die maximale Anzahl gleichzeitiger HTTP-Anforderungen erhöhen. Obwohl die Leistung optimiert werden kann, indem die Anzahl gleichzeitiger Anforderungen erhöht wird, kann ein zu hoher Wert die Leistung wieder mindern. Die ideale Einstellung hängt von den Hardware-, Software- und IT-Anforderungen ab.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Um den zu konfigurierenden WACS zu stoppen, klicken Sie mit der rechten Maustaste auf den Server und klicken auf **Server stoppen**.
3. Doppelklicken Sie auf den WACS, den Sie konfigurieren möchten.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
4. Geben Sie im Feld *Maximale Anzahl gleichzeitiger Anforderungen* unter **Einstellungen für gleichzeitigen Zugriff (pro Konnektor)** die gewünschte Anzahl gleichzeitiger Anforderungen ein, und klicken Sie auf **Speichern und schließen**.
5. Um den WACS zu starten, klicken Sie mit der rechten Maustaste auf den Server und klicken auf **Server starten**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

12.1.11.7 Wiederherstellen der Systemstandardwerte

Wenn Sie einen WACS falsch konfiguriert haben, können Sie die Systemstandardwerte über den Central Configuration Manager (CCM) wiederherstellen.

1. Starten Sie den CCM, und klicken Sie auf das Symbol **Server verwalten**.
2. Geben Sie die Anmeldedaten an.
3. Stoppen Sie den WACS im Bildschirm *Server verwalten*.
4. Klicken Sie auf das Symbol **Webschicht-Konfiguration**.

   > **Hinweis**
   >
   > Das Symbol **Webschicht-Konfiguration** ist nur aktiviert, wenn Sie einen angehaltenen WACS auswählen.

   Das Dialogfeld *Webschicht-Konfiguration* wird angezeigt.
5. Klicken Sie auf **Systemstandardwerte wiederherstellen**.
6. Geben Sie ggf. einen freien HTTP-Port an, und klicken Sie auf **OK**.
7. Starten Sie den WACS im Bildschirm *Server verwalten*.

12.1.11.8 Verhindern von Anmeldungen beim WACS über HTTP

In bestimmten Fällen möchten Sie vielleicht, dass nur Benutzer vom lokalen Rechner über HTTP oder HTTPS eine Verbindung zu einem WACS herstellen können. Obwohl der HTTP-Port nicht geschlossen werden kann, können Sie beispielsweise den WACS so konfigurieren, dass nur HTTP-Anforderungen von den Clients akzeptiert werden, die sich auf demselben Rechner wie der WACS befinden. So lassen sich Wartungs- oder Konfigurationsaufgaben auf dem WACS über einen Browser ausführen, der sich auf demselben Rechner wie der WACS befindet , und gleichzeitig werden andere Benutzer daran gehindert, auf den Server zuzugreifen.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den WACS, den Sie ändern möchten.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
3. Deaktivieren Sie im Abschnitt *Webanwendungs-Containerdienst* das Kontrollkästchen **An alle IP-Adressen binden**.
4. Geben Sie im Feld **An Hostnamen oder IP-Adresse binden** den Wert `127.0.0.1` ein, und klicken Sie auf **Speichern & schließen**.
5. Um den WACS zu starten, klicken Sie mit der rechten Maustaste auf den Server und klicken auf **Server starten**.
   Ein auf diese Weise konfigurierter WACS akzeptiert nur Verbindungen vom lokalen Rechner.

12.1.12 WACS-Eigenschaften

Eine vollständige Liste der allgemeinen HTTP-, HTTP über Proxy- und HTTPS-Konfigurationseigenschaften, die für WACS konfiguriert werden können, finden Sie im Abschnitt “Einstellungen für Core Server” unter “ Servereigenschaften (Anhang)”.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Kerndienste-Eigenschaften [Seite 950]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

13 Sichern und Wiederherstellen Ihres Systems

13.1 Übersicht über Sicherung und Wiederherstellung

In diesem Kapitel erfahren Sie, wie Sie die BI-Plattform sichern und das System bei Hardware- und Softwareausfällen sowie Datenverlust wiederherstellen. Zur Ausführung eines Sicherungs- und Wiederherstellungsplans benötigen Sie eine erfahrene SAP-BusinessObjects-Fachkraft, einen Systemadministrator und einen Datenbankadministrator.

Weitere Informationen

Sichern des gesamten Systems [Seite 491]
Sichern von BI-Inhalt [Seite 497]
Sichern der Servereinstellungen mit dem CCM unter Windows [Seite 495]
Sichern von Servereinstellungen unter Unix [Seite 496]
Übersicht des Kopierens des Systems [Seite 509]

13.2 Terminologie

Begriff	Definition
Datenreplikation	Als Datenreplikation wird der Prozess der Erstellung einer oder mehrerer Kopien Ihrer Daten bezeichnet. Die Kopien werden in Echtzeit aktualisiert, beispielsweise bei der Verwendung gespiegelter Laufwerke. Sie ermöglicht Echtzeit-Datensicherung vor physischer Datenbeschädigung, da die Laufwerke jedoch ständig aktualisiert werden, kann das System nicht in einen früheren Zustand zurückversetzt werden, wenn Daten beschädigt oder versehentlich entfernt werden.
Versionierung	Bei der Versionierung werden mehrere Versionen einer oder mehrerer bestimmter Dateien auf Ihrem System erstellt. In diesem Fall ist es möglich, Ihr System in einen früheren Zustand zurückzuversetzen. Alle Datenversionen werden in der Regel auf demselben Hostsystem gespeichert. Bei einer Beeinträchtigung oder Beschädigung des Systems riskieren Sie, sowohl die aktuelle Version als auch die älteren Versionen zu verlieren. Entsprechend werden durch Wiederherstellungsfunktionen Kopien von "gelöschten" Dateien für die spätere Wiederherstellung aufbewahrt, diese werden jedoch auch auf demselben Hostsystem wie die Originaldaten gespeichert. Dies bietet jedoch keinen Schutz vor physischer Datenbeschädigung (z.B. Datenträgerausfall).

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Begriff	Definition
Bare-Metal-Systemsicherung	Eine Bare-Metal-Systemsicherung ist eine Sicherung eines gesamten Dateisystems einschließlich Betriebssystem. Eine Bare-Metal-Systemsicherung soll zur Wiederherstellung eines gesicherten Systems auf Hardware dienen, die weder Software noch Betriebssystem enthält. Wenn eine Bare-Metal-Systemsicherung fehlschlägt, wird das gesamte Dateisystem (einschließlich Betriebssystem) auf einer identischen Hardware wiederhergestellt. Wenn Ihre Wiederherstellungstools die hardware-unabhängige Wiederherstellung unterstützen, kann das Dateisystem auch auf einer beliebigen Hardware wiederhergestellt werden.
Bare-Metal-Systemsicherung im Vergleich zur Anwendungssicherung	Bei einer Bare-Metal-Systemsicherung wird eine Kopie des gesamten Dateisystems einschließlich Betriebssystem erstellt. Dies ermöglicht das Zurücksetzen des gesamten Systems auf eine frühere Version. Bei einer Anwendungssicherung werden Dateien gesichert, die sich auf einzelne Anwendungen beziehen. Die BI-Plattform unterstützt Bare-Metal-Systemsicherungen, jedoch keine Anwendungssicherungen. Wenn eine Bare-Metal-Systemsicherung fehlschlägt, wird das gesamte Dateisystem (einschließlich Betriebssystem) auf einer identischen Hardware wiederhergestellt. Wenn Ihre Wiederherstellungstools die hardware-unabhängige Wiederherstellung unterstützen, kann das Dateisystem auch auf einer beliebigen Hardware wiederhergestellt werden. Eine vollständige BI-Plattform-Systemsicherung wird Sicherungssatz genannt.
Sicherungssatz	Ein Sicherungssatz umfasst die folgenden Sicherungen, die zu demselben Zeitpunkt erstellt wurden: • Eine Sicherungskopie der CMS-Systemdatenbank • Eine Bare-Metal-Sicherung des gesamten Dateisystems, einschließlich Betriebssystem, aller Rechner in der BI-Plattform-Implementierung • Eine Sicherungskopie der Input-FRS- und Output-FRS-Dateispeicher (falls diese nicht Bestandteil des Dateisystems der BI-Plattform sind) • Eine Sicherungskopie der Webschichtkomponenten (falls diese nicht Bestandteil des Dateisystems der BI-Plattform sind) • Eine Sicherungskopie der Audit-Datenbank
Coldbackup im Vergleich zu Hotbackup	Ein Coldbackup wird durchgeführt, während das System gestoppt und nicht für Benutzer verfügbar ist. Hotbackups werden durchgeführt, wenn das System ausgeführt wird und den Benutzern zur Verfügung steht, und Daten können sich während der Sicherung ändern. Bei der Durchführung eines Hotbackups müssen die Sicherungsschritte in der entsprechenden Reihenfolge ausgeführt werden, was bei einem Coldbackup nicht der Fall ist. Die BI-Plattform unterstützt sowohl Cold- als auch Hotbackups. Das Hotbackup wird teilweise auch als “Onlinebackup” bezeichnet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

13.3 Anwendungsfälle für Sichern und Wiederherstellen

In der folgenden Tabelle sind verschiedene Ziele, die Sie sich unter Berücksichtigung der vorhandenen Ressourcen unter Umständen gesetzt haben, sowie die am besten für Sie geeignete Sicherheitslösung aufgeführt.

Ziel	Erforderliche Ressourcen	Lösung
Ziel: Wiederherstellen eines Systems 1. Mein BI-Plattformsystem wurde beschädigt. Daher muss ich es wieder in einen funktionierenden Zustand versetzen, in dem es zum Zeitpunkt der letzten Sicherung war. 2. Ein Rechner, auf dem die BI-Plattform gehostet wurde, wurde beschädigt. Ich muss ihn durch einen neuen Rechner ersetzen.	• Ein Zielsystem mit identischer Hardware wie im Quellsystem UND • Sicherungen des Quellsystems	Gehen Sie anhand des Workflows zum Sichern und Wiederherstellen des Systems in diesem Handbuch vor. Siehe das Verfahren unter *Sichern des gesamten Systems* [Seite 491]. Erstellen Sie das Zielsystem aus Sicherungskopien des Quellsystems neu.
Ziel: Wiederherstellen von Objekten Ich möchte ein Dokument oder ein anderes Objekt, das versehentlich gelöscht wurde, wiederherstellen.	• Sicherungen von Datenbanken und Dateien des Quellsystems UND • Detaillierte Systeminformationen, die in *Exportieren aus einem Quellsystem* [Seite 513] beschrieben sind	Erstellen Sie mithilfe von Sicherungen eine Kopie des Systems auf einem anderen Rechner über den im Kapitel " Kopieren Ihrer BI-Plattform-Implementierung" beschriebenen Workflow zum Erstellen einer Systemkopie. Verwenden Sie anschließend das Hochstufungsverwaltungstool, um die versehentlich gelöschten Objekte aus dem neuen System hochzustufen. Gehen Sie anhand des Workflows zum Kopieren von Systemen vor. Beginnen Sie mit *Planen des Kopierens Ihres Systems* [Seite 510], und folgen Sie den Anweisungen im restlichen Kapitel. **Hinweis** Sie können das Zielsystem auf einem Rechner mit einer vorhandenen BI-Plattform-Implementierung erstellen, die dieselbe Version, dasselbe Support Package und dieselbe Patch-Ebene aufweist, oder auf einem "neuen" Computer ohne installierte BI-Plattform.
Ziel: Wiederherstellen von Objekten 2 Ich möchte ein Dokument oder ein anderes Objekt, das versehentlich gelöscht wurde, wiederherstellen.	Ein System mit Hochstufverwaltungsversionierung	Stellen Sie mithilfe der Hochstufverwaltung eine ältere Version des Dokuments wieder her. Einzelheiten hierzu finden Sie im verwandten Thema zur Hochstufverwaltung.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ziel	Erforderliche Ressourcen	Lösung
Ziel: Sichern von Objekten Ich möchte einige Objekte (z.B. Dokumente, Ordner, Benutzer) sichern.	Ein System mit Hochstufverwaltungsversionierung	Sichern Sie den BI-Inhalt mithilfe der Hochstufverwaltung, und exportieren Sie dann den Inhalt in Business-Intelligence-Archive-Dateien (LCMBIAR-Dateien). Wenn Inhalt beschädigt wird oder verloren geht, können Sie ihn später wiederherstellen, ohne das gesamte System wiederherzustellen. Einzelheiten hierzu finden Sie im verwandten Thema zur Hochstufverwaltung.

Weitere Informationen

Sicherungen [Seite 490]
Planen des Kopierens Ihres Systems [Seite 510]
Übersicht [Seite 521]

13.4 Sicherungen

Ein Sicherungs- und Wiederherstellungsplan besteht aus Schritten, die im Falle eines Systemausfalls aufgrund einer Naturkatastrophe oder eines unerwarteten Fehlers ergriffen werden müssen. Der Plan dient der Minimierung der Auswirkungen der Katastophe auf die täglichen Arbeitsabläufe, damit Sie wichtige Funktionen aufrechterhalten oder rasch wieder aufnehmen können.

Zur Sicherung der BI-Plattform-Implementierung haben Sie drei Optionen:

- Sicherung des gesamten Systems, was die Wiederherstellung des gesamten Systems ermöglicht. In diesem Fall ist eine Wiederherstellung von lediglich einem Teil des Systems nicht möglich. Wenn Sie die BI-Plattform neu erstellen möchten, anstatt sie anhand einer Sicherung wiederherzustellen, lesen Sie das zugehörige Thema über das Erstellen von Systemkopien.
- Sicherung der Servereinstellungen, was die Wiederherstellung lediglich der Servereinstellungen ohne Wiederherstellung anderer Objekte ermöglicht, wobei der aktuelle Status des BI-Inhalts des Systems aufrechterhalten bleibt.
- Sicherung von BI-Inhalten (z.B. Dokumente), was eine selektive Wiederherstellung von Teilen des BI-Inhalts ermöglicht, ohne dass alle Objekte wiederhergestellt werden müssen.

Einzelheiten zu allen drei Sicherungsarten finden Sie in den verwandten Themen.

➡ Tipp

Führen Sie regelmäßig Sicherungen durch, um Datenverluste zu vermeiden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

➔ Tipp

Sie können eine Sicherung eines BI-Plattform-Systems erstellen und es dann auf demselben oder einem anderen Hostrechner wiederherstellen, um eine Kopie des Systems zu erstellen.

Weitere Informationen

Sichern des gesamten Systems [Seite 491]
Sichern der Servereinstellungen [Seite 494]
Sichern von BI-Inhalt [Seite 497]
Übersicht des Kopierens des Systems [Seite 509]

13.4.1 Sichern des gesamten Systems

Sichern Sie das gesamte BI-Plattformsystem, indem Sie ein Cold- oder Hotbackup durchführen, wodurch ein Sicherungssatz erstellt wird. Wenn Sie mehrere Sicherungssätze von unterschiedlichen Zeitpunkten aufbewahren, haben Sie mehr Optionen beim Wiederherstellen des Systems. Sichern Sie Ihr System so oft wie für die Geschäftsanforderungen Ihres Unternehmens erforderlich.

Sie können das BI-Plattformsystem stoppen und ein Coldbackup durchführen, oder Sie können ein Hotbackup durchführen. Bei einem Hotbackup bleibt das System weiter betriebsbereit und ist während des Sicherungsprozesses für die Benutzer verfügbar. Dies hat den Vorteil, dass keine Systemausfallzeit entsteht.

ℹ Hinweis

Das Transaktionsprotokoll sollte in ein anderes Dateisystem als das Hauptdatenbank-Serversystem geschrieben werden und regelmäßig Sicherungen dieses Transaktionsprotokolls erstellen, und es zusammen mit den anderen Dateien im Sicherungsdatensatz ablegen.

ℹ Hinweis

Stellen Sie beim Erstellen einer Sicherungkopie von Audit-Daten sicher, dass das Datenbank-Transaktionsprotokoll für die Audit-Datenbank im Sicherungssatz enthalten ist. Es müssen keine temporären Audit-Dateien in der Sicherungskopie enthalten sein.

13.4.1.1 Hotbackups

Mit der Funktion "Hotbackup" können Sie das BI-Plattformsystem sichern, während die Benutzer gleichzeitig im System weiterarbeiten können. Falls Ihr Unternehmen während der Sicherung Ihres Systems den Arbeitsbetrieb aufrechterhalten muss, aktivieren und konfigurieren Sie Hotbackups in der Central Management Console.

Über die Einstellung **Maximale Dauer des Hotbackups** wird die maximale Zeitdauer, die das Hotbackup in Anspruch nehmen darf, festgelegt – von dem Zeitpunkt, an dem die CMS-Sicherung beginnt, bis zu dem

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Zeitpunkt, an dem die FRS-Sicherung endet. Ist die angegebene Dauer zu kurz, können Dateien gelöscht werden, bevor sie vom Sicherungsprogramm kopiert werden können. Um dies zu vermeiden, ist es sicherer, die für die Sicherung benötigte Zeit zu überschätzen. Berücksichtigen Sie bei dieser Frage die Systemressourcen, da ein hoher Wert den FRS-Dateispeicher geringfügig vergrößern kann.

> **Hinweis**
>
> Das Hotbackup ist aktiviert, solange das Kontrollkästchen **Hotbackup aktivieren** in der CMC ausgewählt ist. Die Einstellung für **Maximal Dauer des Hotbackups** wirkt sich nicht darauf aus, ob das Hotbackup aktiviert ist.

Das System wird am besten zu einer bestimmten Sicherungszeit wiederhergestellt. Wenn Ihre Systemsicherungen beispielsweise täglich um 3 Uhr ausgeführt werden, können Sie das System auf einfache Weise wieder in dem Zustand wiederherstellen, den es zu Beginn der CMS-Systemsicherung hatte (3 Uhr am Datum Ihrer Wahl). Wenn die Transaktionsprotokollierung auf der CMS-Datenbank oder der Audit-Datenbank aktiviert ist, können Sie nach dem Ausfall einer dieser Datenbanken das System in dem Zustand wiederherstellen, den es unmittelbar vor dem Ausfall hatte.

Um die größtmögliche Sicherheit zu gewährleisten, speichern Sie die Transaktionsprotokollierungsdatensätze an einem anderen Speicherort als die primären Datenbanksicherungsdatensätze. Dadurch wird sichergestellt, dass bei einem Datenbankfehler die Datenbank wieder in den Zustand zurückversetzt werden kann, in dem sie sich kurz vor dem Ausfall befand.

> **Hinweis**
>
> Aufgrund einer Größenbeschränkung für das Transaktionsprotokoll auf älteren Versionen von IBM DB2 werden Aufgaben in Zusammenhang mit Hotbackups und dem Transaktionsprotokoll nur dann unterstützt, wenn die CMS-Systemdatenbank unter der DB2-Datenbankserver-Version 9.5 Fixpack 5 oder neuer (für die 9.5-Linie) oder 9.7 Fixpack 1 oder neuer (für die 9.7-Linie) gehostet wird.

> **Hinweis**
>
> Es wird empfohlen, das Transaktionsprotokoll in ein anderes Dateisystem als das Hauptdatenbank-Serversystem zu schreiben, regelmäßig Sicherungen des Transaktionsprotokolls zu erstellen und es zusammen mit den anderen Dateien im Sicherungsdatensatz abzulegen.

Unter Umständen wird die Dateiänderung während des Hotbackups von folgenden Komponenten nicht unterstützt: Clients von Crystal Reports 2013 Designer, Web-Intelligence-Rich-Clients und Universe-Design-Tool-Clients, die älter als 4.0 FP3 sind, und selbst entwickelte Thick-Client-Anwendungen, die mit SDK-Versionen vor 4.0 FP3 kompiliert wurden. Wenn diese Clientanwendungen während der Sicherungen BI-Inhalt ändern, können sie die Qualität der während der Sicherung geänderten Daten beeinträchtigen. Sie können verhindern, dass Clientanwendungen Dokumente ändern, sodass die Konsistenz gesicherter Daten gewährleistet wird. Aktualisieren Sie Clientanwendungen nach Möglichkeit auf 4.0 FP3. Andernfalls sollten Sie Umgehungslösungen finden. Sie können beispielsweise Benutzer von Clientanwendungen auffordern, die vorhandenen Objekte zu löschen und neue Versionen zu speichern, anstatt die Objekte zu ändern.

13.4.1.1.1 Aktivieren von Hotbackups

1. Öffnen Sie die Central Management Console (CMC).

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Öffnen Sie im Bereich *Verwalten* die Seite **Einstellungen**.
3. Wählen Sie im Abschnitt *Hotbackup* die Option **Hotbackup aktivieren**.
4. Geben Sie die geschätzte maximale Anzahl an Minuten für die Sicherung unter **Maximale Dauer des Hotbackups (Minuten)** ein.

   Stellen Sie sicher, dass die für die Sicherung der CMS-Datenbank und des Dateisystems benötigte Zeit auf dem Hostrechner der BI-Plattform berücksichtigt wurde.

   > **Hinweis**
   >
   > Falls die tatsächliche Dauer der Sicherung länger als der hier eingegebene Wert ist, können Inkonsistenzen in den gesicherten Daten auftreten. Um dies zu vermeiden, ist es sicherer, die für die Sicherung benötigte Zeit zu überschätzen.

5. Damit ältere (vor 4.0 FP3) Anwendungen von Web-Intelligence-Rich-Client, Crystal Reports Designer oder mit dem SDK selbst entwickelte Thick-Client-Anwendungen Dokumente im System ändern können, aktivieren Sie das Kontrollkästchen **Support für ältere Anwendungen aktivieren (Sicherungsbeschränkungen)**.

   Wenn Sie die Änderung von Dokumenten durch ältere Clientanwendungen während Sicherungsvorgängen zulassen, könnte dies zu Inkonsistenzen in den während der Sicherung geänderten Dokumenten führen. Weitere Informationen zu Einschränkungen bei der Sicherung finden Sie in der zugehörigen Verknüpfung zu Hotbackups.
6. Klicken Sie auf **Aktualisieren**.
   Der Hotbackup ist aktiviert.

Nach der Aktivierung der Hotbackup-Unterstützung können Sie Sicherungen mit den Datenbank- und Dateisystemsicherungstools Ihres Anbieters durchführen.

Weitere Informationen

Hotbackups [Seite 491]
Durchführen eines Hot- oder Coldbackups des Systems [Seite 493]

13.4.1.2 Durchführen eines Hot- oder Coldbackups des Systems

Informationen zum Durchführen eines Hotbackups finden Sie in dem zugehörigen Thema über Voraussetzungen und weitere Informationen für Hotbackups. Wenn Sie ein Coldbackup durchführen, stoppen Sie alle Knoten auf Ihrer BI-Plattform-Implementierung.

> **Achtung**
>
> Wenn Sie eine Sicherung durchführen, ohne Hotbackups zu aktivieren und ohne alle Knoten zu stoppen, kann dies zu Dateninkonsistenzen zwischen der CMS-Datenbank und dem FRS-Dateispeicher führen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Bei Hotbackups ist es wichtig, dass die Prozesse in der beschriebenen Reihenfolge durchgeführt werden. Bei Coldbackups können die Prozesse in beliebiger Reihenfolge durchgeführt werden. Es ist in beiden Fällen jedoch nicht erforderlich zu warten, bis jede einzelne Sicherung abgeschlossen ist, bevor mit dem nächsten Schritt begonnen wird.

1. Verwenden Sie die Datenbank-Provider-Tools zum Sichern der CMS-Systemdatenbank (Central Management Server).

   > **Hinweis**
   >
   > Verwenden Sie bei Hotbackups die Sicherungstools des Datenbank-Providers im atomaren Onlinemodus.

2. Verwenden Sie Ihre Datenbank-Provider-Tools im atomaren Onlinemodus zum Sichern der BI-Plattform-Audit-Datenbank.
3. Sichern Sie das gesamte Dateisystem, einschließlich des Betriebssystems aller Rechner in der BI-Plattform-Implementierung.
   a) Wenn die Input- und Output-FRS-Dateispeicher bei der Sicherung der BI-Plattform nicht einbezogen werden (separate Hostrechner), erstellen Sie anhand Ihrer Dateisicherungstools von beiden eine Sicherungskopie.
   b) Wenn die Webschichtkomponenten bei der Sicherung der BI-Plattform nicht einbezogen werden (separate Hostrechner), erstellen Sie anhand Ihrer Dateisicherungstools eine Sicherungskopie.

   Verwenden Sie für Hotbackups nach Möglichkeit atomarische Dateisicherungstools.

Wenn Sie einen Coldbackup durchgeführt haben, warten Sie, bis alle Sicherungen abgeschlossen sind, und starten Sie dann die BI-Plattformknoten.

Weitere Informationen

Hotbackups [Seite 491]

13.4.2 Sichern der Servereinstellungen

Zum Schutz des Systems vor falsch konfigurierten Servereinstellungen sichern Sie die Servereinstellungen regelmäßig in einer BIAR-Datei. Wenn Sicherungen der Server verfügbar sind, können Sie Einstellungen wiederherstellen, ohne dass die CMS-Systemdatenbank (Central Management Server), Datei-Repositorys oder Business-Intelligence-Inhalt wiederhergestellt werden müssen.

Die Servereinstellungen müssen unbedingt jedes Mal gesichert werden, wenn Sie Änderungen an der Implementierung des Systems vornehmen. Dazu gehört auch das Erstellen, Umbenennen, Verschieben und Löschen von Knoten oder Erstellen oder Löschen von Servern. Sie sollten die Servereinstellungen sichern, bevor Sie die Einstellungen ändern, und erneut, wenn Sie mit den vorgenommenen Einstellungen zufrieden sind.

Sichern Sie die Servereinstellungen der BI-Plattform mit dem Central Configuration Manager (CCM) oder einem Skript in einer BIAR-Datei, und speichern Sie die Datei danach auf einem separaten Computer oder Speichermedium.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Wenn Sie Servereinstellungen in einer Implementierung sichern oder wiederherstellen, in der SSL aktiviert ist, müssen Sie SSL zunächst über den CCM deaktivieren und nach Abschluss der Sicherung oder Wiederherstellung wieder aktivieren.

Unter Windows finden Sie das Skript `BackupCluster.bat` im Verzeichnis `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

Unter Unix finden Sie das Skript `backupcluster.sh` im Verzeichnis `/<INSTALLVERZ>/sap_bobj/enterprise_xi40/<plattform64>/scripts`.

Weitere Informationen

Konfigurieren des SSL-Protokolls [Seite 179]

13.4.2.1 Sichern der Servereinstellungen mit dem CCM unter Windows

Mit diesen Schritten werden die Servereinstellungen für den gesamten Cluster gesichert. Es ist nicht möglich, die Einstellungen für einzelne Server zu sichern.

> **Hinweis**
>
> Bei Verwendung eines temporären CMS müssen Sie den CCM auf einem Rechner verwenden, auf dem lokale CMS-Binärdateien installiert sind.

1. Starten Sie den CCM, und klicken Sie in der Symbolleiste auf **Serverkonfiguration sichern**.
   Der *Assistent zum Sichern der Serverkonfiguration* wird angezeigt.
2. Klicken Sie auf **Weiter**, um den Assistenten zu starten.
3. Geben Sie an, ob die Serverkonfigurationseinstellungen mithilfe eines vorhandenen CMS gesichert werden sollen oder ob ein temporärer CMS erstellt werden soll.
   - Zum Sichern der Servereinstellungen von einem System, das gerade ausgeführt wird, wählen Sie **Vorhandenen ausgeführten CMS verwenden**, und klicken Sie auf **Weiter**.
   - Zum Sichern der Servereinstellungen von einem System, das nicht ausgeführt wird, wählen Sie **Neuen temporären CMS starten** aus und klicken auf **Weiter**.
4. Wenn Sie einen temporären CMS verwenden, wählen Sie eine Portnummer für die Ausführung des CMS aus, und geben Sie die Datenbankverbindungsinformationen an.

   Um weitgehend auszuschließen, dass Benutzer auf das System zugreifen, während Sie es wiederherstellen, geben Sie eine Portnummer an, die nicht mit den von dem vorhandenen CMS verwendeten Portnummern identisch ist.
5. Geben Sie den Clusterschlüssel ein, und klicken Sie auf **Weiter**, um fortzufahren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6. Wenn Sie dazu aufgefordert werden, melden Sie sich beim CMS an, indem Sie das System, den Benutzernamen und das Kennwort eines Kontos mit Administratorrechten angeben, und klicken Sie auf **Weiter**, um fortzufahren.
7. Geben Sie den Speicherort und den Namen einer BIAR-Datei an, in die die Serverkonfigurationseinstellungen gesichert werden sollen, und klicken Sie auf **Weiter**, um fortzufahren.
   Auf der Seite *Bestätigung* werden die von Ihnen angegebenen Informationen angezeigt.
8. Prüfen Sie, ob die auf der Seite *Bestätigung* angezeigten Informationen korrekt sind, und klicken Sie auf **Fertig stellen**, um fortzufahren.
   Der CCM sichert die Serverkonfigurationseinstellungen für den gesamten Cluster in der BIAR-Datei, die Sie angeben. Die Details der Sicherungsprozedur werden in eine Protokolldatei geschrieben. Der Name und der Pfad der Protokolldatei werden in einem Dialogfeld angezeigt.
9. Falls die Sicherung fehlgeschlagen ist, suchen Sie in der Protokolldatei nach dem Grund.
10. Klicken Sie auf **OK**, um den Assistenten zu schließen.

13.4.2.2 Sichern von Servereinstellungen unter Unix

Verwenden Sie unter Unix das Skript `serverconfig.sh`, um die Servereinstellungen der Implementierung in eine BIAR-Datei zu sichern.

1. Wählen Sie **5 – Serverkonfiguration sichern** aus, und drücken Sie die *Eingabetaste*.
2. Geben Sie an, ob die Serverkonfigurationseinstellungen mithilfe eines vorhandenen CMS gesichert werden sollen oder ob ein temporärer CMS erstellt werden soll.
   - Um Servereinstellungen von einem laufenden System zu sichern, wählen Sie **vorhandene** aus, und drücken Sie die *Eingabetaste*.
   - Um Servereinstellungen von einem nicht laufenden System zu sichern oder Servereinstellungen wiederherzustellen, wählen Sie **temporär** aus, und drücken Sie die *Eingabetaste*.
3. Falls Sie zum Sichern der Servereinstellungen einen temporären CMS verwenden, wählen Sie auf den nächsten Bildschirmen eine Portnummer für die Ausführung des temporären CMS und die Verbindungsinformationen für die CMS-Systemdatenbank aus.

   Um weitgehend auszuschließen, dass Benutzer auf das System zugreifen, während Sie es wiederherstellen, geben Sie eine Portnummer an, die nicht mit den von dem vorhandenen CMS verwendeten Portnummern identisch ist.
4. Melden Sie sich bei entsprechender Aufforderung am CMS an, indem Sie den System- und Benutzernamen sowie das Kennwort eines Kontos mit Administratorberechtigungen angeben und die *Eingabetaste* drücken.
5. Geben Sie bei entsprechender Eingabeaufforderung den Speicherort und den Namen einer BIAR-Datei an, in die die Serverkonfigurationseinstellungen gespeichert werden sollen, und drücken Sie die *Eingabetaste*.
   Die von Ihnen angegebenen Informationen werden auf einem Übersichtsseite angezeigt.
6. Stellen Sie sicher, dass die angezeigten Informationen richtig sind, und drücken Sie die *Eingabetaste*, um fortzufahren.
   Das Skript `serverconfig.sh` sichert die Serverkonfigurationseinstellungen für den gesamten Cluster in die angegebene BIAR-Datei. Details des Sicherungsvorgangs werden in eine Protokolldatei geschrieben. Name und Pfad der Protokolldatei werden angezeigt.
7. Falls die Sicherung fehlgeschlagen ist, suchen Sie in der Protokolldatei nach dem Grund.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

13.4.2.3 Sichern von Servereinstellungen mit einem Skript

Sie können die Servereinstellungen Ihrer Implementierung sichern, indem Sie die Datei `BackupCluster.bat` unter Windows oder das Skript `backupcluster.sh` unter Unix ausführen.

Unter Windows finden Sie die Datei `BackupCluster.bat` im Verzeichnis **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

Unter Unix befindet sich die Datei `backupcluster.sh` im Verzeichnis `/`**<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/`**<platform64>**`/scripts`.

Weitere Informationen

BackupCluster- und RestoreCluster-Skript [Seite 506]

13.4.3 Sichern von BI-Inhalt

Die Hochstufverwaltung sollte verwendet werden, um Ihre Business-Intelligence-Inhalte, wie z.B. Berichte, Benutzer und Gruppen sowie Universen, regelmäßig zu sichern. Mit aktuellen Sicherungen Ihrer Inhalte kann Business Intelligence wiederhergestellt werden, ohne dass eine Wiederherstellung des gesamten Systems oder Ihrer Servereinstellungen erforderlich ist.

Weitere Informationen zur Verwendung der Hochstufverwaltung finden Sie im Kapitel “Hochstufverwaltung”.

Informationen zur Verwendung von Subversion in Kombination mit der Hochstufverwaltung finden Sie im Kapitel “ Versionsverwaltung”.

13.5 Wiederherstellen des Systems

Wenn das System fehlerhaft oder beschädigt ist, können Sie das gesamte System wiederherstellen, wobei die BI-Plattform wiederhergestellt wird. Ob eine vollständige Wiederherstellung erforderlich ist, hängt von Zustand des Systems ab. Wenn das System normal arbeitet, aber Inhalt verloren gegangen ist oder beschädigt wurde, können Sie entscheiden, nur den Business-Intelligence-Inhalt (BI-Inhalt) wiederherzustellen. Falls der BI-Inhalt gültig ist, aber die Konfiguration Ihrer Plattformserver fehlerhaft ist, haben Sie die Möglichkeit, nur die Servereinstellungen wiederherzustellen.

Das Verfahren zum Wiederherstellen eines Hotbackup oder Coldbackups ist das gleiche.

Weitere Informationen

Wiederherstellen des gesamten Systems [Seite 498]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wiederherstellen der Servereinstellungen [Seite 503]
Wiederherstellen von BI-Inhalt [Seite 506]

13.5.1 Wiederherstellen des gesamten Systems

Wenn Sie das gesamte System wiederherstellen, wird das BI-Plattform-Cluster ebenfalls wiederhergestellt. Abhängig davon, was im System fehlgeschlagen ist, haben Sie u.U. die Möglichkeit, nur eine teilweise Wiederherstellung durchzuführen.

Wenn eine der folgenden Komponenten fehlgeschlagen oder verloren gegangen ist, stellen Sie das gesamte System wieder her:

- die CMS-Datenbank

  Hinweis

  Wenn die restliche BI-Plattform normal arbeitet, aber die CMS-Datenbank abgestürzt ist, können Sie diese wiederherstellen, ohne das gesamte System wiederherzustellen.

- der FRS-Dateispeicher
- das Dateisystem des Rechners

Hinweis

Für das Zielsystem ist es für eine vollständige Wiederherstellung des Systems nicht erforderlich, dass die BI-Plattform bereits installiert ist.

Wenn nur die Audit-Datenbank beschädigt oder verloren gegangen ist, können Sie sie wiederherstellen, ohne das gesamte System wiederherzustellen.

Wenn der Webschicht-Inhalt beschädigt oder verloren gegangen ist, können Sie ihn wiederherstellen, ohne das gesamte System wiederherzustellen.

Weitere Informationen

Wiederherstellen des gesamten Systems [Seite 498]
Wiederherstellen ausschließlich der Audit-Datenbank [Seite 500]
Wiederherstellen von Webschicht-Inhalt [Seite 500]
Wiederherstellen ausschließlich der CMS-Datenbank [Seite 501]

13.5.1.1 Wiederherstellen des gesamten Systems

Vor der Wiederherstellung des Systems müssen Sie sämtliche Knoten in der BI-Plattform-Implementierung über den Central Configuration Manager (CCM) stoppen und den Zeitpunkt auswählen, auf den das System zurückgesetzt werden soll.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Falls Sie den aktuellen Zustand des Systems wiederherstellen möchten, sichern Sie das System vor der Wiederherstellung.

1. Suchen Sie folgende Sicherungsdateien:
   - CMS-Datenbanksicherung
   - Sicherungen der Input-FRS- und Output-FRS-Dateispeicher
   - Sicherungen der Dateisysteme für jeden Hostrechner im BI-Plattform-Cluster

   > **Hinweis**
   >
   > Stellen Sie sicher, dass Sie die Sicherungen validieren, und dass alle oben aufgeführten Dateien aus demselben Sicherungssatz stammen. Wenn der Sicherungssatz als Hotbackup abgerufen wurde, stellen Sie sicher, dass der Startzeitstempel der CMS-Datenbanksicherung zeitlich früher als der entsprechende Zeitstempel für FRS-Dateispeicher, Webschicht und Host-Rechner-Dateisystem liegt. Alle diese Dateien sind erforderlich, auch wenn nur eine Komponente fehlgeschlagen ist.
2. Verwenden Sie Ihre Dateiwiederherstellungstools zum Wiederherstellen des Dateisystems aller Hostrechner im BI-Plattform-Cluster.
3. Verwenden Sie Ihre Dateiwiederherstellungstools zum Wiederherstellen der Input- und Output-FRS-Dateispeicher.
4. Stellen Sie die CMS-Datenbank mit Ihren Datenbanktools wieder her.
5. Wenn Sie das Kennwort der CMS-Datenbank nach dem Erstellen der Sicherung geändert haben, aktualisieren Sie es über den CCM auf allen Knoten und Hostrechnern der BI-Plattform.
6. Wenn Sie die Audit-Funktion verwenden:
   a) Suchen Sie die letzten Sicherungen und Transaktionsprotokolle für die Audit-Datenbank.
   b) Verwenden Sie die Datenbanktools zum Wiederherstellen der Audit-Datenbank.
   c) Führen Sie ein Rollforward für die Audit-Datenbank durch, und wiederholen Sie das Transaktionsprotokoll.
7. Wählen Sie eine der folgenden Optionen zum Wiederherstellen des Suchindex aus:
   - Wenn Sie das Suchindex-Wiederherstellungskript ausführen möchten, lesen Sie den Abschnitt *Ausführen des Suchindex-Wiederherstellungsskripts* [Seite 502] und befolgen Sie die darin enthaltenen Anweisungen. Dies ermöglicht eine schnellere Wiederherstellung des vollständigen Index.
   - Wenn Sie Ihren Suchindex lieber neu erstellen möchten, anstatt das Wiederherstellungsskript zu verwenden, starten Sie Ihre BI-Plattform-Knoten anhand des CCM. Dies ist ein einfacheres Verfahren, jedoch haben Sie während der Neuerstellung des Index nur teilweisen Suchzugriff auf die Plattformdaten.
8. Starten Sie das System, und notieren Sie die Zeit zur Verwendung in den nachfolgenden erforderlichen Schritten.
9. Verifizieren Sie, dass das System erwartungsgemäß funktioniert, und führen Sie eine Integritätsprüfung durch.

Führen Sie nach Verifizierung des Systems folgende Schritte aus:

- Führen Sie das Repository Diagnotic Tool aus, um nicht verwendete temporäre Dateien zu entfernen und überprüfen Sie die Konsistenz des Repositorys. Siehe Abschnitt "Repository Diagnostic Tool" dieses Handbuchs.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Falls Sie das Index-Wiederherstellungsskript nicht verwendet haben, erstellen Sie Ihren Plattform-Suchindex neu.
- Veröffentlichungsaufträge, die während der Sicherung des Systems ausgeführt wurden, werden als fehlgeschlagen angezeigt. Führen Sie diese Instanzen nicht erneut aus, sondern starten Sie einen neuen Veröffentlichungsauftrag.
- Wenn Ihre Audit-Datenbank wiederhergestellt wurde, führen Sie eine SQL-Abfrage zum Entfernen aller Ereignisse aus, die zwischen dem Datenbankfehler und dem Neustart (dem Zeitpunkt, den Sie in Schritt 8 notiert haben) aufgetreten sind. Beispiel: `delete from [DB_NAME].ADS_EVENT where Start_Time > '<[Zeitpunkt des DB-Fehlers]>' and Start_Time < '<[Zeitpunkt der DB-Wiederherstellung]>'`

Weitere Informationen

Indizierung von Inhalten im CMS-Repository [Seite 741]

13.5.1.2 Wiederherstellen ausschließlich der Audit-Datenbank

Bevor Sie die Audit-Datenbank wiederherstellen, stoppen Sie mit dem Central Configuration Manager (CCM) alle Knoten in der BI-Plattform-Implementierung. Entscheiden Sie außerdem, bis zu welchem Zeitpunkt Sie die Datenbank wiederherstellen möchten.

> **Hinweis**
>
> Führen Sie diese Aufgabe nur aus, wenn Sie sicher sind, dass die Audit-Datenbank die einzige beeinträchtigte Komponente der BI-Plattform ist. Wenn weitere Komponenten betroffen sind, führen Sie eine vollständige Systemwiederherstellung durch.

1. Suchen Sie die letzten Sicherungen und Transaktionsprotokolle für die Audit-Datenbank.
2. Verwenden Sie die Datenbanktools zum Wiederherstellen der Audit-Datenbank.
3. Führen Sie ein Rollforward für die Audit-Datenbank durch, und wiederholen Sie das Transaktionsprotokoll.

Weitere Informationen

Wiederherstellen des gesamten Systems [Seite 498]

13.5.1.3 Wiederherstellen von Webschicht-Inhalt

Vor der Wiederherstellung des Webschichtinhalts müssen Sie alle Knoten in Ihrer BI-Plattform-Implementierung mit dem Central Configuration Manager (CCM) stoppen. Außerdem müssen Sie entscheiden, bis zu welchem Zeitpunkt Sie den Webschichtinhalt wiederherstellen möchten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wenn Sie die Option haben möchten, zum aktuellen Status des Systems zurückzukehren, müssen Sie vor der Wiederherstellung eine Sicherung des Systems durchführen.

Falls die Webschicht beschädigt ist, kann sie individuell wiederhergestellt werden.

1. Verwenden Sie Datei-Wiederherstellungstools, um die Webschichtordner auf dem Hostrechner der Webschicht wiederherzustellen.
2. Starten Sie alle Knoten für Ihre BI-Plattform-Implementierung über den CCM neu.

13.5.1.4 Wiederherstellen ausschließlich der CMS-Datenbank

> **Hinweis**
>
> Führen Sie dieses Verfahren nur durch, wenn ausschließlich die CMS-Datenbank abgestürzt ist. Wenn die Datenbank oder andere Komponenten fehlerhaft sind, müssen Sie eine vollständige Wiederherstellung des Systems durchführen.

Reparieren oder tauschen Sie den Hostrechner der CMS-Datenbank aus. Stellen Sie bei einem Austausch sicher, dass er denselben Namen wie der vorherige Rechner sowie dieselben Porteinstellungen und Datenbank-Anmeldedaten hat.

> **Hinweis**
>
> Falls der Rechner nicht mit demselben Namen und denselben Anmeldedaten wiederhergestellt werden kann, müssen sie den CCM zur Aktualisierung dieser Datenbank-Verbindungsinformationen für jeden Knoten im Cluster verwenden und diese Knoten neu starten.

1. Stoppen Sie alle BI-Plattform-Knoten mit dem CCM.
2. Suchen Sie den neuesten CMS-Datenbank-Sicherungssatz.
3. Stellen Sie die CMS-Datenbank mit Ihren Datenbanktools wieder her.
4. Suchen Sie das neueste Transaktionsprotokoll für die CMS-Datenbank, also das Protokoll mit den Transaktionen, die nach der letzten Sicherung durchgeführt wurden.
5. Wiederholen Sie das gesamte Transaktionprotokoll für die CMS-Datenbank.
6. Starten Sie die BI-Plattform-Knoten über den CCM.

Nachdem Sie verifiziert haben, dass das System ordnungsgemäß funktioniert, führen Sie folgende Schritte aus:

- Führen Sie das Repository Diagnotic Tool aus, um nicht verwendete temporäre Dateien zu entfernen und überprüfen Sie die Konsistenz des Repositorys. Siehe Abschnitt "Repository Diagnostic Tool" dieses Handbuchs.
- Veröffentlichungsaufträge, die während der Sicherung des Systems ausgeführt wurden, werden als fehlgeschlagen angezeigt. Führen Sie diese Instanzen nicht erneut aus, sondern starten Sie einen neuen Veröffentlichungsauftrag.

Weitere Informationen

Indizierung von Inhalten im CMS-Repository [Seite 741]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

13.5.1.5 Suchindex-Wiederherstellung

Mit der Plattform-Suchfunktion wird eine Reihe von Index- und Informationsdateien im System verwaltet, um die Suche effizienter zu gestalten. Falls das System wiederhergestellt werden muss, können in diesen Informationsdateien Inkonsistenzen entstehen. Sie können diese Inkonsistenzen reparieren, entweder, indem Sie das Index-Wiederherstellungsskript verwenden, oder indem Sie den Index neu erstellen.

Die Neuerstellung des Index ist ein einfacher Prozess, belegt jedoch erhebliche Ressourcen und dauert einige Zeit, bis er abgeschlossen ist. Suchen, die während der Neuerstellung durchgeführt werden, geben nur Ergebnisse für die indizierten Teile der Datenbank zurück. Das Wiederherstellungsskript umfasst einen komplizierteren Prozess, stellt jedoch einen vollständigen, funktionierenden Index zur Verfügung.

Führen Sie beim Wiederherstellen einer Implementierung mit mehreren Rechnern das Skript auf allen Rechnern aus, die den Suchdienst hosten. Verwenden Sie für den ersten Rechner in einem Cluster die Option *-Both* und anschließend auf allen folgenden Rechnern in diesem Cluster die Option *-ContentStore*.

Weitere Informationen

Indizierung von Inhalten im CMS-Repository [Seite 741]

13.5.1.5.1 Ausführen des Suchindex-Wiederherstellungsskripts

- Bestätigen Sie, dass der CMS ausgeführt wird, und stoppen Sie alle Adaptive Processing Server (APS) mit dem installierten Suchdienst.

  > **Hinweis**
  >
  > Diese APS müssen so schnell wie möglich nach dem Start des Knotens gestoppt werden.

- Setzen Sie `JAVA_HOME` auf den Speicherort `sapjvm/bin` im BI-Plattform-Installationsverzeichnis.
- Auf das Datenverzeichnis der Plattformsuche kann über den Rechner zugegriffen werden, auf dem Sie das Skript ausführen.

1. Öffnen Sie ein Befehlszeilenfenster auf dem CMS- oder APS-Hostrechner (bei Verwendung eines Windows-Betriebssystems).
2. Navigieren Sie zum Verzeichnis **`<INSTALLVERZ>`**`\SAP BusinessObjects Enterprise XI 4.0\java\lib\`.

   Unix-Rechner verwenden den entsprechenden Unix-Dateipfad.
3. Geben Sie *java -jar platformSearchOnlineHotbackupRestore.jar* ein und drücken die **Eingabetaste**.
4. Geben Sie an der Eingabeaufforderung folgende Informationen ein und drücken die **Eingabetaste**:
   - Speicherort der BI-Plattform-Installation (z.B. **`<INSTALLVERZ>`**`/SAP BusinessObjects Enterprise XI 4.0`)
   - Ihre CMS-Anmeldedaten, einschließlich des CMS-Namens, der Benutzer-ID und des Kennworts sowie des Authentifizierungstyps. Für den Authentifizierungstyp gibt es folgende Optionen:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- secEnterprise
- secLDAP
- secWinAD
- secSAPR3

5. Wenn Sie zur Eingabe des Index-Wiederherstellungstyps aufgefordert werden, geben Sie eine der folgenden Optionen ein und drücken die **Eingabetaste**.

Wert	Beschreibung
-Both	Dieser Wert sollte für Einzelserverimplementierungen oder bei Implementierungen mit mehreren Rechnern für den ersten APS-Hostrechner mit dem Suchdienst verwendet werden: Verwenden Sie in einem System mit mehreren Such-APS bei der ersten Ausführung des Skripts den Wert *-Both* (aktualisiert Datenbank und Inhaltsspeicher). Wenn das Skript für alle anderen APS ausgeführt wird, verwenden Sie den Wert *-ContentStore* (aktualisiert nur den Inhaltsspeicher).
-ContentStore	Dieser Wert sollte beim Ausführen des Skripts auf APS-Hostrechnern mit installiertem Suchdienst verwendet werden, wenn es sich nicht um den ersten Computer im Cluster handelt, in dem das Skript ausgeführt wird.
-Exit	Beendet das Skript, ohne den Index wiederherzustellen.

6. Schließen Sie das Befehlszeilenfenster, nachdem das Skript ausgeführt wurde (für Windows-Rechner).

Starten Sie alle gestoppen APS.

13.5.2 Wiederherstellen der Servereinstellungen

Wenn Sie die Servereinstellungen des Systems aus einer BIAR-Datei wiederherstellen müssen, können Sie entweder den Central Configuration Manager (CCM) oder das RestoreCluster-Skript zum Wiederherstellen der Servereinstellungen verwenden. Das Wiederherstellen des Serverinhalts aus einer BIAR-Datei hat keine Auswirkungen auf Business-Intelligence-Inhalt wie Berichte, Benutzer und Gruppen oder Sicherheitseinstellungen.

> **Hinweis**
>
> Beim Wiederherstellen der Servereinstellungen wird nur die Wiederherstellung der Einstellungen eines gesamten Clusters unterstützt. Es ist nicht möglich, nur die Einstellungen einiger Server im Cluster wiederherzustellen.

> **Hinweis**
>
> Falls Sie Servereinstellungen in einer Implementierung mit aktiviertem SSL sichern oder wiederherstellen, müssen Sie SSL zunächst über CCM deaktivieren und dann nach abgeschlossener Sicherung bzw. Wiederherstellung erneut aktivieren.

Weitere Informationen

Konfigurieren von Servern für SSL [Seite 174]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

13.5.2.1 Wiederherstellen der Servereinstellungen mit dem CCM unter Windows

Sie können Servereinstellungen mithilfe des Central Configuration Manager (CCM) wiederherstellen. Nachdem Sie Servereinstellungen wiederhergestellt haben, müssen Sie die Knoten des Systems auf allen Rechnern im Cluster des Systems neu erstellen.

1. Stoppen Sie alle Knoten auf allen Rechnern im Cluster, für den Sie Serverkonfigurationseinstellungen wiederherstellen, indem Sie den Server Intelligence Agent für jeden Knoten stoppen.
2. Starten Sie den CCM auf einem Rechner, der einen CMS hostet.
3. Klicken Sie in der Symbolleiste auf **Serverkonfiguration wiederherstellen**.
   Der *Assistent zum Wiederherstellen der Serverkonfiguration* wird angezeigt.
4. Klicken Sie auf **Weiter**, um den Assistenten zu starten.
5. Geben Sie bei entsprechender Eingabeaufforderung die Portnummer des zu verwendenden temporären Central Management Servers (CMS) und die Informationen für die Verbindung zu der CMS-Systemdatenbank an, und klicken Sie auf **Weiter**, um fortzufahren.
6. Geben Sie den Clusterschlüssel ein, und klicken Sie auf **Weiter**, um fortzufahren.
7. Melden Sie sich bei entsprechender Aufforderung am CMS an, indem Sie den CMS-Namen und den Benutzernamen sowie das Kennwort eines Kontos mit Administratorberechtigungen angeben. Klicken Sie dann zum Fortfahren auf **Weiter**.
8. Geben Sie den Speicherort und den Namen der BIAR-Datei an, die die wiederherzustellenden Serverkonfigurationseinstellungen enthält, und klicken Sie zum Fortfahren auf **Weiter**.
   Der Inhalt der BIAR-Datei wird auf einer Übersichtsseite angezeigt.
9. Klicken Sie auf **Weiter**, um fortzufahren.
   Die von Ihnen eingegebenen Informationen werden auf einer Übersichtsseite angezeigt.
10. Klicken Sie auf **Fertig stellen**, um fortzufahren.
    Sie werden in einer Warnmeldung darüber informiert, dass die vorhandenen Servereinstellungen mit den in der BIAR-Datei enthaltenen Werten überschrieben werden und die aktuellen Servereinstellungen verloren gehen, wenn Sie fortfahren.
11. Klicken Sie auf **Ja**, um die Serverkonfigurationseinstellungen wiederherzustellen.

    Der CCM stellt die Serverkonfigurationseinstellungen für den gesamten Cluster aus der BIAR-Datei wieder her. Details der Wiederherstellung werden in eine Protokolldatei geschrieben. Der Name und der Pfad der Protokolldatei werden in einem Dialogfeld angezeigt.
12. Wenn der Wiederherstellungsvorgang fehlschlägt, prüfen Sie die Protokolldatei, um den Grund zu ermitteln.
13. Klicken Sie auf **OK**, um den Assistenten zu schließen.

Die Servereinstellungen aus der BIAR-Datei werden auf dem System wiederhergestellt. Alle in der BIAR-Datei vorhandenen Knoten und Server, die vor der Wiederherstellung nicht auf dem System vorhanden waren, werden erstellt.

> **Hinweis**
>
> Knoten und Server, die im System vorhanden waren, jedoch nicht in der BIAR-Datei, werden aus dem Repository entfernt. Die Knoten und Server werden zwar noch im CCM angezeigt, allerdings können Sie die Dateien `dbinfo` und `bootstrap` für Knoten manuell löschen.

Sie müssen die Knoten im System auf jedem Rechner des Clusters neu erstellen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Verwenden von Knoten [Seite 404]

13.5.2.2 Wiederherstellen von Servereinstellungen mit dem CCM unter UNIX

Verwenden Sie auf UNIX-Rechnern das Skript `serverconfig.sh` zum Wiederherstellen der Servereinstellungen der Implementierung aus einer BIAR-Datei.

1. Wählen Sie **6 – Serverkonfiguration wiederherstellen** aus, und drücken Sie die *Eingabetaste*.
2. Geben Sie einen Port für den zu verwendenden temporären Central Management Server (CMS) ein, und drücken Sie die *Eingabetaste*.
3. Geben Sie auf den folgenden Bildschirmen die Verbindungsdaten für die CMS-Systemdatenbank ein.
4. Melden Sie sich bei entsprechender Aufforderung beim CMS an, indem Sie den System- und Benutzernamen sowie das Kennwort eines Kontos mit Administratorberechtigungen angeben und die *Eingabetaste* drücken.
5. Geben Sie bei entsprechender Aufforderung den Speicherort und den Namen der BIAR-Datei an, aus der die Konfigurationseinstellungen des Servers wiederhergestellt werden sollen, und drücken Sie die *Eingabetaste*. Es wird ein Übersichtsbildschirm mit den eingegebenen Informationen angezeigt.
6. Stellen Sie sicher, dass die auf dem Bildschirm angezeigten Informationen richtig sind, und drücken Sie die **Eingabetaste**, um fortzufahren.
   Das `serverconfig.sh`-Skript stellt die Konfigurationseinstellungen des Servers für das gesamte Cluster anhand der angegebenen BIAR-Datei wieder her. Die Details des Wiederherstellungsverfahrens werden in eine Protokolldatei geschrieben. Name und Pfad der Protokolldatei werden am Bildschirm angezeigt.
7. Falls die Wiederherstellung fehlschlägt, überprüfen Sie die Protokolldatei, um den Grund zu ermitteln.

13.5.2.3 Wiederherstellen der Servereinstellungen anhand eines Skripts

Sie können die Servereinstellungen der Implementierung auch wiederherstellen, indem Sie unter Windows das Skript `RestoreCluster.bat` und unter UNIX das Skript `restorecluster.sh` ausführen.

Unter Windows befindet sich die Datei `RestoreCluster.bat` im Verzeichnis **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

Unter Unix befindet sich die Datei `restorecluster.sh` im Verzeichnis `/`**<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/`**<PLATFORM64>**`/scripts`.

Weitere Informationen

BackupCluster- und RestoreCluster-Skript [Seite 506]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

13.5.3 Wiederherstellen von BI-Inhalt

Wenn Sie Business-Intelligence-Inhalt (BI-Inhalt) in LCMBIAR-Dateien gesichert haben, können Sie diesen mit der Hochstufverwaltung wiederherstellen, ohne das gesamte System wiederherstellen zu müssen. Weitere Informationen finden Sie im Kapitel “Hochstufverwaltung”.

13.6 BackupCluster- und RestoreCluster-Skript

In der folgenden Tabelle werden die mit dem `BackupCluster`-Skript verwendeten Befehlszeilenparameter beschrieben.

> **Hinweis**
>
> Mit diesem Skript werden nur die Servereinstellungen für einen Cluster gesichert. Andere Daten müssen gesondert gesichert werden.

Tabelle 17: BackupCluster-Parameter

Name	Beschreibung	Beispiel:
-backup	Name und Pfad der BIAR-Datei, in der die wiederherzustellenden Servereinstellungen Ihres Systems gesichert werden sollen.	`-backup "C:\Users\Administrator\Desktop\my.biar"`
-cms	Der Hostname des Rechners, auf dem Ihr Central Management Server sich befindet. Falls Ihr CMS auf einem anderen Port als dem Standardport 6400 ausgeführt wird, müssen Sie auch die Portnummer angeben.	`-cms mycms:6400`
-username	Der Benutzername des Administratorkontos.	`-username Administrator`
-password	Das Kennwort des Administratorkontos.	`-password Password1`

In der folgenden Tabelle werden die mit dem `RestoreCluster`-Skript verwendeten Befehlszeilenparameter beschrieben.

Tabelle 18: RestoreCluster-Parameter

Name	Beschreibung	Beispiel:
-restore	Name und Pfad der BIAR-Datei, die die wiederherzustellenden Serverkonfigurationseinstellungen enthält.	`-restore "C:\Users\Administrator\Desktop\my.biar"`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Name	Beschreibung	Beispiel:
-username	Der Benutzername des Administratorkontos.	**`-username Administrator`**
-password	Das Kennwort des Administratorkontos.	**`-password Password1`**
-displaycontents	Zeigt die Liste der Knoten und Server an, die in der BIAR-Datei enthalten sind.	**`-displaycontents "C:\Users\Administrator\Desktop\my.biar"`**

> **Hinweis**
>
> Führen Sie das Skript `RestoreCluster` mit dem Parameter *-displaycontents* aus, um den Inhalt der BIAR-Datei vor der Wiederherstellung der Servereinstellungen anzuzeigen.

Folgende Parameter werden benötigt, wenn Sie Servereinstellungen von einem nicht ausgeführten System sichern oder Servereinstellungen wiederherstellen.

Tabelle 19: Bei Verwendung eines temporären CMS verwendete Parameter

Name	Beschreibung	Beispiel:
-usetempcms	Erstellt einen temporären CMS für den angegebenen Vorgang. Nach Fertigstellung des Vorgangs wird der temporäre CMS gestoppt.	**`-usetempcms`**
-cmsport	Die Portnummer des temporären CMS.	**`-cmsport 6700`**
-dbdriver	Der Datenbanktreiber der CMS-Systemdatenbank. Zulässige Werte: • **`db2databasesubsystem`** • **`maxdbdatabasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlserverdatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`newdbdatabasesubsystem`** **Hinweis** Der Parameter **`newdbdatabasesubsystem`** dient der Verwendung mit SAP-HANA-Datenbanken.	**`-dbdriver sqlserverdatabasesubsystem`**

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Name	Beschreibung	Beispiel:
-connect	Die CMS-Systemdatenbankverbindungs-Zeichenfolge.	**-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"**
-dbkey	Der Clusterschlüssel.	**-dbkey abc1234**

Beispiel

Das folgende Beispiel zeigt, wie Sie Ihre Servereinstellungen in einer BIAR-Datei mit einem vorhandenen CMS sichern.

```
-backup "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
```

Beispiel

Das folgende Beispiel zeigt, wie Sie den Inhalt der BIAR-Datei anzeigen.

```
-displaycontents "C:\Users\Administrator\Desktop\mybiar.biar"
```

Beispiel

Das folgende Beispiel zeigt, wie Sie Ihre Einstellungen anhand einer BIAR-Datei wiederherstellen. Zum Wiederherstellen der Servereinstellungen muss immer ein temporärer CMS verwendet werden.

```
-restore "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
-usetempcms
-cmsport 6400
-dbdriver sqlserverdatabasesubsystem
-connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
-dbkey abc1234
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

14 Kopieren Ihrer BI-Plattform-Implementierung

14.1 Übersicht des Kopierens des Systems

In diesem Kapitel wird beschrieben, wie Sie ein Duplikat der BI-Plattform-Implementierung zu Test-, Standby- und anderen Zwecken erstellen.

Weitere Informationen

Übersicht über Sicherung und Wiederherstellung [Seite 487]

14.2 Terminologie

Begriff	Definition
Quellsystem	Die ursprüngliche BI-Plattformimplementierung.
Zielsystem	Die neue Implementierung, die Sie erstellen möchten.
Systemkopie	Erstellung eines Duplikats von einer vorhandenen BI-Plattform-Implementierung.
Homogene Systemkopie	Erstellung eines Systemduplikats, in dem Quell- und Zielsystem denselben Betriebssystem- und Datenbanktyp aufweisen. Die BI-Plattform unterstützt nur die homogene Systemkopie.
Heterogene Systemkopie	Erstellung eines Systemduplikats, in dem Quell- und Zielsystem verschiedene Betriebssystem- oder Datenbanktypen verwenden, aber auf denselben Daten basieren.
Datenbankkopie	Erstellung eines Duplikats der CMS-Systemdatenbank oder -Audit-Datenbank unter Verwendung von Datenbankanbietertools.

14.3 Anwendungsfälle für Systemkopien

In der folgenden Tabelle sind verschiedene Ziele, die Sie sich unter Berücksichtigung der vorhandenen Ressourcen unter Umständen gesetzt haben sowie die am besten für Sie geeignete Lösung aufgeführt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ziel	Erforderliche Ressourcen	Lösung
Ziel: identische Kopie Ich möchte ein Duplikatsystem für Standby- und Testzwecke mit identischer Hardwarekonfiguration und identischen IP-Adressen/ Rechnernamen erstellen.	• Ein Zielsystem mit identischer Hardware wie im Quellsystem UND • Sicherungskopien des Quellsystems oder Zugriff auf das Quellsystem zur Sicherungserstellung	Gehen Sie anhand des Workflows zum Sichern und Wiederherstellen des Systems in diesem Handbuch vor. Siehe das Verfahren unter *Sichern des gesamten Systems* [Seite 491]. Erstellen Sie das Zielsystem aus Sicherungskopien des Quellsystems neu.
Ziel: Kopie Ich möchte ein Duplikatsystem für Standby-, Test- oder Schulungszwecke mit anderer Hardware und anderen IP-Adressen/Rechnernamen aus dem Quellsystem erstellen.	• Quellsystem (in Ausführung oder gestoppt) ODER Sicherungskopien der Quellsystemdatenbank und -dateien UND • Detaillierte Systeminformationen, die in *Exportieren aus einem Quellsystem* [Seite 513] beschrieben sind	Halten Sie sich an den Workflow zum Kopieren von Systemen. Beginnen Sie mit *Planen des Kopierens Ihres Systems* [Seite 510], und folgen Sie den Anweisungen im restlichen Kapitel. **Hinweis** Sie können das Zielsystem auf einem Rechner mit einer vorhandenen BI-Plattform-Implementierung erstellen, die dieselbe Version, dasselbe Support Package und dieselbe Patch-Ebene aufweist, oder auf einem "neuen" Computer ohne installierte BI-Plattform.

Weitere Informationen

Sicherungen [Seite 490]
Planen des Kopierens Ihres Systems [Seite 510]

14.4 Planen des Kopierens Ihres Systems

Eine Systemkopie muss Ihr aktuelles System nicht widerspiegeln. Sie können eine Kopie Ihres Systems erstellen und einige Zeit warten, bevor Sie mit der Neuerstellung der Kopie im Zielsystem fortfahren. Alternativ können Sie eine frühere Sicherung des Quellsystems als Basis für Ihr Zielsystem verwenden. Dies bedeutet, dass die Kopie des Systems dessen Stand zum Zeitpunkt ihrer Erstellung widerspiegelt. Wenn Sie beispielsweise einen Monat warten, erstellt die Kopie das System auf dem Stand neu, den es vor einem Monat hatte.

Nachdem Sie die Verwendungsbeispiele aus dem vorherigen Abschnitt geprüft und sich für dasjenige entschieden haben, das Ihre Anforderungen am besten erfüllt, erstellen Sie einen Systemkopieplan.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Erstellen Sie einen Systemkopieplan

Bei der Planung des Kopierens eines Systems müssen Sie Folgendes im Voraus planen:

- Wird das Quellsystem gestoppt oder ist es während der Kopieerstellung aktiv? (Der Kopiervorgang kann in beiden Fällen durchgeführt werden.)
  - Wenn das Quellsystem gestoppt wird, wie viel Ausfallzeit ist erforderlich?
  - Planen Sie etwas Zeit für Tests ein, um die Integrität des Zielsystems zu gewährleisten.
- Welche Datenbanktools sollen zur Sicherung und Wiederherstellung der Datenbank verwendet werden?
- Auf welchen Rechnern des Zielsystems wird implementiert, und wo werden die einzelnen Knoten gehostet?
- Welche optionalen Komponenten sollen kopiert werden?
- Der für die CMS-Zieldatenbank zu verwendende Datenbanktyp und alle anderen optionalen Datenbanken, die kopiert werden sollen.

Berücksichtigen Sie auch Folgendes:

- Welche BI-Plattformkomponenten sind auf dem Quellsystem installiert? Sie können über die Funktion **Software** > **Ändern** des Installationsprogramms die Liste der aktuell installierten Komponenten anzeigen.
- Wenn das Zielsystem in einem anderen Hardware-Setup als das Quellsystem installiert wird, muss das Zielsystem u.U. abgestimmt werden, um die Leistung zu optimieren. Lesen Sie die Informationen zur Verbesserung der Systemleistung im *SAP BusinessObjects Business Intelligence Sizing Companion Guide*.
- Im Zielsystem sollte die Berichterstellung aus anderen Berichtsdatenbanken als den Quellsystemdatenbanken erfolgen. In diesem Fall müssen Sie die Datenbankverbindungsinformationen für die Berichtsdatenbanken ändern. Sie können dabei denselben DSN-Namen verwenden, aber den DSN auf dem Zielsystem auf eine andere Datenbank zeigen lassen.

Erforderliche Quellsystemkomponenten

- CMS-Systemdatenbank
- FRS-Dateispeicher
- Konfigurationsdateien der semantischen Schicht
- Audit-Datenbank (optional)
- Überwachungsdatenbank (optional)
- Datenbank der Hochstufverwaltung (optional)

14.5 Überlegungen und Einschränkungen

Wenn Sie eine Kopie der BI-Plattform-Implementierung anfertigen, sollten Sie folgende Punkte berücksichtigen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Bereich	Überlegung
SAP-Business-Warehouse-Integrationen	Wenn Sie die BI-Plattform und SAP ERP oder BW in einer integrierten Umgebung verwenden, sollten Sie die Dokumentation zum Kopieren des SAP-Systems lesen, bevor Sie das System kopieren. Die Systemkopiehandbücher sind unter *http://www.sdn.sap.com/irj/sdn/systemcopy* verfügbar (SMP-Anmeldung erforderlich). Wählen Sie Ihre SAP-NetWeaver-Version aus. Die relevanten Anleitungen zum Kopieren befinden sich im Ordner mit den Installationshandbüchern.
Programmversion	Quell- und Zielsystem müssen denselben Versionsstand und dasselbe Support-Package- und Patch-Level aufweisen.
Inhalt und Konfigurationseinstellungen	Das System kann nur komplett kopiert werden. Sie können keine ausgewählten Inhalte oder Konfigurationseinstellungen des Systems kopieren.
Installationspfad	Der Installationspfad für den Speicherort von Quelle und Ziel muss identisch sein: Wenn Sie z. B. das Quellsystem auf `C:\SAP BusinessObjects Enterprise XI 4.0` installiert haben, müssen Sie das Ziel ebenfalls auf `C:\SAP BusinessObjects Enterprise XI 4.0` installieren.
Hostbetriebssystem	Die Betriebssysteme von Quelle und Ziel müssen identisch sein.
CMS-Datenbanksoftwaretyp	CMS-Quell- und Zieldatenbanken müssen vom selben Typ sein. Sie haben die Option, nach dem Kopieren des Systems zu einem anderen unterstützten Datenbanktyp zu wechseln.
Audit-Datenbanksoftwaretyp	Wenn Sie Audit-Daten kopieren, müssen die Quell- und die Ziel-Audit-Datenbank vom selben Typ sein. Nachdem die Kopie erstellt wurde, können Sie eine neue Datenbank eines anderen Typs einrichten. **Hinweis** Wenn Sie eine neue Datenbank einrichten, werden vorhandene Ereignisse nicht in diese kopiert. Nur neue Ereignisse werden in der neuen Datenbank aufgezeichnet.
Webschichtanpassung	Webschichtkomponenten werden nicht von dem Kopierverfahren aus dem Quellsystem kopiert. Wenn Sie die Webschicht angepasst haben (z.B. `.properties`-Dateien im Ordner `custom` geändert haben), wenden Sie diese Anpassungen manuell auf das Ziel an.
Nicht von diesen Anleitungen abgedeckte Themen	Dieser Workflow beschreibt nicht den Export oder Import einer Datenbank. Verwenden Sie die Datenbankanbietertools zum Kopieren und Wiederherstellen der Datenbank.

Folgende Daten werden beim Kopieren des Systems kopiert:

- die CMS-Repository-Datenbank. (Enthält Berichte, Analysen, Rechte, Benutzer und Benutzergruppen, Servereinstellungen und anderen BI-Inhalt und Systeminhalt)

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- die Audit-Datenbank. (Enthält von BI-Plattform-Servern oder Clientanwendungen ausgelöste Audit-Ereignisse)
- die Überwachungsdatenbank. (Enthält Trenddaten aus Metriken, Diagnosen und Kontrollmodulen)
- Die Datenbank der Hochstufverwaltung. (Enthält verschiedene Versionen von Berichten, Analysen, andere BI-Ressourcen und Versionsinformationen)

> **Hinweis**
>
> Eine Beschreibung der Datenbanken und ihres Inhalts finden Sie in Abschnitt *Datenbanken* [Seite 35] in diesem Handbuch.

- Konfigurationsdateien der semantischen Schicht

Webschichtkonfiguration, Suchindex und alle nicht oben ausdrücklich angegebenen Daten werden nicht kopiert.

Überlegungen zu Dateiwiederherstellungskopien

Wenn Sie ein System für den speziellen Zweck der Wiederherstellung einer versehentlich gelöschten Datei kopieren, sollten Sie folgende zusätzliche Überlegungen berücksichtigen:

Führen Sie unter Verwendung der Sicherungskopie die Schritte aus dem Verfahren *Importieren in ein Zielsystem* [Seite 517]auf dem Produktionssystem aus.

- Installieren Sie nicht alle Knoten, sondern nur den ersten Knoten für den CMS und seine Datenbank.
- Installieren Sie die Audit-, die Hochstufverwaltungs- oder die Überwachungsdatenbank nicht.
- Erstellen Sie die Verbindungen zu der Audit- oder der Berichterstellungsdatenbank nicht neu.

Stufen Sie mithilfe des LCM das Objekt, das Sie wiederherstellen möchten, aus dem Zielsystem zum Quellsystem hoch.

14.6 Verfahren zum Kopieren vom System

Die folgenden Verfahren führen Sie durch die zwei Phasen beim Kopieren der BI-Plattform-Implementierung.

14.6.1 Exportieren aus einem Quellsystem

Notieren Sie folgende Informationen aus dem Quellsystem: Wenn Sie diese Informationen hier festhalten möchten, können Sie ein Arbeitsblatt verwenden, das unter *Systemkopie-Arbeitsblatt* [Seite 1034] verfügbar ist.

Eigenschaft	Speicherort
CMS-Clusterschüssel (bewahren Sie die Aufzeichnung an einem sicheren Ort auf).	Vom Systemadministrator bei der Installation der BI-Plattform erstellt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Speicherort
Namen der Knoten.	Wechseln Sie zur Registerkarte **Server** der CMC, und klappen Sie in der Struktur links **Knoten** auf.
Rechnername und BI-Plattform-Installationsordner jedes Rechners in der Implementierung.	Wechseln Sie zur Registerkarte **Server** der CMC, klicken Sie mit der rechten Maustaste auf den CMS, und wählen Sie **Platzhalter** aus. Suchen Sie den Wert des Platzhalters *%INSTALLROOTDIR%*.
BI-Plattform-Administratorkennwort (bewahren Sie die Aufzeichnung an einem sicheren Ort auf).	Vom Systemadministrator bei der Installation der BI-Plattform erstellt.
Alle Datenbankverbindungen, die vom CMS verwendet werden können, und die ihnen zugeordneten Benutzernamen und Kennwörter. Dazu kann auch die Audit-Datenbank gehören, wenn Sie diese Informationen kopieren möchten. Beschaffen Sie diese Informationen für alle Rechner im Cluster. **Hinweis** Wenn Sie die Audit-Datenbank kopieren, benötigen Sie außerdem die Verbindungsnamen und die Anmeldedaten der Audit-Datenbank.	Wechseln Sie zur Registerkarte **Server** der CMC, klicken Sie mit der rechten Maustaste auf den CMS, und wählen Sie **Metriken** aus. Suchen Sie folgende Metriken: • *Systemdatenbank-Verbindungsname* • *Systemdatenbank-Servername* • *Systemdatenbank-Benutzername* • *Datenquellenname* • *Name der Audit-Datenbankverbindung* (optional) • *Name des Audit-Datenbankbenutzers* (optional)
Für jeden Rechner im Cluster die Details (Clienttypen, Versionen) aller anderen Datenbankverbindungen (die z.B. von Universen und Berichten verwendet werden). Stellen Sie sicher, dass Sie Benutzernamen und Kennwörter einbeziehen.	Für Crystal-Reports-Berichte, die Berichte direkt aus Datenbanken erstellen, betrachten Sie mithilfe der Designerversionen von SAP Crystal Reports 2013 oder SAP Crystal Reports für Enterprise die Verbindungsinformationen. Für Universumsverbindungsinformationen verwenden Sie das Information-Design-Tool (.unx) oder das Universe-Design-Tool (.unv).
Versionsstand, Support-Package- und Patch-Level des Quellsystems.	Unter Windows können Sie diese Angaben mithilfe der Programmfunktion *Ändern/Entfernen* ausfindig machen. Unter Unix können Sie das Dienstprogramm `modifyOrRemoveProducts.sh` im BI-Plattform-Installationsverzeichnis verwenden.
Dateispeicherorte der einzelnen Input FRS und Output FRS in der Implementierung.	Wechseln Sie zur Registerkarte **Server** der CMC, klicken Sie mit der rechten Maustaste auf den Input oder Output FRS, und wählen Sie **Eigenschaften** aus. Suchen Sie die Eigenschaft *Dateispeicherverzeichnis*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Speicherort
	Hinweis Wenn der Wert mit % beginnt, handelt es sich um einen Platzhalter. Klicken Sie dann auf **Platzhalter**, und notieren Sie das unter dem Platzhalter aufgelistete Verzeichnis.
Der Speicherort des Hochstufverwaltungs-Datenbankordners und des Subversion-Ordners, falls Promotion Management kopiert werden soll.	Der Standardordner für die Datenbank der Hochstufverwaltung ist bei Windows-Installationen `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOverride` und unter Unix `<INSTALLVERZ>/sap_bobj/data/LCM/LCMOverride`. Die Standardspeicherorte für die Subversion-Dateien bei Windows-Installation sind: • `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\CheckOut` • `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository` und unter Unix: • `<INSTALLVERZ>/check_out`(Dieses Verzeichnis wird erst erstellt, nachdem Sie Subversion zum Auschecken von Dateien verwendet haben.) • `$HOME/LCM_Repository`
Der Ordner der Überwachungsdatenbank, falls die Überwachungsdatenbank kopiert werden soll	Dies ist in der CMC festgelegt. Wechseln Sie in den Verwaltungsbereich **Anwendungen** der CMC, wählen Sie **Überwachungstool** > **Eigenschaften**, und suchen Sie *Sicherungsverzeichnis der Trenddatenbank*. Der Standardordner in der Windows-Installation ist `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB` und unter Unix `<INSTALLVERZ>/sap_bobj/Data/TrendingDB`.
Der Pfad zum Ordner der semantischen Ebene	Der Standardordnerpfad in Windows-Installationen ist `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionsServer\`.

Nachdem Sie die vorstehenden Informationen aufgezeichnet haben:

1. Erstellen Sie unter Verwendung der Sicherungstools des Datenbankanbieters eine Sicherungskopie der folgenden Datenbanken:
   - CMS-Systemdatenbank
   - Audit-Datenbank (optional)

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Sichern Sie unter Verwendung von Dateisicherungstools die folgenden Dateisätze:
   - FRS-Input- und -Output-Dateispeicher
   - Überwachungstrenddatenbank (optional). Dies wird erreicht, indem Dateien aus dem Überwachungsordner gesichert werden, wie auf dem Arbeitsblatt aufgezeichnet. Standardmäßig unter Windows ist dies: **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB`. Unter Unix: **<INSTALLVERZ>**`/sap_bobj/Data/TrendingDB`.
   - Datenbank der Hochstufverwaltung (optional). Dies wird erreicht, indem Dateien aus dem Datenbankordner gesichert werden, wie auf dem Arbeitsblatt aufgezeichnet. Standardmäßig unter Windows ist dies: **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOverride`. Unter Unix: **<INSTALLVERZ>**`/sap_bobj/data/LCM/LCMOverride`.
   - Subversion-Datenbank der Hochstufverwaltung (optional). Dies wird erreicht, indem Dateien aus dem Subversionsordner gesichert werden, wie auf dem Arbeitsblatt aufgezeichnet. Standardmäßig unter Windows:
     - **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\CheckOut`
     - **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository`

     und unter Unix:
     - **<INSTALLVERZ>**`/check_out`(Dieses Verzeichnis wird erst erstellt, nachdem Sie Subversion zum Auschecken von Dateien verwendet haben.)
     - `$HOME/LCM_Repository`
   - Konfigurationsdateien aus dem Ordner für die semantische Schicht: Datei `cs.cfg` im Ordner `connectionServer` und alle `.sbo`- und `.prm`-Dateien in dessen Unterordnern.

   > **Hinweis**
   >
   > Einschränkungen und eine ausführliche Beschreibung dieses Workflows finden Sie im Abschnitt *Hotbackups* [Seite 491].

3. Folgende Dateien können vom Benutzer angepasst werden. Wenn Sie eine dieser Dateien angepasst haben, sichern Sie die Dateien aus dem Quellsystem, und stellen Sie sie später wieder in demselben Order auf dem Zielsystem her:
   - `BO_trace.ini` installiert unter:
     - `[INSTALLVERZ]SAP BusinessObjects Enterprise XI 4.0/conf`
   - `clientSDKOptions.xml` installiert unter:
     - `[INSTALLVERZ]SAP BusinessObjects Enterprise XI 4.0/java/lib`
     - `[INSTALLVERZ]SAP BusinessObjects Enterprise XI 4.0/win32_x86`
     - `[INSTALLVERZ]SAP BusinessObjects Enterprise XI 4.0/win64_x64`
   - `CRConfig.xml` installiert unter:
     - `[INSTALLVERZ]SAP BusinessObjects Enterprise XI 4.0/java`
   - `mdas.properties` installiert unter:
     - `[INSTALLVERZ]/SAP BusinessObjects Enterprise XI 4.0/java/pjs/services/MDAS/resources/com/businessobjects/multidimensional/services`
   - WDeploy-Konfigurationsdateien installiert unter `[INSTALLVERZ]SAP BusinessObjects Enterprise XI 4.0/wdeploy/conf`:
     - `config.apache`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- `config.jboss7`
- `config.sapappsvr73`
- `config.tomcat6`
- `config.tomcat7`
- `config.weblogic11`
- `config.websphere7`
- `config.websphere8`
- `wdeploy.conf`

4. Folgende Webschichtdateien können vom Benutzer angepasst werden. Wenn Sie an einer dieser Dateien Änderungen vorgenommen haben, sichern Sie die Dateien aus dem Quellsystem. Zu einem späteren Zeitpunkt müssen diese Dateien wiederhergestellt werden, oder die Änderungen müssen erneut auf das Zielsystem angewendet werden.
   - `BO_trace.ini` installiert unter:
     - `[INSTALLVERZ]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/BOE/WEB-INF/TraceLog`
     - `[INSTALLVERZ]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/conf`
   - `clientaccesspolicy.xml` installiert unter:
     - `[INSTALLVERZ]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
   - `clientSDKOptions.xml` installiert unter:
     - `[INSTALLVERZ]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/clientapi/WEB-INF/lib`
     - `[INSTALLVERZ]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/lib`
   - `crossdomain.xml` installiert unter:
     - `[INSTALLVERZ]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
     - `[INSTALLVERZ]tomcat/webapps/ROOT`
   - Jegliche angepasste Dateien im `konfigurierten/angepassten` Ordner (in der Webschicht). Sichern Sie diese Dateien, um die Anpassung in das Zielsystem zu übertragen.
5. Sichern Sie sämtliche benutzerdefinierten Erweiterungen, die Sie manuell zum Quellsystem hinzugefügt haben; zum Beispiel Veröffentlichungserweiterungen, benutzerdefinierte Bibliotheken usw.

Bewahren Sie die oben erfassten Informationen mit der Kopie der Datenbanken und Dateien auf. Es ist sinnvoll, eine zweite Kopie aufzubewahren, die Sie nach Bedarf für spätere Systemkopierverfahren aktualisieren können.

14.6.2 Importieren in ein Zielsystem

Bei diesem Verfahren wird vorausgesetzt, dass Sie bereits Sicherungskopien der Datenbanken und Systemdateien der Quellimplementierung erstellt haben, die Sie im Zielsystem verwenden möchten. Alle Sicherungsdateien müssen aus demselben Sicherungssatz stammen. Außerdem benötigen Sie die Details (z.B. Clusterschlüssel und Datenbankanmeldedaten), die Sie unter “Exportieren aus einem Quellsystem” notiert haben.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Falls das Zielsystem an dem Netzwerkspeicherort mit Zugriff auf die Ressourcen des Quellsystems abgelegt wird, stellen Sie sicher, dass das Zielsystem erst auf diese Ressourcen zugreift, nachdem es neu konfiguriert wurde. Dies kann durch Einsatz einer Firewall zwischen den Zielsystem- und den Quellsystemressourcen oder Stoppen des Quellsystems während des Starts des Zielsystems ermöglicht werden. Nachdem Sie das Zielsystem das erste Mal gestartet haben, kann die Firewall entfernt bzw. das Quellsystem gestartet werden.

Wenn die BI-Plattform bereits auf dem Zielsystem installiert ist, stellen Sie sicher, dass es denselben Versionsstand und dasselbe Support-Package- und Patch-Level wie das Quellsystem zum Zeitpunkt der Erstellung der Kopie aufweist. Stellen Sie außerdem sicher, dass es denselben Installationspfad wie das Quellsystem verwendet.

1. Erstellen Sie auf dem Zielsystem die Verbindungen zu der oder den Datenbanken, in die Sie das CMS-Repository, die Audit-Datenbank und die Berichterstellungsdatenbank stellen möchten.

   > **Hinweis**
   >
   > Obwohl die Verbindungen auf eine andere Datenbank zeigen können, müssen sie denselben Verbindungsnamen oder DSN haben und dieselben Anmeldedaten verwenden wie das Quellsystem.

2. Stellen Sie mithilfe der Datenbanktools die CMS-Systemdatenbank und ggf. die Audit-Datenbank aus der Quellsystemsicherung in der Zieldatenbank wieder her.

   Wenn die Universen oder Berichte auf dem Zielsystem eine andere Berichterstellungsdatenbank verwenden müssen, ändern Sie die Datenbankverbindung so, dass sie zu dieser Datenbank zeigt.

   Wenn Sie weitere Anleitungen zu diesem Schritt benötigen, lesen Sie das Thema *Wiederherstellen des Systems* [Seite 497].

3. Wenn die BI-Plattform auf dem Zielhostsystem installiert ist, fahren Sie mit Schritt 4 fort. Wenn die BI-Plattform nicht installiert ist, installieren Sie sie auf dem Zielhostsystem, und berücksichtigen Sie dabei folgende Schritte:

   a) Installieren Sie die Programmversion und das Support-Package- und Patch-Level, die auch auf dem Quellsystem installiert sind.
   b) Verwenden Sie denselben Installationspfad wie das Quellsystem.
   c) Wählen Sie dieselben Komponenten, die auf dem Quellsystem installiert waren.
   d) Wenn Sie vom Installationsprogramm aufgefordert werden, die CMS-Datenbank (und ggf. die Audit-Datenbank) zu erstellen, wählen Sie die Option **Vorhandene Datenbank verwenden**, und geben Sie den Verbindungsnamen und die Verbindungsinformationen aus Schritt 1 ein.

      > **Hinweis**
      >
      > Reinitialisieren Sie die CMS-Datenbank nicht.

   e) Wenn Sie aufgefordert werden, den **Knotennamen** einzugeben, verwenden Sie die Namen, die Portnummern, das Plattformadministratorkennwort und den Clusterschlüssel, die auch auf dem Zielsystem verwendet werden.

      Vollständige Installationsanleitungen finden Sie im *Installationshandbuch für SAP BusinessObjects Business Intelligence*. Wenn die Installation des Systems abgeschlossen ist, fahren Sie mit Schritt 6 fort.

      > **Hinweis**
      >
      > Wenn Sie die Audit-Daten nicht aus dem Quellsystem kopieren, können Sie eine neue Audit-Datenbank erstellen, indem Sie das Auditing während der Installation konfigurieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

f) Stoppen Sie alle Knoten im CCM.

4. Falls die BI-Plattform bereits auf dem Zielsystem installiert ist, stoppen Sie alle Knoten im CCM. Starten Sie den CCM auf dem CMS-Hostrechner des Zielsystems.
5. Wenn die BI-Plattform bereits installiert ist, fügen Sie mithilfe der Option **Knoten neu erstellen** einen neuen Knoten hinzu.
   a) Verwenden Sie den **Knotennamen** und die **SIA-Portnummer** des Quellsystems.
   b) Wählen Sie **Neuen temporären CMS starten**.
   c) Wählen Sie eine neue **CMS-Portnummer** (kann jeder freie Port sein) und einen **CMS-Datenbanktyp** (der mit dem Typ der wiederhergestellten Datenbank übereinstimmt).
   d) Geben Sie die Details der Verbindung ein, für die die CMS-Datenbank in Schritt 1 wiederhergestellt wurde.
   e) Geben Sie den Clusterschlüssel des Quellsystems ein.
   f) Geben Sie das Administratorkennwort des Quellsystems ein.
6. Stellen Sie die Input- und Output-FRS-Dateispeicher auf dem Dateispeicher des Zielsystems wieder her. Verwenden Sie denselben Ordner, wie den im Quellsystem verwendeten Ordner.
7. Stellen Sie den Überwachungsdatenbankordner (falls Sie Überwachungsinformationen kopieren möchten) im selben Ordner, wie der im Quellsystem verwendete Ordner wieder her.
8. Stellen Sie den Hochstufverwaltungs-Datenbankordner (wenn Sie Hochstufverwaltungsinformationen kopieren möchten) im selben Ordner wieder her, der auch für das Quellsystem verwendet wurde.
9. Stellen Sie die Subversion-Dateien (wenn Sie Hochstufverwaltungsinformationen kopieren möchten) im selben Ordner wieder her, der auch für das Quellsystem verwendet wurde.
10. Stellen Sie die Dateien der semantischen Ebene/des Verbindungskonfigurationsservers im selben Ordner wie der im Quellsystem verwendete Ordner wieder her.
11. Starten Sie die Hostrechner des Zielsystems neu.
12. Falls Sie die BI-Plattform auf dem Zielsystem in Schritt 3 installiert haben, wenden Sie alle erforderlichen Support Packages oder Patches an, um mit dem Quellsystem gleichzuziehen.
13. Wenn das Zielsystem auf mehreren Hostrechnern ausgeführt wird, müssen die Schritte 1 bis 11 für jeden Hostrechner wiederholt werden.

    Verwenden Sie die Installationsoption "Erweitert", wenn Sie zusätzliche BI-Plattform-Knoten installieren. Denken Sie daran, dass dieselben Knotennamen wie im Quellsystem für die zusätzlichen Knoten im Zielsystem verwendet werden müssen.
14. Falls die CMS-Datenbank des Zielsystems einen anderen Datenbanktyp als das Quellsystem aufweist, führen Sie das Verfahren *Kopieren von Daten von einer CMS-Systemdatenbank in eine andere* [Seite 444] mit dem CCM aus und geben die Datenbank, die Sie für die Kopie verwenden möchten, als Ziel an.
15. Stellen Sie durch den Benutzer anpassbare Dateien wieder her, die Sie in Schritt 3 des Prozesses " Exportieren aus einem Quellsystem" gesichert haben.
16. Stellen Sie die Webschichtdateien wieder her, die Sie in Schritt 4 des Prozesses "Exportieren aus einem Quellsystem" gesichert haben.

    "Webschicht" bezieht sich auf den WDeploy-Bereitstellungsbereich, in dem Sie Ihre Anpassungen vornehmen können sowie auf den Webschichtinhalt, der auf dem Anwendungsserver implementiert wird.

    Wenden Sie beim Anwenden der Änderungen auf das Zielsystem keine Änderungen auf das Anwendungsserververzeichnis an; wenden Sie die Änderungen auf den WDeploy-Bereitstellungsbereich an, und implementieren Sie die Webschicht anschließend mit WDeploy auf dem Anwendungsserver.

    Der WDeploy-Bereitstellungsbereich befindet sich unter Windows im folgenden Verzeichnis: `<INSTALLVERZ>/SAP BusinessObjects Enterprise XI 4.0/warfiles`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

17. Stellen Sie die Erweiterungen wieder her, die Sie in Schritt 5 des Prozesses “Exportieren aus einem Quellsystem” gesichert haben.

Schritte nach der Systemkopie der BI-Plattform:

1. Die Installation des ersten Knotens auf dem Ziel erstellt einen temporären CMS, der am Ende der Installation gestoppt wird. Gehen Sie in der CMC zur Seite "Server", und löschen Sie diesen CMS.

   ➔ Nicht vergessen

   Falls Sie das Quellsystem nicht entfernen (oder falls Sie es parallel zum Zielsystem verwenden), sollte das Cluster auf dem Zielsystem umbenannt werden.

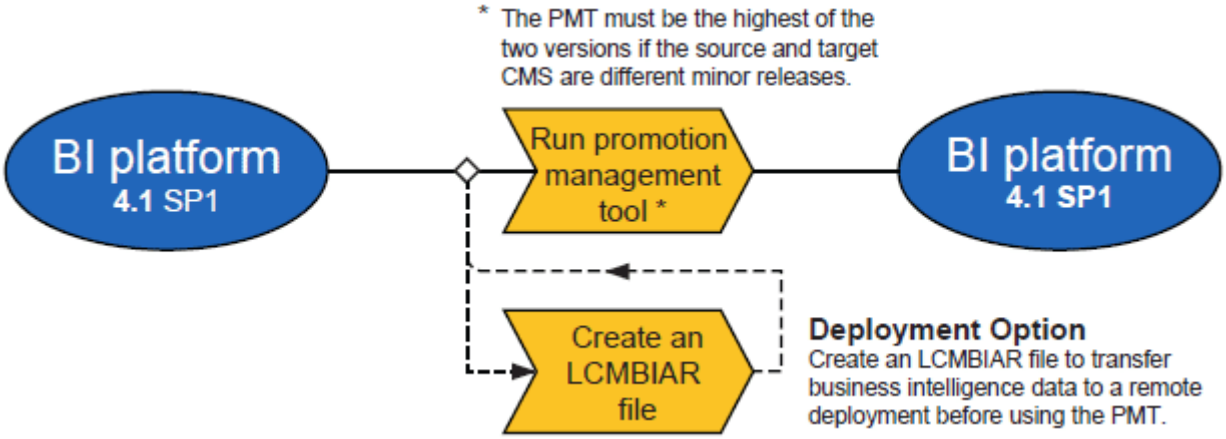
2. Führen Sie das Repository Diagnostic Tool für die Ziel-CMS-Datenbank aus.
3. Konfigurieren Sie ggf. die Windows-AD-Einzelanmeldung auf dem Zielsystem. Siehe *SSO bei der BI-Plattform mit AD-Authentifizierung* [Seite 282].
4. Konfigurieren Sie ggf. SLD auf dem Zielsystem. Einzelheiten hierzu finden Sie im SAP-Hinweis 1508421: “SAP SLD Data Supplier für Apache Tomcat”
5. Führen Sie auf dem Zielsystem eine Integritätsprüfung aus, um dessen Integrität zu prüfen.
6. Führen Sie eine vollständige Neuindizierung der Suche aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15 Hochstufverwaltung

15.1 Herzlich willkommen bei der Hochstufverwaltung

15.1.1 Übersicht



Mit der Hochstufverwaltung können Sie Business-Intelligence-Ressourcen (BI) von einem Repository in ein anderes verschieben, Abhängigkeiten von Ressourcen verwalten und ein Rollback von hochgestuften Ressourcen im Zielsystem durchführen, falls erforderlich. Es unterstützt außerdem die Verwaltung verschiedener Versionen derselben BI-Ressource.

Die Hochstufverwaltung ist in die Central Management Console integriert. Sie können eine BI-Ressource nur dann von einem System auf ein anderes hochstufen, wenn sowohl auf dem Quell- als auch auf dem Zielsystem dieselbe Version der BI-Plattform installiert ist.

15.1.2 Funktionen

Mit der Hochstufungsverwaltung können Sie folgende Aktionen für InfoObjects in der Zielbereitstellung ausführen.

- Neuen Auftrag erstellen
- Vorhandenen Auftrag kopieren
- Auftrag bearbeiten
- Auftragshochstufung zeitgesteuert verarbeiten
- Auftragsverlauf anzeigen
- Als LCMBIAR exportieren
- BIAR/LCMBIAR importieren

Der Hochstufungs-Workflow umfasst auch die folgenden Aufgaben:

- **Abhängigkeiten verwalten** – Mit dieser Funktion können Sie von InfoObjects abhängige Objekte in dem hochzustufenden Auftrag auswählen, filtern und verwalten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- **Zeitgesteuert verarbeiten** – Mit dieser Funktion können Sie einen Zeitpunkt für die Auftragshochstufung festlegen, anstatt ihn sofort nach der Erstellung hochzustufen. Sie können die Auftragshochstufung einmalig oder regelmäßig zeitgesteuert ausführen lassen.
- **Sicherheit** – Mit dieser Funktion können Sie InfoObjects mit den zugehörigen Sicherheitsrechten sowie ggf. mit den zugehörigen Anwendungsrechten hochstufen.
- **Probeweise Hochstufung** – Mit dieser Funktion können Sie die Hochstufung testen, um sicherzustellen, dass vor der tatsächlichen Hochstufung der InfoObjects alle nötigen Vorkehrungen getroffen werden können.
- **Rollback** – Mit dieser Funktion können Sie das Zielsystem nach der Hochstufung eines Auftrags wieder in seinen vorherigen Zustand zurückversetzen. Sie können ein Rollback für den gesamten Auftrag oder einen Teil des Auftrags durchführen.
- **Auditing** – Die von der Hochstufverwaltung generierten Ereignisse werden in der Audit-Datenbank gespeichert. Mit dieser Funktion können Sie die in der Audit-Datenbank protokollierten Ereignisse überwachen.
- **Überschreibungseinstellungen** der Hochstufverwaltung – Mit dieser Funktion können Sie die Überschreibungen über eine Auftragshochstufung prüfen und hochstufen.

15.1.3 Anwendungszugriffsrechte

In diesem Abschnitt werden die Anwendungszugriffsrechte für die Hochstufverwaltung beschrieben.

- Zugriffsrechte für die Hochstufverwaltung lassen sich in der CMC festlegen.
- Sie können genau abgestimmte Anwendungsrechte für verschiedene Funktionen innerhalb der Hochstufverwaltung einstellen.

Um bestimmte Rechte für die Hochstufverwaltung festzulegen, führen Sie die folgenden Schritte aus:

1. Melden Sie sich an der CMC an und wählen **Anwendungen**.
2. Doppelklicken Sie auf **Hochstufverwaltung**.
3. Klicken Sie auf **Benutzersicherheit**, und wählen Sie einen Benutzer aus. Sie können Sicherheitsrechte für den Benutzer anzeigen oder zuweisen.
4. Folgende Rechte stehen speziell für die Hochstufverwaltung zur Verfügung:
    - Zugang zum Bearbeiten von Überschreibungen gewähren
    - Zugriff gewähren und Sicherheitsrechte einschließen
    - Zugang zur Administration gewähren
    - Zugriff auf "Abhängigkeiten verwalten" gewähren
    - Auftrag erstellen
    - Auftrag löschen
    - Auftrag bearbeiten
    - LCMBIAR bearbeiten
    - Als LCMBIAR exportieren
    - LCMBIAR importieren
    - Auftrag hochstufen
    - Rollback-Auftrag
    - BOMM-Objekte (BusinessObjects-Metadatenobjekte)anzeigen und auswählen
    - Business Views anzeigen und auswählen
    - Kalender anzeigen und auswählen

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Verbindungen anzeigen und auswählen
- Profile anzeigen und auswählen
- QaaWS anzeigen und auswählen
- Berichtsobjekte anzeigen und auswählen
- Sicherheitseinstellungen anzeigen und auswählen
- Universen anzeigen und auswählen

5. Wenn Sie einem ausgewählten Benutzer Rechte zuweisen möchten, wählen Sie das entsprechende Recht aus und klicken auf **Sicherheit zuweisen**.

Die Zugriffsrechte für die Hochstufverwaltung werden in der CMC festgelegt.

15.1.4 Unterstützung für WinAD in der Hochstufverwaltung

Um die ordnungsgemäße Funktion der Anwendung Hochstufverwaltung zu gewährleisten, müssen Sie den `javaargs`-Argumenten für alle Adaptive Job Server Folgendes hinzufügen:

```
Djava.security.auth.login.config=<path>
\bsclogin.conf,Djava.security.krb5.conf=<path>\krb5.ini
```

➡ Nicht vergessen

Geben Sie den korrekten Pfad zu `bsclogin.conf` und `krb5.ini` in Ihrer Implementierung an.

15.1.5 Überschreibungsinformationen in BI-Plattform 4.1 SP3

Ab BI-Plattform 4.1 SP3 wurde die Derby-Datenbank durch im Repository gespeicherte Informationen ersetzt. Die Hochstufung von 4.0 SPx bzw. 4.1 SPx erfolgt automatisch.

Schlägt die automatische Hochstufung fehl (beispielsweise wenn der APS nach der Hochstufung Fehler anzeigt), können Sie das Kennzeichen für die erzwungene Migration manuell setzen:

1. Stoppen Sie den Adaptive Processing Server (APS), auf dem die Hochstufungsverwaltung ausgeführt wird.
2. Fügen Sie dem APS den Parameter `-Dcom.businessobjects.lcm.migrateoverrides=true` hinzu.
3. Starten Sie den APS, und lassen Sie die erzwungene Migration ausführen.

➡ Nicht vergessen

Nachdem die Migration abgeschlossen wurde, entfernen Sie den Parameter aus dem APS.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15.2 Erste Schritte mit der Hochstufverwaltung

15.2.1 Zugriff auf die Hochstufverwaltung

Um auf die Hochstufverwaltung zuzugreifen, wählen Sie auf der CMC-Startseite **Hochstufverwaltung**.

Alle Benutzer mit Ansichtsrechten für den Ordner **Hochstufungsaufträge** können die Hochstufverwaltung starten. Um Aufträge erstellen, zeitgesteuert verarbeiten und hochstufen zu können, müssen dem Benutzer jedoch zusätzliche Rechte durch den Administrator gewährt werden.

15.2.2 Benutzeroberflächen-Komponenten

In diesem Kapitel werden die GUI-Komponenten in der Hochstufverwaltung beschrieben.

- Symbolleiste des Hochstufverwaltung-Arbeitsbereichs
- Arbeitsbereich
- Strukturbereich
- Detailbereich
- Strukturliste und Job Viewer-Seite

Symbolleiste des Hochstufverwaltung-Arbeitsbereichs

In der folgenden Tabelle werden die in der Symbolleiste des Hochstufverwaltung-Arbeitsbereichs enthaltenen Optionen aufgeführt und die Aufgaben, die mit diesen Optionen ausgeführt werden können, beschrieben:

Option	Beschreibung
	ermöglicht das Erstellen eines neuen Ordners. Der neue Ordner wird als Unterordner im Ordner **Hochstufungsaufträge** erstellt.
	ermöglicht das Kopieren und Entfernen des ausgewählten Auftrags oder Ordners vom aktuellen Speicherort.
	ermöglicht das Kopieren des Auftrags oder Ordners vom aktuellen Speicherort.
	ermöglicht das Einfügen des kopierten Auftrags oder Ordners in einen neuen Speicherort.
	ermöglicht das Löschen eines vorhandenen Auftrags.
	ermöglicht das Regenerieren der Startseite, um eine aktualisierte Liste der Aufträge und Ordner abzurufen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung
Eigenschaften	ermöglicht das Ändern der Eigenschaften für einen ausgewählten Auftrag. Sie können Titel, Beschreibung und Schlüsselwörter des ausgewählten Auftrags ändern.
Änderungsverlauf	ermöglicht die Anzeige des Verlaufs des ausgewählten Auftrags.
Neuer Auftrag	ermöglicht das Erstellen eines neuen Auftrags.
Importieren	ermöglicht den Import von BIAR-, LCMBIAR- oder Überschreibungsdateien.
Bearbeiten	ermöglicht das Bearbeiten des ausgewählten Auftrags.
Hochstufen	ermöglicht das Hochstufen des ausgewählten Auftrags.
Rollback	ermöglicht es, den hochgestuften Auftrag im Zielsystem rückgängig zu machen. **Hinweis** Falls der Auftrag Objekte in das Ziel hochstuft, werden diese Objekte beim Rollback gelöscht. Falls der Auftrag Objekte im Ziel aktualisiert, wird beim Rollback die vorherige Version der Objekte wiederhergestellt.
	ermöglicht die Navigation zwischen verschiedenen Seiten der Auftragsliste. Mit dieser Option können Sie von einer Seite zur nächsten Seite oder zu einer bestimmten Seite durch Eingabe der Seitennummer wechseln.
Suchen	ermöglicht die Suche nach bestimmten Aufträgen. Sie können den Auftrag anhand des Namens, der Schlüsselwörter, der Beschreibung oder aller drei Parameter suchen.
Hochstufungsaufträge	ermöglicht das Anzeigen von Aufträgen und Ordnern.
Hochstufungsstatus	Zeigt die hochgestuften Aufträge nach Ihrem Status, wie z.B. "Erfolg", "Fehler" oder "Teilerfolg", an.

Arbeitsbereich

Der Arbeitsbereich auf der Startseite der Hochstufverwaltung zeigt eine Liste der Aufträge an. In diesem Bereich können Sie Namen, Status, Erstellungszeit und den Zeitpunkt der letzten Ausführung des Auftrags, Quell- und Zielsystem sowie den Auftragsersteller anzeigen.

Strukturbereich

Der Strukturbereich auf der Startseite der Hochstufverwaltung zeigt die Baumstruktur mit den Ordnern **Hochstufungsaufträge** und **Hochstufungsstatus** an. Die Aufträge werden in einer hierarchischen Struktur unter

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

dem Ordner **Hochstufungsaufträge** angezeigt. Der Ordner **Hochstufungsstatus** zeigt die hochgestuften Aufträge nach ihrem Status an.

Job Viewer-Bereich

Die Seite “Job Viewer” wird angezeigt, wenn ein Benutzer einen neuen Auftrag anlegt oder einen vorhandenen Auftrag erstellt. Sie enthält eine dynamisch generierte Liste der hochzustufenden InfoObjects sowie einen Detailbereich. In dieser Liste sind die InfoObjects in die Kategorien Benutzergruppen, Universen und Verbindungen unterteilt. Der Detailbereich enthält die Inhalte des in der Liste ausgewählten Knotens.

15.2.3 Verwenden der Option "Einstellungen"

Über die Option "Einstellungen" können Sie die Einstellungen konfigurieren, bevor Sie InfoObjects von einer Implementierung der BI-Platform in eine andere Implementierung der BI-Plattform und des SAP-Systems hochstufen. In diesem Abschnitt wird die Verwendung der Option "Einstellungen" beschrieben.

Klicken Sie auf die Dropdown-Liste **Einstellungen** im Bildschirm *Hochstufungsaufträge*. In dieser Dropdown-Liste werden folgende Optionen angezeigt:

- **Systeme verwalten** – Diese Option ermöglicht das Hinzufügen aller für Hochstufverwaltungsaktivitäten erforderlichen Systeme.
- **Rollback-Einstellungen** – Diese Option ermöglicht die Auswahl eines Systems, für das Rollbacks aktiviert sind.
- **Auftragseinstellungen** – Diese Option ermöglicht das Anzeigen abgeschlossener Instanzen auf der Seite "Abhängigkeiten" sowie das Verwalten von Aktivitäten zur Bereinigung von Auftragsinstanzen. Außerdem ist hier das Filtern nach Auftragserstellungsdatum möglich.
- **CTS-Einstellungen** – Mit dieser Option können Sie Informationen zum Webdienst und zum SAP-BW-System für die Integration des Enhanced Change and Transport Systems hinzufügen.

15.2.3.1 Verwendung der Option "Systeme verwalten"

In diesem Abschnitt wird die Verwendung der Option "Systeme verwalten" beschrieben. Mithilfe dieser Option können Sie Hostsysteme hinzufügen oder entfernen.

Zum Hinzufügen eines Hostsystems führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Symbolleiste des Hochstufverwaltung-Arbeitsbereichs auf **Einstellungen** und dann auch **Systeme verwalten**.

   Das Fenster *Systeme verwalten* wird angezeigt. In diesem Fenster wird eine Liste mit Hostnamen, Portnummern, Anzeigenamen und Beschreibungen angezeigt.
2. Klicken Sie auf **Hinzufügen**.

   Das Dialogfeld *System hinzufügen* wird angezeigt.
3. Geben Sie den Hostnamen, die Portnummer, den Anzeigenamen und die Beschreibung in die entsprechenden Felder ein.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Wählen Sie die Option **Als Quellsystem kennzeichnen** aus, um das System als Quellsystem zu identifizieren, d. h., das System, aus dem die Verbindungsinformationen stammen. Diese Option ist hilfreich beim Arbeiten mit Überschreibungen.

4. Klicken Sie auf **OK**, um das System hinzuzufügen.

   Das Hostsystem wird zu der Liste hinzugefügt.

> **Hinweis**
>
> Um ein Hostsystem zu entfernen oder zu bearbeiten, wählen Sie ein Hostsystem aus, und wählen Sie **Entfernen** oder **Bearbeiten**.

Weitere Informationen

Verwenden der Option "Rollbackeinstellungen" [Seite 527]
Verwenden der Option "Auftragseinstellungen" [Seite 527]

15.2.3.2 Verwenden der Option "Rollbackeinstellungen"

Der Rollbackprozess ist standardmäßig auf Systemebene aktiviert. Mit der Option **Rollbackeinstellungen** können Sie den Rollbackprozess auf Systemebene deaktivieren.

Um den Rollbackprozess auf Systemebene zu deaktivieren, führen Sie folgende Schritte aus:

1. Wählen Sie im Fenster *Rollback* aus der Liste der Hostsysteme das Hostsystem aus, das den Rollback-Prozess deaktivieren soll.
2. Klicken Sie auf **Speichern & schließen**, um die Änderungen zu speichern.

Weitere Informationen

Verwenden der Option "Auftragseinstellungen" [Seite 527]

15.2.3.3 Verwenden der Option "Auftragseinstellungen"

Unter der Option "Auftragseinstellungen" können Sie angeben, ob vollständig hochgestufte Instanzen auf der Seite “Abhängigkeiten verwalten” angezeigt werden sollen, und welche Anzahl von Auftragsinstanzen im System zulässig ist. Sie können eine der folgenden Optionen auswählen:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- **Abgeschlossene Instanzen auf der Seite "Abhängigkeiten verwalten" anzeigen** - Diese Option zeigt vollständig hochgestufte Instanzen, die einem Auftrag hinzugefügt werden können, auf der Seite " Abhängigkeiten verwalten".
- **Instanzen löschen, wenn mehr als N Instanzen eines Auftrags vorhanden sind** - Unter dieser Option kann die maximale Anzahl von Auftragsinstanzen pro Auftrag im System festgelegt werden.
- **Instanzen nach N Tagen löschen für Auftrag** - Unter dieser Option können Sie das Löschen von Instanzen festlegen, die vor einer bestimmten Anzahl von Tagen erstellt wurden.
- In der Liste **Erstellte Aufträge anzeigen** können Sie das Zeitintervall für die Anzeige von in einem bestimmten Zeitraum erstellten Aufträgen auswählen.

Zum Festlegen der Option **Auftragseinstellungen** führen Sie folgende Schritte aus:

1. Wählen Sie die Option aus, und geben Sie den gewünschten Wert ein.
2. Klicken Sie auf **Speichern**, um die aktualisierten Änderungen zu speichern.

Sie können auf **Standardeinstellungen** klicken, um die Standardwerte festzulegen und auf **Schließen**, um das Fenster zu schließen.

> **Hinweis**
>
> Die alten Auftragsinstanzen werden erst beim nächsten Ausführen des Auftrags gelöscht.

Weitere Informationen

Verwenden der Option „Versionsverwaltungseinstellungen“ [Seite 582]

15.2.3.4 Verwenden der Option "Überschreibungseinstellungen"

Die Option "Überschreibungseinstellungen" ermöglicht das Hochstufen von Überschreibungen mithilfe einer Auftragshochstufung oder einer LCMBIAR-Datei. Diese Option ermöglicht das Scannen, Hochstufen und Bearbeiten der Datenbankverbindungsinformationen für Crystal-Reports- und Universen-Verbindungen. Mit dieser Option ist auch das Bearbeiten der QAAWS-URLs möglich.

> **Hinweis**
>
> Um die Option "Überschreibungseinstellungen" verwenden zu können, müssen Sie Adobe Flash Viewer installieren.

Der Begriff *System* wird für folgende Vorgänge verwendet. Es gibt drei Arten von Systemen:

- *Ursprung* - Das ursprüngliche System jeglicher Verbindungsinformationen.
- *Zentrale Hochstufverwaltung* - Das System, auf dem die Hochstufverwaltung ausgeführt wird.
- *Ziel* - Das Endsystem, in das die BI-Ressourcen hochgestuft werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15.2.3.4.1 Hochstufen von Überschreibungen

Fügen Sie vor dem Hochstufen von Überschreibungen ein Hostsystem hinzu. Information über das Hinzufügen eines Hostsystems finden Sie unter *Verwendung der Option "Systeme verwalten"* [Seite 526].

Um die Überschreibungen hochzustufen, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Symbolleiste des Hochstufverwaltung-Arbeitsbereichs auf die Option **Überschreibungseinstellungen**.
   Das Fenster *Überschreibungseinstellungen* wird angezeigt.
2. Wenn Sie am zentralen Hochstufverwaltungssystem angemeldet sind, melden Sie sich vom System ab.
3. Klicken Sie auf **Anmelden**, um eine Verbindung zum Ursprungssystem herzustellen.
   Das Fenster *Systemanmeldung* wird angezeigt.
4. Wählen Sie das als **Ursprung** markierte Quellsystem aus, um die Objekte zu durchsuchen, und melden Sie sich mit gültigen Anmeldedaten beim System an.
5. Wählen Sie in der Dropdownliste **Start** neben **Scan** die Option **Start**.
   Der Scan-Vorgang wird gestartet. Die *Liste der eindeutigen Verbindungen* wird angezeigt.

   > **Hinweis**
   >
   > Um einen wiederkehrenden Scan-Vorgang zeitgesteuert zu verarbeiten, wählen Sie in der Dropdown-Liste **Wiederholungseinstellungen**.

6. Ändern Sie in der Liste der Überschreibungen den Status von den hochzustufenden Objekten in "Aktiv", und klicken Sie auf **Speichern**.
7. Klicken Sie auf **Überschreibungen hochstufen**.
   Das Fenster *Überschreibungen hochstufen* mit der Liste der Zielsysteme wird angezeigt.
8. Klicken Sie auf **Anmelden**, um sich beim Zielsystem mit gültigen Anmeldedaten anzumelden.

   Sie können mehrere Zielsysteme angeben.
9. Klicken Sie auf **Hochstufen**.
   Die Hochstufung der Überschreibungen ist abgeschlossen.

   > **Hinweis**
   >
   > Wenn die Überschreibungen im Zielsystem während der Hochstufung der InfoObjects fehlschlagen, setzt das System den Auftragsstatus auf `Teilerfolg` und den Warnungsstatus des Objekts auf `Überschreibungen fehlgeschlagen`.

10. Melden Sie sich vom Ursprungssystem ab.
11. Klicken Sie auf dem Bildschirm *Überschreibungseinstellungen* auf **Anmelden**.
    Das Fenster "Systemanmeldung" wird angezeigt.
12. Melden Sie sich mit gültigen Anmeldedaten an einem der Zielsysteme an.
    In der *Liste der eindeutigen Verbindungen* werden alle hochgestuften Objekte aufgeführt. Der Status dieser Objekte ist "Inaktiv".
13. Aktivieren Sie das Kontrollkästchen **Auswählen** für die Objekte, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
14. Überschreiben Sie die entsprechenden Werte, und klicken Sie dann auf **Fertig**.
    Die bearbeiteten Objekte erhalten den Status "Aktiv".

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15. Klicken Sie auf **Speichern**.

15.2.3.4.2 Hochstufen von Überschreibungen mit BIAR-Dateien

Fügen Sie vor dem Hochstufen von Überschreibungen ein Hostsystem hinzu. Information über das Hinzufügen eines Hostsystems finden Sie unter *Verwendung der Option "Systeme verwalten"* [Seite 526].

Um die Überschreibungen durch BIAR-Dateien hochzustufen, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Symbolleiste des Hochstufverwaltung-Arbeitsbereichs auf die Option **Überschreibungseinstellungen**.
   Das Fenster *Überschreibungseinstellungen* wird angezeigt.
2. Wenn Sie am zentralen Hochstufverwaltungssystem angemeldet sind, melden Sie sich vom System ab.
3. Klicken Sie auf **Anmelden**, um eine Verbindung zum Ursprungssystem herzustellen.
   Das Fenster *Systemanmeldung* wird angezeigt.
4. Wählen Sie auf dem Bildschirm *Überschreibungseinstellungen* das als **Ursprung** markierte Quellsystem aus, um die Objekte zu durchsuchen, und melden Sie sich mit gültigen Anmeldedaten beim System an.
5. Wählen Sie in der Dropdownliste **Start** neben **Scan** die Option **Start**.
   Der Scan-Vorgang wird gestartet, und die Liste der Überschreibungen wird angezeigt.

   > **Hinweis**
   >
   > Um einen wiederkehrenden Scan-Vorgang zeitgesteuert zu verarbeiten, wählen Sie in der Dropdown-Liste **Wiederholungseinstellungen**.

6. Ändern Sie in der Liste der Überschreibungen den Status der entsprechenden Objekte in "Aktiv", und klicken Sie auf **Speichern**.
7. Klicken Sie auf **Überschreibungen hochstufen**.
   Das Fenster *Überschreibungen hochstufen* mit der Liste der Zielsysteme wird angezeigt.
8. Aktivieren Sie zur Verschlüsselung der BIAR-Datei mittels Kennwort das Kontrollkästchen **Kennwortverschlüsselung**.
   Die Felder **Kennwort** und **Kennwort bestätigen** werden aktiviert.
9. Geben Sie im Feld **Kennwort** ein Kennwort ein. Geben Sie dasselbe Kennwort noch einmal im Feld **Kennwort bestätigen** ein.
10. Klicken Sie auf **Exportieren**, und speichern Sie die BIAR-Datei mit den Überschreibungen in einem Dateisystem.
11. Melden Sie sich über die CMC am Zielsystem an, und klicken Sie in der Hochstufungsverwaltung auf **Importieren** > **Datei überschreiben**.
    Das Fenster *LCMBIAR-Datei importieren* wird angezeigt.
12. Klicken Sie auf **Durchsuchen**, um zur BIAR-Datei zu navigieren.
13. Geben Sie im Feld **Kennwort** ein Kennwort für die BIAR-Datei ein.

    > **Hinweis**
    >
    > Das Feld **Kennwort** wird nur angezeigt, wenn die ausgewählte BIAR-Datei mit einem Kennwort verschlüsselt ist.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

14. Klicken Sie auf **OK**. Die Hochstufung der Überschreibungen ist abgeschlossen.
15. Melden Sie sich vom Ursprungssystem ab.
16. Klicken Sie auf dem Bildschirm *Überschreibungseinstellungen* auf **Anmelden**.
    Das Fenster *Systemanmeldung* wird angezeigt.
17. Melden Sie sich beim Zielsystem mit gültigen Anmeldedaten an.
    In der Liste der Überschreibungen werden die importierten Objekte aufgeführt. Der Status dieser Objekte ist "Inaktiv".
18. Aktivieren Sie das Kontrollkästchen **Auswählen** für die Objekte, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**. Die bearbeiteten Objekte sind durch ein Symbol gekennzeichnet.

    > **Hinweis**
    >
    > Sie können die Überschreibungsobjekte löschen, indem Sie auf das Symbol klicken.

19. Überschreiben Sie die entsprechenden Werte, und klicken Sie dann auf **Fertig**.
    Die bearbeiteten Objekte erhalten den Status "Aktiv".
20. Klicken Sie auf **Speichern**.

15.2.3.4.3 Hochstufen von Überschreibungen mit CTS+

Fügen Sie vor dem Hochstufen von Überschreibungen ein Hostsystem hinzu. Information über das Hinzufügen eines Hostsystems finden Sie unter *Verwendung der Option "Systeme verwalten"* [Seite 526].

Um die Überschreibungen durch CTS+ hochzustufen, führen Sie die folgenden Schritte aus:

> **Hinweis**
>
> Starten Sie die Hochstufverwaltung über die SAP-Authentifizierung, um diese Option verfügbar zu machen.

1. Klicken Sie in der Symbolleiste des Hochstufverwaltung-Arbeitsbereichs auf die Option **Überschreibungseinstellungen**.
   Das Fenster *Überschreibungseinstellungen* wird angezeigt.
2. Wenn Sie am zentralen Hochstufverwaltungssystem angemeldet sind, melden Sie sich vom System ab.
3. Klicken Sie auf **Anmelden**, um eine Verbindung zum Ursprungssystem herzustellen.
   Das Fenster *Am System anmelden* wird angezeigt.
4. Wählen Sie das als **Ursprung** markierte Quellsystem aus, um die Objekte zu durchsuchen, und melden Sie sich mit gültigen Anmeldedaten beim System an.
5. Wählen Sie in der Dropdownliste **Start** neben **Scan** die Option **Start**.
   Der Scan-Vorgang wird gestartet. Die *Liste der Überschreibungen* wird angezeigt.

   > **Hinweis**
   >
   > Um einen wiederkehrenden Scan-Vorgang zeitgesteuert zu verarbeiten, wählen Sie in der Dropdown-Liste **Wiederholungseinstellungen**.

6. Ändern Sie in der Liste der Überschreibungen den Status von den hochzustufenden Objekten in "Aktiv", und klicken Sie auf **Speichern**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7. Klicken Sie auf **Überschreibungen hochstufen**.
   Das Fenster *Überschreibungen hochstufen* mit der Liste der Zielsysteme wird angezeigt.
8. Wählen Sie in der Dropdown-Liste **Hochstufungsoptionen** die Option **Hochstufen mit CTS+** aus.
9. Klicken Sie auf **Hochstufen**.
10. Gehen Sie zum Freigeben der Überschreibungen an das Zielsystem wie folgt vor:
    a) Melden Sie sich am Domänencontroller von CTS+ an, und öffnen Sie die Web-Benutzeroberfläche des *Transport Organizers*. Weitere Informationen zur Verwendung der Web-Benutzeroberfläche des Transport Organizers erhalten Sie unter *Web-Benutzeroberfläche des Transport Organizers*.
    b) Wenn der Status der Anforderung **Modifiable** (Modifizierbar) lautet, klicken Sie auf **Release** (Freigeben), um die Transportanforderung des SAP BOE-Objekts freizugeben. Weitere Informationen zur Freigabe von Transportanforderungen mit ABAP-fremden Objekten finden Sie unter *Freigabe von Transportanforderungen mit ABAP-fremden Objekten*.
    c) Schließen Sie die Web-Benutzeroberfläche des *Transport Organizers*.
11. Gehen Sie zum Importieren der Überschreibungen in das Zielsystem wie folgt vor:
    a) Melden Sie sich beim Domänencontroller von CTS+ an.
    b) Rufen Sie die STMS-Transaktion auf, um das Transport Management System zu öffnen.
    c) Klicken Sie auf das Symbol **Importübersicht**.

       Der Bildschirm *Importübersicht* wird angezeigt. Hier können Sie die Elemente in der Importqueue von allen Systemen einsehen.
    d) Klicken Sie auf die System-ID des Ziel-Hochstufverwaltungssystems.
       Es wird eine Liste der Transportanforderungen angezeigt, die in das System importiert werden können.
    e) Klicken Sie auf **Regenerieren**.
    f) Importieren Sie die relevanten Transportanforderungen. Weitere Informationen finden Sie unter *Importieren von Anforderungen*.
12. Die Hochstufung der Überschreibungen ist abgeschlossen.
13. Melden Sie sich mit gültigen Anmeldedaten an einem der Zielsysteme an.
    In der "Liste der Überschreibungen" werden alle hochgestuften Objekte aufgeführt. Der Status dieser Objekte ist "Inaktiv".
14. Aktivieren Sie das Kontrollkästchen **Auswählen** für die Objekte, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
15. Überschreiben Sie die entsprechenden Werte, und klicken Sie dann auf **Fertig**.
    Die bearbeiteten Objekte erhalten den Status „Aktiv“.
16. Klicken Sie auf **Speichern**.

15.2.3.5 Verwenden der Option "CTS-Einstellungen"

Mit dieser Option können Sie Webdienste hinzufügen und BW-Systeme in Ihrer Umgebung verwalten. Im Abschnitt *Konfigurieren von CTS+-Einstellungen im Hochstufverwaltungstool* [Seite 570] finden Sie weitere Informationen zum Verwenden der Option "CTS-Einstellungen" und zum Einrichten des CTS für den Einsatz mit der Hochstufverwaltung.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15.3 Verwenden der Hochstufverwaltung

Wenn Sie sich bei der Hochstufverwaltung anmelden, wird standardmäßig die Seite *Hochstufungsaufträge* angezeigt.

Die *Hochstufungsaufträge*-Startseite enthält eine Reihe von Registerkarten, über die Sie folgende Aufgaben ausführen können:

- Klicken Sie auf **Neuer Auftrag**, um einen neuen Auftrag zu erstellen. Sie können auch mit der rechten Maustaste auf die Startseite klicken und in der Liste **Neuer Auftrag** auswählen.
- Wählen Sie **Importieren** > **Datei importieren**, um eine BIAR- oder eine LCMBIAR-Datei direkt aus dem Dateisystem zu importieren, anstatt das gesamte Verfahren zum Erstellen eines neuen Auftrags durchzuführen.
- Wählen Sie **Importieren** > **Datei überschreiben** aus, um Überschreibungen zu importieren.
- Wählen Sie in der Liste einen Auftrag aus, den Sie bearbeiten möchten, und wählen Sie dann **Bearbeiten**.
- Wählen Sie in der Liste einen Auftrag aus, und klicken Sie dann auf **Hochstufen**, um den Auftrag aus dem Quellsystem in das Zielsystem hochzustufen, oder exportieren Sie den Auftrag in eine LCMBIAR-Datei.
- Wählen Sie in der Liste einen zuvor ausgeführten Auftrag aus, und wählen Sie dann **Rollback**, um die hochgestuften Objekte aus dem Zielsystem zurückzusetzen.
- Wählen Sie in der Liste einen zuvor ausgeführten Auftrag aus, und wählen Sie dann **Verlauf**, um die vorherigen Hochstufungsinstanzen des ausgewählten Auftrags anzuzeigen.
- Wählen Sie in der Liste einen Auftrag aus, und klicken Sie auf **Eigenschaften**, um die Eigenschaften des ausgewählten Auftrags einzusehen, beispielsweise Titel, ID, Dateiname und Beschreibung.

Der Anwendungsbereich *Hochstufungsaufträge* zeigt die Liste der im System vorhandenen Aufträge und Ordner mit folgenden Informationen für jeden Auftrag oder Ordner an:

- **Name:** Zeigt den Namen des erstellten Auftrags oder Ordners an.
- **Status:** Zeigt den Status des Auftrags an, beispielsweise "Erstellt", "Erfolg", "Teilerfolg", "Wird ausgeführt" oder "Fehler".
- **Erstellt:** Zeigt das Erstellungsdatum und die Erstellungsuhrzeit des Auftrags bzw. des Ordners an.
- **Letzte Ausführung:** Zeigt Datum und Uhrzeit der letzten Hochstufung des Auftrags an.
- **Quellsystem:** Zeigt den Namen des Systems an, von dem der Auftrag hochgestuft wird.
- **Zielsystem:** Zeigt den Namen des Systems an, in das der Auftrag hochgestuft wird.
- **Erstellt von:** Zeigt den Namen des Benutzers an, der den jeweiligen Auftrag oder Ordner erstellt hat.

> **Hinweis**
>
> Die Hochstufverwaltung verwendet für all ihre Aktivitäten das BI-Plattform-SDK.

15.3.1 Erstellen und Löschen von Ordnern

In diesem Abschnitt wird beschrieben, wie Ordner auf der Hochstufungsaufträge-Startseite erstellt und gelöscht werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15.3.1.1 Erstellen von Ordnern

In diesem Abschnitt wird das Erstellen von Ordnern beschrieben.

Zum Erstellen eines Ordners führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Symbolleiste "Hochstufverwaltung" auf .
2. Geben Sie den Ordnernamen im Dialogfeld *Ordner erstellen* ein.
3. Klicken Sie auf **OK**.

Es wird ein neuer Ordner erstellt.

Weitere Informationen

Einen Auftrag erstellen [Seite 534]
Löschen eines Ordners [Seite 534]

15.3.1.2 Löschen eines Ordners

In diesem Abschnitt wird das Löschen von Ordnern beschrieben.

Zum Löschen eines Ordners führen Sie die folgenden Schritte aus:

1. Wählen Sie auf der *Hochstufungsaufträge*-Startseite einen Ordner aus.
2. Klicken Sie auf .

   Es wird ein Bestätigungsdialogfeld angezeigt.
3. Klicken Sie auf **OK**.

Der ausgewählte Ordner wird gelöscht.

Weitere Informationen

Einen Auftrag erstellen [Seite 534]

15.3.2 Einen Auftrag erstellen

In diesem Abschnitt wird das Erstellen von neuen Aufträgen mit der Hochstufverwaltung beschrieben.

In der folgenden Tabelle sind die GUI-Elemente und Felder, die Sie zum Erstellen eines neuen Auftrags verwenden können, aufgeführt:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Feld	Beschreibung
Name	Name des zu erstellenden Auftrags
Beschreibung	Beschreibung des zu erstellenden Auftrags
Schlüsselwörter	Die Schlüsselwörter für den Inhalt des zu erstellenden Auftrags.
Auftrag speichern unter	Der standardmäßig ausgewählte Ordner wird angezeigt.
Quellsystem	Name des BI-Plattformsystems, von dem ein Auftrag hochgestuft werden soll.
Zielsystem	Name des BI-Plattformsystems, in das ein Auftrag hochgestuft werden soll.
Benutzername	Die Anmelde-ID, die Sie für die Anmeldung beim Quell- oder Zielsystem verwenden müssen.
Kennwort	Das Kennwort, das Sie für die Anmeldung beim Quell- oder Zielsystem verwenden müssen.
Authentifizierung	Der Authentifizierungstyp, der zur Anmeldung beim Quell- oder Zielsystem verwendet wird. Die Hochstufverwaltung unterstützt folgende Authentifizierungstypen: • Enterprise • Windows AD • LDAP • SAP

Hinweis

Stellen Sie vor der Auftragserstellung sicher, dass die Überschreibungen, falls vorhanden, bearbeitet und im Zielsystem aktualisiert wurden, damit der Inhalt der BI-Plattform automatisch aktualisiert wird. Weitere Informationen finden Sie im Abschnitt "Verwenden der Option "Überschreibungseinstellungen"".

Zum Erstellen eines neuen Auftrags mit der Hochstufverwaltung führen Sie die folgenden Schritte aus:

1. Starten Sie die Hochstufverwaltung.
2. Klicken Sie auf der *Hochstufungsaufträge*-Startseite auf **Neuer Auftrag**.
3. Geben Sie den Namen, die Beschreibung und die Schlüsselwörter für den Auftrag in die entsprechenden Felder ein.

   Hinweis

   Die Eingabe von Informationen in die Felder "Beschreibung", "Schlüsselwörter" und "Zielsystem" ist optional.

4. Wählen Sie im Feld **Auftrag speichern im** den Ordner aus, in dem der Auftrag gespeichert werden soll.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Das Feld **Auftrag speichern in** wird standardmäßig mit dem Namen des Ordners belegt, der im Ordnerbereich vor dem Klicken auf **Neuer Auftrag** hervorgehoben ist.

5. Wählen Sie Quell- und Zielsystem aus den entsprechenden Dropdownlisten aus.

   Falls der Name des Systems nicht in der Dropdownliste angezeigt wird, klicken Sie auf die Option **Bei einem neuen CMS anmelden**. Ein neues Fenster wird geöffnet. Geben Sie den Namen des Systems sowie den Benutzernamen und das Kennwort ein.
6. Klicken Sie auf **Erstellen**.

   Das Fenster "Objekte hinzufügen" wird angezeigt.
7. Wählen Sie die dem Auftrag hinzuzufügenden Objekte aus dem Quellsystem aus, und wählen Sie dann **Hinzufügen & Schließen**.
8. Klicken Sie auf **Speichern**.

Der neu erstellte Auftrag wird im CMS-Repository des Quellsystems gespeichert.

> **Hinweis**
>
> Wenn Sie einen Auftrag mit einem Ordner als primärem Objekt erstellen und der Auftrag wiederkehrend ist, umfasst der Auftrag jeglichen Inhalt, der dem Ordner während der nächsten Laufzeit hinzugefügt wird.

Weitere Informationen

Verwenden der Option "Überschreibungseinstellungen" [Seite 528]

15.3.2.1 Anmelden an einem neuen CMS

In diesem Abschnitt wird die Anmeldung bei einem neuen CMS beschrieben.

Führen Sie zur Anmeldung bei einem neuen CMS folgende Schritte aus:

1. Starten Sie die Hochstufverwaltung.
2. Erstellen Sie einen neuen Auftrag.

   Weitere Informationen über das Erstellen neuer Aufträge finden Sie unter *Einen Auftrag erstellen* [Seite 534].
3. Wählen Sie in der Dropdownliste **Quellsystem** die Option **Bei einem neuen CMS anmelden**.
   Das Dialogfeld *Systemanmeldung* wird angezeigt.
4. Wählen Sie in der Dropdown-Liste das System aus, oder geben Sie einen neuen Systemnamen ein.
5. Geben Sie die Anmeldedaten ein, wählen Sie den geeigneten Authentifzierungstyp, und klicken Sie auf **Anmelden**.
6. Wählen Sie in der Dropdownliste **Zielsystem** die Option **Bei einem neuen CMS anmelden**.
7. Wählen Sie in der Dropdown-Liste das System aus, oder geben Sie einen neuen Systemnamen ein.
8. Geben Sie die Anmeldedaten ein, wählen Sie den geeigneten Authentifzierungstyp, und klicken Sie auf **Anmelden**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Bearbeiten von Aufträgen [Seite 538]
Hinzufügen eines InfoObjects zu einem Auftrag [Seite 539]
Hochstufen von Aufträgen mit nicht verbundenen Repositorys [Seite 541]
Zeitsteuern von Auftragshochstufungen [Seite 546]

15.3.3 Erstellen eines neuen Auftrags durch Kopieren eines vorhandenen Auftrags.

In diesem Abschnitt wird beschrieben, wie ein neuer Auftrag durch Kopieren eines vorhandenen Auftrags erstellt wird.

Führen Sie folgende Schritte aus, um einen neuen Auftrag durch Kopieren eines vorhandenen Auftrags zu erstellen:

1. Starten Sie die Hochstufverwaltung.
2. Klicken Sie auf der *Hochstufungsaufträge*-Startseite auf **Neuer Auftrag**.
3. Wählen Sie die Option **Vorhandenen Auftrag kopieren**

   Das Fenster *Vorhandenen Auftrag kopieren* wird geöffnet und zeigt die Liste der Aufträge im Ordner **Hochstufungsaufträge** an.
4. Wählen Sie den gewünschten Auftrag aus der Auftragsliste aus, und klicken Sie auf **Erstellen**.

   Daraufhin werden der Name, Schlüsselwörter und eine Beschreibung des Auftrags sowie die Felder *Auftrag speichern im* und *Ziel* angezeigt. Sie können diese Felder nach Bedarf bearbeiten.
5. Durchsuchen Sie das Feld **Auftrag speichern im**, und wählen Sie einen Ordner, in dem Sie den Auftrag speichern möchten, und klicken Sie auf **Erstellen**.

Ein neuer Auftrag wird erstellt, und das Fenster *Objekte hinzufügen* wird angezeigt.

Weitere Informationen

Hinzufügen eines InfoObjects zu einem Auftrag [Seite 539]
Bearbeiten von Aufträgen [Seite 538]
Hochstufen von Aufträgen mit nicht verbundenen Repositorys [Seite 541]

15.3.4 Suchen nach Aufträgen

Mit der Suchfunktion der Hochstufverwaltung können Sie einen Auftrag im Repository suchen.

Zum Suchen eines Auftrags führen Sie die folgenden Schritte aus:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Geben Sie den zu suchenden Text in das Feld **Suchen** auf der Startseite ein.
2. Klicken Sie auf die Liste neben dem Feld **Suchen**, um die Suchparameter anzugeben. Sie können folgende Suchparameter angeben:
   - **Titel durchsuchen** – Mit dieser Option können Sie einen Auftrag anhand seines Namens suchen.
   - **Schlüsselwort suchen** – Mit dieser Option können Sie einen Auftrag anhand seines Schlüsselworts suchen.
   - **Beschreibung suchen** – Mit dieser Option können Sie einen Auftrag anhand seiner Beschreibung suchen.
   - **Alle Felder durchsuchen** – Mit dieser Option können Sie einen Auftrag anhand seines Titels, seiner Schlüsselwörter und seiner Beschreibung suchen.
3. Klicken Sie auf das Symbol "Suchen".

Weitere Informationen

Hinzufügen eines InfoObjects zu einem Auftrag [Seite 539]
Bearbeiten von Aufträgen [Seite 538]

15.3.5 Bearbeiten von Aufträgen

In diesem Abschnitt wird das Bearbeiten von Aufträgen beschrieben.

> **Hinweis**
>
> Beim Bearbeiten eines Auftrags wird kein neuer Auftrag erstellt.

Zum Bearbeiten eines Auftrags führen Sie die folgenden Schritte aus:

1. Starten Sie die Hochstufverwaltung.
2. Wählen Sie auf der *Hochstufungsaufträge*-Startseite den zu bearbeitenden Auftrag aus.
3. Klicken Sie auf **Bearbeiten**.

   Die Details des ausgewählten Auftrags werden angezeigt. Sie können nach Bedarf InfoObjects hinzufügen oder entfernen, Abhängigkeiten verwalten oder den Auftrag hochstufen.

Der Name des Quellsystems kann beim Bearbeiten des Auftrags nicht geändert werden.

Weitere Informationen

Hinzufügen eines InfoObjects zu einem Auftrag [Seite 539]
Hochstufen von Aufträgen mit nicht verbundenen Repositorys [Seite 541]
Zeitsteuern von Auftragshochstufungen [Seite 546]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15.3.6 Hinzufügen eines InfoObjects zu einem Auftrag

Jeder Auftrag muss einen Satz InfoObjects enthalten. Daher müssen Sie InfoObjects zu einem Auftrag hinzufügen, bevor Sie ihn in das Zielsystem hochstufen.

> **Hinweis**
>
> Beim Hochstufen eines Crystal-Reports-Berichts, der auf Business-View-InfoObjects (Datenverbindung, Datengrundlage, Business-Elemente und Business View) basiert, müssen Sie die Sicherheitsinformationen (Datenzugriffsrecht für Datenverbindung und Recht zum Anzeigen von Datenfeldern für Datengrundlage- und Business-Elemente) einschließen, um Daten in einem Bericht auf dem Zielsystem anzeigen zu können.

Führen Sie die folgenden Schritte aus, um ein InfoObject zu einem Auftrag hinzuzufügen:

1. Starten Sie die Hochstufverwaltung.
2. Erstellen Sie einen neuen Auftrag, oder bearbeiten Sie einen vorhandenen Auftrag.
   Informationen zum Erstellen von neuen Aufträgen finden Sie unter *Einen Auftrag erstellen* [Seite 534] und *Bearbeiten von Aufträgen* [Seite 538].
3. Klicken Sie zum Bearbeiten eines Auftrags auf **Objekte hinzufügen**.

   > **Hinweis**
   >
   > Beim Erstellen eines neuen Auftrags wird das Dialogfeld *Objekte hinzufügen* angezeigt.

4. Navigieren Sie zu dem Ordner, aus dem Sie ein InfoObject wählen möchten.
   Die Liste der InfoObjects wird im ausgewählten Ordner angezeigt.
5. Wählen Sie das dem Auftrag hinzuzufügende InfoObject, und klicken Sie auf **Hinzufügen**.

   Wenn Sie ein InfoObject hinzufügen und das Dialogfeld "Objekte aus dem System hinzufügen: `<NAME>`" schließen möchten, klicken Sie auf **Hinzufügen & Schließen**. Das InfoObject wird an den Auftrag angehängt, und das Dialogfeld wird geschlossen.

Nachdem Sie ein InfoObject zu dem Auftrag hinzugefügt haben, klicken Sie mit der rechten Maustaste auf der Seite *Auftrags-Viewer*, und wählen die Hochstufungsprozesse aus, um mit der Hochstufung fortzufahren. Sie können die abhängigen Objekte des ausgewählten InfoObjects mit der Option **Abhängigkeiten verwalten** auf der Seite *Job Viewer* verwalten.

> **Hinweis**
>
> - Die Strukturliste, die im linken Bereich auf der Seite *Auftrags-Viewer* angezeigt wird, zeigt den Auftrag zusammen mit seinen abhängigen Objekten in einer flachen Baumstruktur an.
> - Klicken Sie nach dem Hinzufügen der InfoObjects auf **Speichern**, um die Änderungen zu speichern. Andernfalls wird der Benutzer über eine Option zum Speichern des Auftrags aufgefordert, wenn er die Registerkarte schließt.

Optimale Vorgehensweise: Es wird empfohlen, eine kleine Anzahl von maximal 100 InfoObjects auf einmal zum Hochstufen auszuwählen, um eine optimale Performance der Hochstufverwaltung zu erzielen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Verwalten der Abhängigkeiten eines Auftrags [Seite 540]
Hochstufen von Aufträgen mit nicht verbundenen Repositorys [Seite 541]
Zeitsteuern von Auftragshochstufungen [Seite 546]

15.3.7 Verwalten der Abhängigkeiten eines Auftrags

In diesem Abschnitt wird die Verwaltung von abhängigen Objekten eines InfoObjects beschrieben.

Zum Verwalten der abhängigen Objekte eines InfoObjects führen Sie folgende Schritte aus:

1. Starten Sie die Hochstufverwaltung.
2. Erstellen Sie einen neuen Auftrag, oder bearbeiten Sie einen vorhandenen Auftrag.
   Informationen zum Erstellen von neuen Aufträgen finden Sie unter *Einen Auftrag erstellen* [Seite 534] und *Bearbeiten von Aufträgen* [Seite 538].
3. Fügen Sie dem Auftrag die erforderlichen InfoObjects hinzu, und schließen Sie das Dialogfeld *Objekte hinzufügen*, um zum Fenster *Auftrags-Viewer* zurückzukehren.
4. Klicken Sie auf **Abhängigkeiten verwalten**.
   Das Fenster *Abhängigkeiten verwalten* wird angezeigt. Es zeigt die Liste der InfoObjects und ihre abhängigen Objekte an. Um nur die abhängigen Objekte anzuzeigen, die nicht ausgewählt wurden, klicken Sie auf das Kontrollkästchen **Nur abhängige Objekte anzeigen, die nicht ausgewählt sind**.
5. Wählen Sie in der Dropdownliste **Abhängige Objekte auswählen** die Optionen zum Hinzufügen der gruppierten abhängigen Objekte zum Auftrag. Die abhängigen Objekte werden nicht standardmäßig ausgewählt; Sie müssen die hochzustufenden abhängigen Objekte explizit auswählen.

   Wenn Sie **Alle Universen** aus der Dropdownliste **Abhängige Objekte auswählen** auswählen, werden alle Universen, die in der Liste mit den abhängigen Objekten angezeigt werden, ausgewählt. Sie können die abhängigen Objekte auch einzeln auswählen.

   Sie können auf **Typ** klicken, um die unterstützten Filteroptionen für die InfoObjects anzuzeigen. Eine Dropdown-Liste wird angezeigt. Die Liste zeigt die unterstützten Filteroptionen an. Wählen Sie die Filteroption, und klicken Sie auf **OK**. Die gefilterten InfoObjects werden angezeigt.

   Wenn Sie die abhängigen Objekte in der Spalte **Abhängige Objekte** auswählen und auf **Änderungen anwenden** klicken, werden die abhängigen Objekte automatisch in die Spalte **Objekte im Auftrag** verschoben.

   Sie können den Namen des abhängigen Objekts auch in das Feld **Abhängige Objekte durchsuchen** eingeben, um ein abhängiges Objekt zu suchen.

   Weitere Informationen über die Suche nach abhängigen Objekten finden Sie unter *Suchen nach abhängigen Objekten* [Seite 541].
6. Klicken Sie auf **Änderungen anwenden** , um die Liste der abhängigen Objekte zu aktualisieren und anschließend auf **Anwenden & Schließen**, um die Änderungen zu speichern.

Die abhängigen Objekte werden automatisch vom Tool berechnet. Sie werden entweder basierend auf den InfoObject-Beziehungen oder den InfoObject-Eigenschaften berechnet. Abhängige Objekte, die nicht einer dieser beiden Kategorien zuzuordnen sind, werden in dieser Version des Tools nicht berechnet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Wenn Sie einen Ordner zum Hochstufen auswählen, wird der Inhalt des ausgewählten Ordners als Primärressource betrachtet.

Weitere Informationen

Hochstufen von Aufträgen mit nicht verbundenen Repositorys [Seite 541]

15.3.8 Suchen nach abhängigen Objekten

Mit der erweiterten Suchfunktion in der Hochstufverwaltung können Sie die von InfoObjects abhängigen Objekte im Repository suchen.

Zum Suchen der abhängigen Objekte eines InfoObjects führen sie folgende Schritte aus:

1. Starten Sie die Hochstufverwaltung.
2. Erstellen Sie einen neuen Auftrag oder bearbeiten Sie einen vorhandenen Auftrag.

   Wenn Sie den neuen Auftrag erstellt haben, fügen Sie InfoObjects zu dem Auftrag hinzu. Wenn Sie einen vorhandenen Auftrag bearbeiten, können Sie bei Bedarf Objekte hinzufügen.
3. Klicken Sie auf **Abhängigkeiten verwalten**.
4. Geben Sie im Feld **Abhängige Objekte suchen** den Namen des zu suchenden abhängigen Objekts ein.
5. Klicken Sie auf das Symbol "Suchen".

Weitere Informationen

Verwalten der Abhängigkeiten eines Auftrags [Seite 540]

15.3.9 Hochstufen von Aufträgen mit nicht verbundenen Repositorys

In diesem Abschnitt wird die Hochstufung von Aufträgen vom Quellsystem in das Zielsystem beschrieben, wenn beide Systeme live sind.

Die folgende Tabelle enthält die InfoObject-Typen, die mithilfe der Hochstufverwaltung hochgestuft werden können:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Kategorie	Objekttypen, die hochgestuft werden können
Berichte	Crystal-Reports-Berichte, Web Intelligence, Dashboards, QaaWS, Explorer
Drittanbieter-Objekte	RTF, Textdokument, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Flash, Adobe Acrobat
Benutzer	Benutzer und Benutzergruppen
Server	Servergruppen
BI-Plattform	Ordner, Programm, Ereignisse, Profile, Objektpaket, Hyperlink, Kategorien, Posteingangsdokument, persönlicher Ordner und Favoritenordner
Universum, Arbeitsbereich	Universen UNV, Verbindungen
EPM-Dashboard	Universen, Verbindungen, Berichte, Dashboard und Analysen
BusinessView	DataFoundation
Föderation • Replikationsliste • Replikationsaufträge	Die Replikationsliste stuft folgende Objekte hoch: Flash, .txt, Diskussionen, Dashboards, .pdf, Hyperlink, .xls, Objektpaket, Crystal-Reports-Berichte, Web-Intelligence-Dokumente, Universen, Programm, Verbindungen, DataFoundation, Business Views, .rtf, Profil, Ereignis, Benutzer und Benutzergruppen. Durch Replikationsverbindungen werden Replikationsaufträge, Remoteverbindung, Veröffentlichungen, Diskussion, Pioneer-Verbindung hochgestuft.
BI-Dienste	Web Intelligence-Dokumente, Universen und Verbindungen
Neue InfoObjects	Crystal-Reports-Berichte (rpt/rptr), Pioneer, Dashboard Design, DSL Universe (UNX), Business Layer (BLX), Connection (CNX), Data Fooundation (DFX), WEBI, Explorer, Data Federator, Data Steward, BI-Arbeitsbereich usw.

Zum Hochstufen eines Auftrags führen Sie die folgenden Schritte aus:

1. Starten Sie die Hochstufverwaltung.
2. Wählen Sie auf der *Hochstufungsaufträge*-Startseite den hochzustufenden Auftrag aus.
   Sie können auch mit der rechten Maustaste auf der Startseite auf **Hochstufen** klicken.
3. Wählen Sie bei Bedarf in der Systemliste **Ziel** ein anderes Zielsystem aus.

   Hinweis

   Stellen Sie sicher, dass Sie sowohl beim Quell- als auch beim Zielsystem angemeldet sind, bevor Sie mit dem Hochstufungsprozess fortfahren.

4. Geben Sie im Feld **Änderungsverwaltungs-ID** den entsprechenden Wert ein, und klicken Sie auf **Speichern**.

   Hinweis

   Die Change Management-ID wird zum Abrufen von Informationen zu Protokollierung, Auditing, Auftragsverlauf verwendet. Das Hochstufverwaltungstool ermöglicht das Zuordnen der einzelnen Instanzen der Auftragserstellung zu einer Change Management-ID. Die Change Management-ID ist ein

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Attribut, das der Benutzer beim Anlegen eines neuen Auftrags in der Auftragsdefinition festlegt. Das Tool generiert für jeden Auftrag automatisch eine ID.

5. Klicken Sie auf **Sicherheitseinstellungen**, falls erforderlich. Folgende Optionen werden angezeigt:
   - **Sicherheit nicht hochstufen** – Dies ist die Standardoption.
   - **Sicherheit hochstufen** – Verwenden Sie diese Option, um Aufträge mit den zugehörigen Sicherheitsrechten hochzustufen.
   - **Objektsicherheit hochstufen** – Verwenden Sie diese Option, um die Sicherheit von Objekten und Ordnern hochzustufen
   - **Benutzersicherheit hochstufen** – Ermöglicht die Hochstufung der Rechte der zu einem Auftrag gehörenden Benutzer
   - **Anwendungsrechte einschließen** - Diese Option steht nur zur Auswahl, wenn die Option **Benutzersicherheit hochstufen** aktiviert ist. Wenn die Objekte in dem Auftrag Anwendungsrechte übernehmen, wird der Auftrag mit diesen Rechten hochgestuft.

   Sie können auch auf **Sicherheit anzeigen** klicken, um die Sicherheitsabhängigkeiten der InfoObjects im Auftrag anzuzeigen.
6. Klicken Sie auf **Probeweise hochstufen**, um sicherzustellen, dass kein Konflikt zwischen CUIDs von InfoObjects im Quell- und Zielsystem besteht. Die Hochstufungsdetails werden in den Registerkarten **Erfolg**, **Fehler** und **Warnung** angezeigt. In der ersten Spalte werden die hochzustufenden Objekte, in der zweiten Spalte wird der Hochstufungsstatus der InfoObjects angezeigt. Die Hochstufverwaltung klassifiziert die ausgewählten Objekte in Benutzer, Gruppen und Universen.

   > **Hinweis**
   >
   > Mit dieser Option werden keine InfoObjects zur Hochstufung übergeben.

   Die Probehochstufung kann zu einem der folgenden Ergebnisse führen:
   - `Überschrieben` – Das InfoObject im Zielsystem wird vom InfoObject im Quellsystem überschrieben.
   - `Kopiert` – Das InfoObject im Quellsystem wird in das Zielsystem kopiert.
   - `Verworfen` – Das InfoObject wird nicht vom Quellsystem in das Zielsystem hochgestuft.
   - `Warnung` – Das InfoObject im Zielsystem ist die neuere Version. Sie können das InfoObject aus dem Auftrag entfernen. Wenn Sie das InfoObject jedoch hochstufen möchten, wird es hochgestuft.
   - `Zugeordnet` – Das InfoObject ist einem InfoObject im Zielsystem zugeordnet.
7. Klicken Sie auf **Zeitgesteuerte Verarbeitung**, wenn die Hochstufung zu einem bestimmten Zeitpunkt oder regelmäßig ausgeführt werden soll.
8. Klicken Sie auf **Hochstufen**.
   Der ausgewählte Auftrag wird hochgestuft.

Wenn Sie den Auftrag nicht hochstufen möchten, klicken Sie auf **Speichern**, um Änderungen wie Sicherheit, Change Management-ID und Einstellungen für die zeitgesteuerte Verarbeitung zu speichern.

15.3.10 Hochstufen eines Auftrags mithilfe einer LCMBIAR-Datei

Hochstufen bezeichnet einen Vorgang, bei dem eine BI-Ressource von einem Repository in ein anderes übertragen wird. Wenn sich Quell- und Zielsystem im gleichen Netzwerk befinden, wird das InfoObject von der

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Hochstufverwaltung über WAN oder LAN hochgestuft. Mit der Hochstufverwaltung können Sie jedoch auch InfoObjects hochstufen, wenn sich Quell- und Zielsystem nicht im gleichen Netzwerk befinden.

In Szenarios, in denen sich Quell- und Zielsystem nicht im gleichen Netzwerk befinden, ermöglicht die Hochstufverwaltung das Hochstufen von Aufträgen in das Zielsystem durch Export des Auftrags in das Quellsystem in eine LCMBIAR-Datei und anschließenden Import des Auftrags aus der BIAR-Datei in das Zielsystem.

In diesem Abschnitt wird der Export eines Auftrags in eine LCMBIAR-Datei und der anschließende Import aus der BIAR-Datei in das Zielsystem beschrieben.

> **Hinweis**
>
> Sie können keine LCMBIAR-Dateien verwenden, die mithilfe des Import-Assistenten erstellt wurden.

Weitere Informationen

Exportieren eines Auftrags in eine LCMBIAR-Datei [Seite 544]
Importieren eines Auftrags in eine LCMBIAR-Datei [Seite 545]

15.3.10.1 Exportieren eines Auftrags in eine LCMBIAR-Datei

In diesem Abschnitt wird der Export eines Auftrags in eine LCMBIAR-Datei beschrieben.

Zum Exportieren eines Auftrags in eine LCMBIAR-Datei führen Sie folgende Schritte aus:

1. Starten Sie die Hochstufverwaltung, und erstellen Sie einen neuen Auftrag.

   Weitere Informationen über das Erstellen neuer Aufträge finden Sie unter *Einen Auftrag erstellen* [Seite 534]
2. Wählen Sie in der Dropdownliste **Ziel** die Option **Ausgabe in LCMBIAR-Datei**, und klicken Sie auf **Erstellen**.
3. Klicken Sie auf **Objekte hinzufügen**, um InfoObjects zum Auftrag hinzuzufügen.

   Mit der Option **Abhängigkeiten verwalten** können Sie die abhängigen Objekte des ausgewählten Auftrags verwalten.
4. Aktivieren Sie zur Verschlüsselung der LCMBIAR-Datei mittels Kennwort das Kontrollkästchen **Kennwortverschlüsselung**.
5. Geben Sie im Feld **Kennwort** ein Kennwort ein.
6. Geben Sie das Kennwort im Feld **Kennwort bestätigen** erneut ein.
7. Klicken Sie auf **Hochstufen**.
   Das Fenster *Hochstufen* wird angezeigt.
8. Bearbeiten Sie gegebenenfalls die Sicherheitsoptionen, und wählen Sie dann **Exportieren**.
   Die LCMBIAR-Datei wird erstellt. Die LCMBIAR-Datei kann im Dateisystem gespeichert werden.
9. (Optional) Klicken Sie auf **LCMBIAR-Dateiziel**, und wählen Sie **FTP**, um die LCMBIAR-Datei auf einen FTP-Server zu exportieren. Geben Sie Hostnamen, Port, Benutzernamen, Kennwort, Verzeichnis und Dateinamen ein, und wählen Sie dann **Exportieren**.
10. Wählen Sie in der Dropdownliste **Ziel** die Option **Ausgabe in LCMBIAR-Datei**, und klicken Sie auf **LCMBIAR-Dateiziel**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Sie können den Export eines Auftrags in eine LCMBIAR-Datei zeitsteuern. Weitere Informationen hierzu finden Sie im Abschnitt *Zeitsteuern von Auftragshochstufungen* [Seite 546].

Weitere Informationen

Hinzufügen eines InfoObjects zu einem Auftrag [Seite 539]
Verwalten der Abhängigkeiten eines Auftrags [Seite 540]

15.3.10.2 Importieren eines Auftrags in eine LCMBIAR-Datei

Sie können Aufträge aus einer LCMBIAR-Datei importieren. Die LCMBIAR-Datei wird vom Speichermedium in das Zielsystem kopiert.

> **Hinweis**
>
> Aufträge können auch aus einer mit dem Upgrade-Management-Tool erstellten BIAR-Datei importiert werden.

Zum Importieren einer LCMBIAR-Datei führen Sie die folgenden Schritte aus:

1. Starten Sie die Hochstufverwaltung.
2. Klicken Sie auf der *Hochstufungsaufträge*-Startseite auf **Importieren** > **Datei importieren**.
   Das Fenster *Aus Datei importieren* wird angezeigt.
3. BIAR-Dateien können aus dem Dateisystem oder von einem FTP-Server importiert werden.
   - Um eine BIAR-Datei aus dem Dateisystem zu importieren, führen Sie folgende Schritte durch:
     1. Wählen Sie **Dateisystem**.
     2. Klicken Sie auf **Durchsuchen**, und wählen Sie eine LCMBIAR-Datei aus dem Dateisystem aus.
     3. Geben Sie im Feld **Kennwort** das Kennwort der LCMBIAR-Datei ein.

        > **Hinweis**
        >
        > Das Kennwortfeld wird nur angezeigt, wenn die LCMBIAR-Datei mit einem Kennwort verschlüsselt ist.

     4. Klicken Sie auf **Erstellen**. Der Auftrag wird erstellt.

        > **Hinweis**
        >
        > Falls ein Auftrag mit diesem Namen vorhanden ist, wird das Popup-Fenster "Speichern bestätigen" angezeigt. Klicken Sie auf "Ja", um den vorhandenen Auftrag zu überschreiben. Klicken Sie auf "Nein", um einen Auftrag mit dem Namen `jobname_copy<CURRENT_DATE_AND_TIME>` zu erstellen.

   - Zum Importieren einer LCMBIAR-Datei von einem FTP-Server führen Sie die folgenden Schritte aus:
     1. Wählen Sie **FTP**

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Geben Sie die entsprechenden Informationen in die Felder "Host", "Port", "Benutzername", "Kennwort", "Verzeichnis" und "Dateiname" ein und klicken auf **OK**.

> **Hinweis**
>
> Es können nur LCMBIAR-Dateien importiert bzw. mit dem Upgrade-Management-Tool erstellte BIAR-Dateien aktualisiert werden.

4. Klicken Sie auf **Hochstufen**.
   Das Fenster *Hochstufen – Auftragsname* wird angezeigt.
5. Wählen Sie aus der Dropdownliste **Ziel** das Zielsystem aus. Wenn Sie **Bei einem neuen CMS anmelden** auswählen, werden Sie zur Eingabe von Anmeldedaten aufgefordert. Bestätigen Sie die Anmeldedaten des Zielsystems.
6. Klicken Sie auf **Hochstufen**, um den Inhalt des Zielsystems hochzustufen.

   Sie können auch auf die Option **Probeweise hochstufen** klicken, um die hochzustufenden Objekte und den Hochstufungsstatus anzuzeigen.

Weitere Informationen

Verwalten der Abhängigkeiten eines Auftrags [Seite 540]

15.3.11 Zeitsteuern von Auftragshochstufungen

In diesem Abschnitt wird die zeitgesteuerte Verarbeitung der Hochstufung eines Auftrags beschrieben. Außerdem wird die Eingabe von Wiederholungsoptionen und Parametern erläutert.

Zum Festlegen der zeitgesteuerten Verarbeitung einer Auftragsinstanz führen Sie folgende Schritte aus:

1. Klicken Sie im Dialogfeld *Hochstufen* auf die Option **Zeitgesteuert verarbeiten**.
2. Legen Sie die gewünschte Zeitsteuerungsoption fest und klicken auf **Zeitgesteuert verarbeiten**.

Wenn Sie einem in einem Auftrag enthaltenen Ordner InfoObjects hinzufügen, nachdem der Auftrag zur Hochstufung eingeplant wurde, werden die InfoObjects zum geplanten Zeitpunkt auch in das Ziel hochgestuft.

> **Tipp**
>
> Nach Abschluss der Hochstufung eines Auftrags können Sie alle Instanzen des Auftrags anzeigen, indem Sie den Auftrag auf der Seite *Hochstufungsaufträge* auswählen und in der Symbolleiste auf **Verlauf** klicken.

Die Hochstufung eines Auftrags kann auch auf Basis eines auslösenden Ereignisses erfolgen.

Sie können E-Mail-Benachrichtigungen basierend auf dem Hochstufungsstatus (wie z.B. Erfolg/Teilerfolg/Fehlgeschlagen) auswählen. Detaillierte Informationen zu den verschiedenen Zeitsteuerungsoptionen und der Konfiguration von Benachrichtigungen finden Sie im Abschnitt "Zeitsteuerung".

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Exportieren eines Auftrags in eine LCMBIAR-Datei [Seite 544]

15.3.11.1 Aktualisieren von wiederkehrenden und ausstehenden Auftragshochstufungsinstanzen

Mithilfe der Hochstufverwaltung können Sie den Status von Hochstufungsauftragsinstanzen verfolgen und diese gegebenenfalls über die Option **Wiederkehrende und ausstehende Instanzen** zeitgesteuert verarbeiten.

Um den Status von Auftragshochstufungsinstanzen zu verfolgen und diese zeitgesteuert zu verarbeiten, führen Sie folgende Schritte aus:

1. Starten Sie die Hochstufverwaltung.
2. Wählen Sie auf der *Hochstufungsaufträge*-Startseite einen Auftrag aus.
3. Klicken Sie auf **Verlauf**.
   Das Fenster *Auftragsverlauf* wird angezeigt.
4. Klicken Sie auf **Wiederkehrende und ausstehende Instanzen**.
   Das Fenster *Auftragsverlauf für wiederkehrende und ausstehende Instanzen* wird angezeigt. In diesem Fenster wird die Liste der wiederkehrenden und ausstehenden Hochstufungsauftragsinstanzen angezeigt.

   Sie können bei Bedarf folgende Optionen verwenden:

   - Klicken Sie auf **Hochgestufte Instanzen**, um die Liste der hochgestuften Auftragsinstanzen anzuzeigen.
   - Wählen Sie **Anhalten**, um die ausgewählte ausstehende bzw. wiederkehrende Instanz anzuhalten.
   - Klicken Sie auf **Fortsetzen**, um die angehaltene zeitgesteuerte Verarbeitung der Hochstufungsauftragsinstanz fortzusetzen.
   - Klicken Sie auf **Erneut zeitgesteuert verarbeiten**, um die ausgewählte Hochstufungsauftragsinstanz erneut zeitgesteuert zu verarbeiten.
   - Klicken Sie auf , um die zeitgesteuerte Verarbeitung einer Hochstufungsauftragsinstanz zu löschen.
   - Klicken Sie auf , um den Status einer zeitgesteuerten Hochstufungsauftragsinstanz zu regenerieren.
   - Mit dieser Option können Sie von einer Seite zur nächsten Seite oder zu einer bestimmten Seite durch Eingabe der Seitennummer wechseln.

> **Hinweis**
>
> Die Statusspalte im Fenster *Auftragsverlauf für wiederkehrende und ausstehende Instanzen* zeigt den Status der Hochstufungsauftragsinstanz, z.B. wiederkehrend, ausstehend, an.

Weitere Informationen

Rollback für Aufträge ausführen [Seite 548]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15.3.12 Anzeigen des Auftragsverlaufs

In diesem Abschnitt wird die Anzeige des Verlaufs eines Auftrags beschrieben.

> **Hinweis**
>
> Zum Anzeigen des Verlaufs eines Auftrags müssen Sie sicherstellen, dass der Auftrag einen der folgenden Status aufweist:
>
> - Erfolg
> - Fehler
> - Teilerfolg

Zum Anzeigen des Verlaufs eines Auftrags führen Sie die folgenden Schritte aus:

1. Starten Sie die Hochstufverwaltung.
   Die *Hochstufungsaufträge*-Startseite wird angezeigt.
2. Wählen Sie den Auftrag auf, für den Sie den Verlauf anzeigen möchten, und klicken Sie auf die Registerkarte **Verlauf**.

   Die Auftragsinstanzenzeit, der Auftragsname, der Name des Quell- und Zielsystems, die ID des Benutzers, der den Auftrag hochgestuft hat, und der Status (Erfolg, Fehler oder Teilerfolg) des Auftrags werden angezeigt.

   Sie können den detaillierten Status des Auftrags anzeigen, indem Sie auf die in der Spalte **Status** angezeigte Verknüpfung klicken.

15.3.13 Rollback für Aufträge ausführen

Mit der Option "Rollback" können Sie das Zielsystem nach der Hochstufung eines Auftrags wieder in seinen vorherigen Status zurückversetzen.

Zum Durchführen eines Rollbacks für einen Auftrag führen Sie die folgenden Schritte aus:

1. Starten Sie die Hochstufverwaltung.
   Die *Hochstufungsaufträge*-Startseite wird angezeigt.
2. Folgende Vorgänge können ausgeführt werden:
   - Klicken Sie mit der rechten Maustaste auf den Auftrag, für den ein Rollback ausgeführt werden soll, und wählen Sie **Rollback**.
   - Wählen Sie den Auftrag aus, für den ein Rollback ausgeführt werden soll, und klicken Sie auf die Registerkarte **Rollback**.

   Das Fenster *Rollback* wird angezeigt.
3. Wählen Sie die Instanz aus, für die ein Rollback ausgeführt werden soll, und klicken Sie auf **Vollständiges Rollback**.
   Das Rollback für die Instanz wird durchgeführt.

Rollbacks können nur für die neueste Instanz eines Hochstufungsauftrgas durchgeführt werden. Rollbacks können nicht für mehrere Auftragsinstanzen gleichzeitig durchgeführt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15.3.13.1 Verwenden der Option "Teilrollback"

Mit der Hochstufverwaltung können Sie entweder ein Teilrollback oder ein vollständiges Rollback für InfoObjects in einem Auftrag vom Zielsystem durchführen.

Zum Durchführen eines Teilrollbacks für InfoObjects führen Sie folgende Schritte aus:

1. Starten Sie die Hochstufverwaltung.
   Die *Hochstufungsaufträge*-Startseite wird angezeigt.
2. Folgende Vorgänge können ausgeführt werden:
   - Klicken Sie mit der rechten Maustaste auf den Auftrag, für den ein Rollback ausgeführt werden soll, und wählen Sie **Rollback** aus.
   - Wählen Sie den Auftrag aus, für den ein Rollback ausgeführt werden soll, und klicken Sie auf die Registerkarte **Rollback**.

   Das Fenster *Rollback* wird angezeigt.
3. Wählen Sie die Instanz aus der Liste aus, und klicken Sie auf **Teilrollback**.

   Die Liste der InfoObjects in dem ausgewählten Auftrag wird auf der Seite *Job Viewer* angezeigt.
4. Wählen Sie die InfoObjects, für die ein Rollback ausgeführt werden soll, und klicken Sie auf **Rollback**.

> **Hinweis**
>
> Sie müssen sicherstellen, dass Sie ein Rollback für alle InfoObjects in einer Instanz durchgeführt haben, bevor Sie ein Rollback für die InfoObjects in der nächsten Instanz durchführen.

> **Achtung**
>
> Wenn ein Auftrag mit Sicherheit hochgestuft wird, wird während des Teilrollbacks für InfoObjects möglicherweise kein Rollback für die Sicherheit der ausgewählten abhängigen InfoObjects in ihren früheren Status durchgeführt.

Weitere Informationen

Verwalten mehrerer Versionen von BI-Ressourcen [Seite 580]

15.3.13.2 Rollback von Aufträgen nach Ablauf des Kennworts ausführen

In diesem Abschnitt wird das Ausführen eines Rollbacks für einen Auftrag nach Ablauf des bei dessen Hochstufung verwendeten Kennworts beschrieben.

Zum Ausführen eines Rollbacks für einen Auftrag nach Ablauf des Kennworts führen Sie folgende Schritte aus:

1. Wählen Sie einen Auftrag, für den ein Rollback ausgeführt werden soll, und klicken Sie auf **Rollback**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Wählen Sie im Fenster *Rollback* die Option **Vollständiges Rollback**.

   Es wird eine Fehlermeldung angezeigt. Die Meldung besagt, dass für den Auftrag kein Rollback ausgeführt werden kann. Außerdem werden Sie aufgefordert, sich beim Quell- oder Zielsystem anzumelden.
3. Geben Sie die Anmeldedaten ein, und klicken Sie auf **Anmelden**.

Es wird ein Dialogfeld angezeigt, das anzeigt, dass der Rollbackprozess abgeschlossen ist.

> **Hinweis**
>
> Die Aufträge, die unter Verwendung der Anmeldedaten des Quell- oder Zielsystems hochgestuft wurden, werden automatisch aktualisiert.

Weitere Informationen

Teilrollback von InfoObjects nach Ablauf des Kennworts [Seite 550]
Verwenden der Option "Teilrollback" [Seite 549]

15.3.13.2.1 Teilrollback von InfoObjects nach Ablauf des Kennworts

In diesem Abschnitt wird die Durchführung von Teilrollbacks für InfoObjects nach Ablauf des Kennworts für das Quell- oder Zielsystem beschrieben.

Zum Ausführen eines Teilrollbacks für InfoObjects nach Ablauf des Kennworts führen Sie folgende Schritte aus:

1. Wählen Sie einen Auftrag, für den ein Rollback ausgeführt werden soll, und klicken Sie auf **Rollback**.

   Das Fenster *Rollback* wird angezeigt.
2. Wählen Sie die Option **Teilrollback**.

   Es wird eine Fehlermeldung angezeigt. Die Meldung besagt, dass für die InfoObjects kein Rollback ausgeführt werden kann. Außerdem werden Sie aufgefordert, sich beim Quell- oder Zielsystem anzumelden.
3. Geben Sie die Anmeldedaten ein, und klicken Sie auf **Anmelden**.

   Die Seite *Job Viewer* wird angezeigt. Auf dieser Seite wird die Liste der InfoObjects angezeigt.
4. Wählen Sie die erforderlichen InfoObjects, und klicken Sie auf **Rollback**.

> **Hinweis**
>
> Die Aufträge, die unter Verwendung der Anmeldedaten des Quell- oder Zielsystems hochgestuft wurden, werden automatisch aktualisiert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Rollback für Aufträge ausführen [Seite 548]
Verwenden der Option "Teilrollback" [Seite 549]
Rollback von Aufträgen nach Ablauf des Kennworts ausführen [Seite 549]

15.4 Verwalten unterschiedlicher Versionen eines InfoObjects

Mit der Versionsverwaltung können Sie Versionen von BI-Ressourcen verwalten, die sich im Repository der BI-Plattform befinden. Er unterstützt die beiden Versionsverwaltungssysteme "Subversion" und "ClearCase". In diesem Abschnitt wird die Verwendung der Versionsverwaltungsfunktion in der Hochstufverwaltung beschrieben.

Zum Erstellen und Verwalten verschiedener Versionen eines InfoObjects führen Sie folgende Schritte aus:

1. Starten Sie die Hochstufverwaltung.
2. Klicken Sie mit der rechten Maustaste auf einen Auftrag, wählen Sie **VMS-Aktionen**, und wählen Sie dann **Zu VM hinzufügen**. (Sie können alternativ auch auf der Registerkarte **VMS-Aktionen** die Option **Zu VM hinzufügen** wählen.)

   > **Hinweis**
   >
   > Durch Klicken auf **Zu VM hinzufügen** wird eine Basisversion des Objekts im VMS-Repository erstellt. Die Basisversion wird zum anschließenden Einchecken benötigt.

3. Klicken Sie auf **Einchecken**, um das Dokument im VMS-Repository zu aktualisieren.
   Das Dialogfeld *Eincheck-Kommentare* wird angezeigt.
4. Geben Sie Ihre Kommentare ein, und klicken Sie auf **OK**.
   Die geänderte Versionsnummer des ausgewählten InfoObjects wird in den Spalten "VMS-Version" und "CMS-Version" angezeigt.
5. Zum Abrufen der aktuellen Version des Dokuments vom VMS wählen Sie das betreffende InfoObject, und klicken Sie auf **Aktuelle Version abrufen**.
6. Zum Erstellen einer Kopie der aktuellen Version klicken Sie auf **Kopie erstellen**.
   Eine Kopie der ausgewählten Version wird erstellt.
7. Wählen Sie **Verlauf**, um alle für die ausgewählte Ressource verfügbaren Versionen anzuzeigen.
   Das Fenster *Verlauf* wird angezeigt. Folgende Optionen werden angezeigt:
   - **Version abrufen** – Falls mehrere Versionen vorhanden sind und Sie eine bestimmte Version der BI-Ressource benötigen, können Sie die benötigte Ressource auswählen und auf **Version abrufen** klicken.
   - **Kopie von Version abrufen** – Mit dieser Option können Sie eine Kopie der ausgewählten Version abrufen.
   - **Kopie von Version exportieren** – Mit dieser Option können Sie eine Kopie der ausgewählten Version abrufen und in Ihrem lokalen System speichern.

15.4.1 Anwendungszugriffsrechte für die Versionsverwaltung

In diesem Abschnitt werden die Anwendungszugriffsrechte für die Versionsverwaltung beschrieben.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Zugriffsrechte für die Versionsverwaltung lassen sich in der CMC festlegen.
- Sie können genau abgestimmte Anwendungsrechte für verschiedene Funktionen innerhalb der Versionsverwaltung einstellen.

Um bestimmte Rechte für die Versionsverwaltung festzulegen, führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei der CMC an, und wählen Sie **Anwendungen**.
2. Doppelklicken Sie auf **Versionsverwaltung**.
3. Klicken Sie auf **Benutzersicherheit**, und wählen Sie einen Benutzer aus. Sie können Sicherheitsrechte für den ausgewählten Benutzer anzeigen oder zuweisen.
4. Folgende Rechte stehen nun speziell für die Versionsverwaltung zur Verfügung:
   - "Einchecken" zulassen
   - "Kopie erstellen" zulassen
   - Löschen der Revision zulassen
   - Abrufen der Revision zulassen
   - "Sperren" und "Sperrung aufheben" zulassen
   - BOMM-Objekte anzeigen und versionieren
   - Business Views anzeigen und versionieren
   - Kalender anzeigen und versionieren
   - Verbindungen anzeigen und versionieren
   - Profile anzeigen und versionieren
   - QaaWS anzeigen und versionieren
   - Berichtsobjekte anzeigen und versionieren
   - Sicherheitsobjekte anzeigen und versionieren
   - Universen anzeigen und versionieren
   - Gelöschte Ressourcen anzeigen
5. Wenn Sie einem ausgewählten Benutzer Rechte zuweisen möchten, wählen Sie das entsprechende Recht aus und klicken auf **Sicherheit zuweisen**.

15.4.2 Sichern und Wiederherstellen von Subversion-Dateien

In diesem Abschnitt werden vorgeschlagene Prozeduren für die Sicherung und Wiederherstellung von Subversion-Dateien beschrieben. Der Sicherungs- und Wiederherstellungsplan umfasst Vorsichtsmaßnahmen, die im Fall eines Systemsfehlers aufgrund einer Naturkatastrophe oder eines Katastrophenereignisses ergriffen werden sollen.

15.4.2.1 Sichern von Subversion-Dateien

Führen Sie zum Sichern der Subversion-Dateien folgende Schritte aus:

1. Unter Windows, navigieren Sie zu `<INSTALLDIR>\SAP BusinessObjects Enterprise 4.0\CheckOut` oder unter Unix, navigieren Sie zu `<INSTALLDIR>/sap_bobj/enterprise_40/Subversion/CheckOut`
2. Kopieren Sie den Ordner `CheckOut`, und speichern Sie ihn auf einem beliebigen Sicherungsgerät.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Kopieren Sie das gesamte `<LCM_Repository>`, und speichern Sie es auf einem beliebigen Sicherungsgerät.

15.4.2.2 Wiederherstellen von Subversion-Dateien

Führen Sie zum Wiederherstellen der Subversion-Dateien folgende Schritte aus:

1. Stellen Sie den Ordner "CheckOut" aus dem Speicherort wieder her, in dem er zuvor gesichert wurde.

   > **Hinweis**
   >
   > Klicken Sie in der CMC auf **Anwendungen** > **Versionsverwaltung** > **VMS-Einstellungen**, und stellen Sie sicher, dass im Feld **Arbeitsbereichsverzeichnis** der richtige Pfad zum Auschecken eingegeben wurde.

2. Stellen Sie das LCM_Repository aus dem Speicherort wieder her, in dem es zuvor gesichert wurde.

   > **Hinweis**
   >
   > Klicken Sie in der CMC auf **Anwendungen** > **Versionsverwaltung** > **VMS-Einstellungen**, und stellen Sie sicher, dass im Feld **Installationspfad** der richtige Pfad zum Auschecken eingegeben wurde.

15.5 Hochstufen des vollständigen Repository-Inhalts mithilfe der Hochstufverwaltung

Das Hochstufen der Inhalte eines Repositorys erfordert Planung, Vorbereitung und ausreichend Zeit. In diesem Abschnitt werden die Schritte für eine erfolgreiche Hochstufung von Inhalten aus einer Bereitstellung in eine andere beschrieben.

15.5.1 Vorbereiten der Quell- und Zielsysteme

Die Quell- und Zielsysteme müssen unbedingt optimal konfiguriert sein, bevor Sie Inhalte hochstufen.

1. Im Quellsystem:
   a) Scannen Sie das Quellsystem mithilfe des Repository Diagnostic Tools (RDT), und korrigieren Sie jegliche Inkonsistenzen im Repository oder FRS. Weitere Informationen zum RDT finden Sie im *Benutzerhandbuch für das Repository Diagnostic Tool der Business Intelligence-Plattform*.
   b) Minimieren Sie die Nutzung des Quellsystems, um Änderungen während des Hochstufens weitestgehend zu vermeiden. Systemaktivität kann Objektfehler nach sich ziehen.

      > **Hinweis**
      >
      > Sollten Fehler auftreten, überprüfen Sie den Jobstatus, und beheben Sie jegliche Probleme.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Im Zielsystem:
   a) Verwenden Sie den Lizenzschlüsselcode, um sicherzustellen, dass die richtige, ausreichende Lizenz im Zielsystem eingerichtet ist.

      Hinweis

      Um Fehler beim Hochstufen von Inhalten aufgrund einer unzureichenden Lizenz zu vermeiden, verwenden Sie die gleiche Lizenz in beiden Systemen.

   b) Wenn Sie Drittherstellerauthentifizierung nutzen, muss dies vor dem Hochstufen von Inhalten entsprechend im Zielsystem konfiguriert und aktiviert werden.

      Hinweis

      Nehmen Sie keine Benutzer- oder Benutzergruppenzuordnungen vor. Dies würde zum Anlegen von Benutzern oder Benutzergruppen mit unterschiedlichen CUIDs im Zielsystem führen. Beim Hochstufen werden Objekte anhand ihrer CUID identifiziert und zwischen Quell- und Zielsystem zugeordnet. Das Zuordnen von Benutzern und Benutzergruppen führt zu Fehlzuordnungen von Inhalten, was das Fehlschlagen des Hochstufungsprozesses nach sich zieht.

   c) Stellen Sie sicher, dass alle im Quellsystem erforderlichen Addons auch im Zielsystem installiert sind.

      Hinweis

      Um eine erfolgreiche Migration zu gewährleisten, müssen Sie im Quellsystem Addons wie Analysis oder Design Studio installieren.

   d) Wenn die Inhalte QaaWS-Verbindungen nutzen, müssen Überschreibungen aktiviert sein, um sicherzustellen, dass diese Verbindungen auf die richtigen Webdienste verweisen. Informationen zum Einrichten von Überschreibungen finden Sie im Abschnitt “Überschreibungen”.
   e) Müssen alle abgeschlossenen zeitgesteuerten Instanzen migriert werden, müssen Sie in den **Auftragseinstellungen** der Hochstufverwaltung auf **Abgeschlossene Instanzen auf der Seite "Abhängigkeiten verwalten" anzeigen** klicken.
3. Im zentralen System:
   a) Sie können das Quellsystem, das Zielsystem oder ein anderes System als zentrales System einrichten, in dem Aufträge der Hochstufverwaltung ausgeführt werden. Beim Hochstufen eines vollen Repositorys wird eine große Menge an Inhalten verarbeitet; hierzu werden im zentralen System zusätzliche Systemressourcen benötigt. Verwenden Sie folgende Größenrichtwerte, um das zentrale System für 10.000 Objekte einzurichten:

	Temporäre Speicherplatzzuweisung	Arbeitsspeicherzuweisung	Weitere Konfigurationseinstellungen
`LCM_CLI`	2 GB	2 GB	Aktualisieren Sie die Datei `LCM_CLI.bat` und ändern den Parameter `-Xmx`.
Job Server für Hochstufverwaltung	3 GB	3 GB	Aktualisieren Sie in der CMC die Starteigenschaft des Job Servers der Hochstufverwaltung

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

			durch Hinzufügen des Parameters `-javaargs Xmx3g`.

Beispiel: Der Auftrag umfasst schätzungsweise 50.000 Objekte:

- Weisen Sie `LCM_CLI` (50.000 ÷ 10.000 × 2) 10 GB Arbeitsspeicher zu
- Weisen Sie dem Job Server (50.000 ÷ 10.000 × 3) 15 GB Arbeitsspeicher zu

> **Hinweis**
>
> Diese Richtlinien für Größenordnungen gelten für die meisten Umgebungen. Die Größe der Dokumente kann sich jedoch auf die Ressourcenanforderungen auswirken.

15.5.2 Migrationsstrategien

- Verwenden Sie für alle Auftragshochstufungen die Befehlzeilenschnittstelle (CLI) anstatt der CMC-Webanwendung.
  - Die CLI umgeht die Zeitbeschränkung für Websitzungen auf 20 Minuten, die bei Hochstufaufträgen mit mehr als 1000 Objekten überschritten wird.

    > **Hinweis**
    >
    > Die Objektbeschränkung hängt von ausreichenden Systemressourcen ab.

  - Die CLI ermöglicht eine genaue Kontrolle über die Inhaltshochstufung dank Verwendung einer Abfragesprache zur Auswahl der zu migrierenden Inhalte. Sie können Inhalte des gleichen Typs oder Inhalte im gleichen Verzeichnis auswählen.
  - Die CLI kann in Stapelverarbeitung ausgeführt und Hochstufungsaufträge können mithilfe anderer Scripting-Werkzeuge eingeleitet werden.
- Sorgen Sie für die nötige Sicherheit, indem Sie zuerst die Prinzipale (Benutzer und Benutzergruppen) hochstufen.
  - Indem die Benutzer und Benutzergruppen zuerst hochgestuft werden, bleibt das Sicherheitsmodell im Zielsystem erhalten, was den Erfolg der nachfolgenden Migration der persönlichen Inhalte der Benutzer (z. B. Posteingänge, Favoriten und persönliche Kategorien) sicherstellt.

    > **Hinweis**
    >
    > Es ist wichtig, diesen Schritt zuerst auszuführen, damit die CUIDs der Benutzer und Benutzergruppen im Zielsystem mit denen im Quellsystem übereinstimmen.

- Schalten Sie die Abhängigkeitsberechnung aus.
  - Die Abhängigkeitsberechnung ist eine der arbeitsintensivsten Aufgaben bei der Auftragserstellung. Bei der Migration eines vollständigen Repositorys werden alle Objekte migriert, d. h. eine Berechnung ist nicht erforderlich.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Diese Funktion ist nur hilfreich, wenn unklar ist, welche abhängigen Objekte erforderlich sind.

- Vermeiden Sie die Sicherheitsberechnung nach Möglichkeit.
  - Die Sicherheitsberechnung ist die zweit-arbeitsintensivste Aufgabe bei der Auftragserstellung. Teilen Sie die Hochstufung auf zwei Aufträge auf, wenn Sie viele Dokumente in verschiedenen Verzeichnissen haben und die Sicherheit nur für die Verzeichnisse eingestellt ist. Der erste Auftrag sollte nur Objekte umfassen, für die die Sicherheit aktiviert ist, und der zweite Auftrag sollte nur die Dokumente verarbeiten, für die Sicherheit deaktiviert ist. Auf diese Weise können Sie die Sicherheitsberechnungen nur für die Verzeichnisse ausführen lassen und vermeiden unnötige Berechnungen für alle Dokumente.

    > **Hinweis**
    >
    > Die Objektsicherheit bleibt erhalten, da sie von der Ordnersicherheit geerbt wird.

15.6 Schritte zur vollständigen Systemhochstufung

Die Hochstufung eines gesamten Systems erforder die Ausfphrung von drei getrennten Hochstufungsaufträgen in einer bestimmten Reihenfolge, in denen jeweils bestimmte Inhaltstypen hochgestuft werden. Die folgende Tabelle zeigt eine Übersicht über die Inhaltstypen und Parametereinstellungen für die einzelnen Hochstufungsaufträge.

Hochstufungsauftrag	Inhaltstyp	`exportDependencies`	`includeSecurity`
1	Alle Benutzer und Benutzergruppen	false	true
2	Alle abhängigen Objekte	false	true
3	Alle Primärobjekte	false	true

Nutzen Sie die Befehlszeilenschnittstelle (CLI) zur Erstellung und Ausführung der einzelnen Aufträge. Weitere Informationen zur CLI finden Sie im Abschnitt “Verwenden der Befehlszeilenoption”.

Gemeinsame Parameter

Verwenden Sie folgende Parameter für alle drei Hochstufungsaufträge:

> **Nicht vergessen**
>
> Stellen Sie sicher, dass jeder Parameter in einer eigenen Zeile steht.

```
action=promote
Source_CMS=<SourceSystem>
Source_userName=Administrator
Source_password=<AdministratorPassword>
LCM_CMS=<NameOfCentralSystem>
LCM_userName=Administrator
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
LCM_password=<AdministratorPassword>
Destination_CMS=<TargetSystem>
Destination_userName=Administrator
Destination_password=<AdministratorPassword>
exportDependencies=false
includeSecurity=true
stacktrace=true
consolelog=true
```

15.6.1 Hochstufen von Benutzern und Benutzergruppen (Auftrag 1)

Um identische Sicherheitsmodelle zwischen dem Quell- und dem Zielsystem einzurichten und sicherzustellen, dass die CUIDs der Benutzer- und Benutzergruppenobjekte identisch sind, stufen Sie die Benutzer und die Benutzergruppen zuerst hoch.

1. Erstellen Sie die Datei `usersandgroups.properties` mit den gleichen Parametern, und hängen Sie der Datei folgende Parameter an, um alle Benutzer und Benutzergruppen auszuwählen:

   ```
   exportQuery1=SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID,
   SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
   (SI_KIND='User' OR SI_KIND='UserGroup') AND NOT (SI_ID in (11,12, 501, 1, 2, 3))
   ```

2. Um den Auftrag auszuführen, öffnen Sie das Verzeichnis **<INSTALLDIR>**`\win64x64\scripts`, und führen Sie folgenden Befehl aus:

   ```
   Lcm_cli.bat -lcmproperties=usersandgroups.properties
   ```

15.6.2 Hochstufen abhängiger Objekte (Auftrag 2)

Abhängige Objekte sind abhängig von den Primärobjekten im Public-Ordner und dem Favoriten-Ordner des Benutzers. Um nicht für alle weiteren Aufträge `includeDependencies` auf `true` setzen zu müssen, stufen Sie die abhängigen Objekte im zweiten Schritt hoch. Folgende sind abhängige Objekte:

- Zugriffsberechtigungen
- Anwendungen
- BusinessViews
- Kalender
- Kategorien
- Verbindungen
- Ereignisse
- OLAP-Verbindungen
- Profile
- Projekte
- QaaWS
- Remoteverbindungen
- Replikationslisten

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Servergruppen
- Universen

1. Um alle abhängigen Objekte auszuwählen, erstellen Sie die Datei "dependencies.properties" mit den gemeinsamen Parametern, und hängen Sie der Datei die folgenden Parameter an:

```
#total number of queries (if > 1)
exportQueriesTotal=12
#Projects, Universes, Connections, OLAP Connects: SI_ID=95
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (95)")
#QaaWS: SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'
#-need to ensure Overrides are scanned at the source, promoted to the target and
set to active
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'")
#Events: SI_ID=21
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (21)") and si_specific_kind !
= 'MON.MonitoringEvent'
#Calendars: SI_ID=22
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (22)")
#Categories: SI_ID=45
exportQuery5=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID IN (45)")
#Access Levels: SI_ID=57
exportQuery6=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (57)")
#Server Groups: SI_ID=17
exportQuery7=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (17)")
#Profiles: SI_ID=50
exportQuery8=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (50)")
#Applications: SI_ID=99
exportQuery9=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (99)")
#Remote Connections:  SI_CUID = 'AVwSekNrtFxGqJ6Jp2rLwrI'
exportQuery10=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID = 'AVwSekNrtFxGqJ6Jp2rLwrI'")
#Replication Lists:  SI_CUID = 'ASOr8wap3MJOgdWV5HLcZ1M'
exportQuery11=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='ASOr8wap3MJOgdWV5HLcZ1M'")
#BusinessViews: SI_ID=98
exportQuery12=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (98)")
```

2. Um den Auftrag auszuführen, öffnen Sie das Verzeichnis **<INSTALLDIR>**`\win64x64\scripts`, und führen Sie folgenden Befehl aus:

```
Lcm_cli.bat -lcmproperties=dependencies.properties
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15.6.3 Hochstufen von Primärobjekten (Auftrag 3)

Primärobjekte sind BI-Kerndokumente, die sich im Public-Ordner und im Favoriten-Ordner der Benutzer befinden. Vorausgesetzt, dass der zweite Hochstufungsauftrag bereits ausgeführt wurde, werden die Beziehungen zwischen abhängigen Objekten wiederhergestellt, indem alle abhängigen Objekte migriert und zuletzt alle Primärobjekte hochgestuft werden.

1. Erstellen Sie die Datei `primaryobjects.properties` mit den gleichen Parametern, und hängen Sie der Datei folgende Parameter an, um alle Benutzer und Benutzergruppen auszuwählen:

```
#total number of queries (if > 1)
exportQueriesTotal=4
#All Public Folders
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)")
#All user collaterals (Inbox, FavoriteFolder, PersonalCategory)
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='Inbox')")
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='FavoritesFolder')")
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='PersonalCategory')")
```

2. Um den Auftrag auszuführen, öffnen Sie das Verzeichnis **`<INSTALLDIR>`**`\win64x64\scripts`, und führen Sie folgenden Befehl aus:

```
Lcm_cli.bat -lcmproperties=primaryobjects.properties
```

> **Hinweis**
>
> Wenn der Public-Ordner oder der Favoriten-Ordner der Benutzer über 50.000 Objekte enthält, kann es notwendig sein, diesen abschließenden Auftrag in mehrere kleinere Aufträge aufzuteilen.

> **Hinweis**
>
> Stellen Sie sicher, dass die beiden Rechner, auf denen der Befehlszeilenschnittstellen-Befehl und der Job Server der Hochstufverwaltung ausgeführt werden, den Größenanforderungen entsprechen. Weitere Informationen finden Sie im Abschnitt “Größenanpassung”.

15.6.4 Nach der Hochstufung

Mithilfe der Hochstufverwaltung werden lediglich die Servergruppen hochgestuft, nicht jedoch ihre Server. Um sicherzustellen, dass Berichte mit zugeordneten Servern weiterhin erstellt werden können, müssen die entsprechenden Server erneut angelegt und den richtigen Servergruppen zugeordnet werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15.7 Verwenden der Befehlszeilenoption

Die Befehlszeilenoption der Hochstufverwaltung ermöglicht das Hochstufen von Objekten von einer BI-Plattform-Bereitstellung auf eine andere. Sie können ein Batchskript für mehrere Aufträge erstellen.

> **Tipp**
>
> Nutzen Sie die Befehlszeilenoption für Aufträge, die eine große Anzahl an Objekten enthalten.

Die Hochstufverwaltung unterstützt folgende Auftragshochstufungstypen über die Befehlszeile:

- Exportieren einer vorhandenen Hochstufungsauftragsvorlage nach LCMBIAR mit Kennwortverschlüsselung.
- Exportieren einer vorhandenen Hochstufungsauftragsvorlage nach LCMBIAR ohne Kennwortverschlüsselung.
- Exportieren einzelner oder mehrerer Plattformabfragen
- Hochstufen mehrerer Plattformabfragen
- Hochstufen mit einer vorhandenen Auftragsvorlage
- Importieren und Hochstufen einer vorhandenen LCMBIAR-Datei
- Durchführen der Live-to-Live-Hochstufung

15.7.1 Ausführen des Befehlszeilenprogramms unter Windows

Um das Befehlszeilenprogramm auszuführen, führen Sie die folgenden Schritte aus:

1. Starten Sie ein Befehlszeilenfenster oder eine Shell.
2. Navigieren Sie zu dem entsprechenden Verzeichnis.

   Der Verzeichnispfad für Windows ist z.B. `-C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib`
3. Führen Sie eine der folgenden Aktionen aus:
   - Führen Sie LCMCLI aus; vergewissern Sie sich vor der Ausführung des Programms, dass der Java-Pfad eingestellt ist.

     Command (Befehl): `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <Eigenschaftsdatei>`
   - Führen Sie die BAT-Datei über `C:\Programme (x86)\ SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts\lcm_cli.bat` aus

     Command (Befehl): `lcm_cli.bat -lcmproperty <Eigenschaftsdatei>`

     > **Hinweis**
     >
     > Geben Sie an der Eingabeaufforderung gültige Kennwörter ein.

Das Befehlszeilenprogramm Hochstufverwaltung verwendet eine **`<Eigenschaftendatei>`** als Parameter. Die **`<Eigenschaften>`**-Datei enthält die erforderlichen Parameter, um mit der Hochstufverwaltung über die auszuführenden Aktionen zu kommunizieren; d.h. Verbindung mit welcher Implementierung der BI-Plattform, Verbindungsmethoden, hochzustufende Objekte.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Die Datei muss das Format **<Dateiname>**.properties haben

Zum Beispiel: **<MeineEigenschaften.properties>**

15.7.2 Ausführen des Befehlszeilenprogramms unter Unix

Um das Befehlszeilenprogramm auszuführen, führen Sie die folgenden Schritte aus:

1. Starten Sie die Shell.
2. Navigieren Sie zu dem entsprechenden Verzeichnis.

   Zum Beispiel: /usr/u/qaunix/Aurora604/sap_bobj/enterprise_xi40/java/lib
3. Führen Sie eine der folgenden Aktionen aus:
   - Führen Sie LCMCLI aus; vergewissern Sie sich vor der Ausführung des Programms, dass der Java-Pfad eingestellt ist.

     Command (Befehl): java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <Eigenschaftsdatei>
   - Führen Sie die BAT-Datei über <Iinstallationsverzeichnispfad>\sap_bobj\lcm_cli.sh aus

     Command (Befehl): lcm_cli.sh -lcmproperty <Eigenschaftsdatei>

> **Hinweis**
>
> Geben Sie an der Eingabeaufforderung gültige Kennwörter ein.

15.7.3 Befehlszeilenparameter

In der folgenden Tabelle werden die Parameter und die zulässigen Werte für die Befehlszeilenoption der Hochstufverwaltung beschrieben.

> **Nicht vergessen**
>
> Befehlszeilenparameter dürfen nicht in Anführungszeichen gesetzt werden.

Parameter	Zulässige Werte	Beschreibung	Obligatorisch oder Optional
action	Exportieren, Hochstufen Beispiel: action=export	Mithilfe dieser Option können Sie die Operation festlegen, die die CLI ausführen muss. Diese Operation kann eine der folgenden Optionenen ausführen: • Hochstufen von Objekten aus einer LCMBIAR-Datei oder einem Hochstufverwaltungsauftrag in ein BI-Plattformsystem.	Obligatorisch

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Zulässige Werte	Beschreibung	Obligatorisch oder Optional
		• Exportieren von Objekten aus einem BI-Plattformsystem in eine LCMBIAR-Datei.	
`consolelog`	True oder False	Dieser Parameter wird zur Anzeige des kompletten Protokolls des vom Benutzer ausgeführten Befehls im Befehlsprotokoll verwendet.	Optional Falls dieser Parameter nicht angegeben wird, ist der Standardwert "false".
`Destination_authentication`	secEnterprise, secWinAD, secLDAP,secSAPR3 Beispiel: `Destination_authentication=<Authentifizierung>`	Dieser Parameter gibt den zu verwendenden Authentifizierungstyp an.	Optional Wenn der Authentifizierungstyp nicht angegeben ist, wird `secEnterprise` verwendet.
`Destination_clientID`	Client-ID Beispiel: `Destination_clientID=<System-ID>`	Dieser Parameter wird nur für die SAP-Authentifizierung verwendet.	Obligatorisch für die SAP-Authentifizierung.
`Destination_CMS`	Freiformtext. Beispiel: `Destination_CMS=<CMS-Name:Portnr.>`	Über diesen Parameter kann der Benutzer angeben, mit welchem CMS das Tool eine Verbindung herstellen muss.	Obligatorisch, falls `action=promote`
`Destination_password`	Freiformtext. Beispiel: `Destination_password=<Kennwort>`	Dieser Parameter gibt das zum Benutzerkonto gehörige Kennwort an.	Obligatorisch, falls `action=promote`
`Destination_systemID`	System-ID Beispiel: `Destination_systemID=<System-ID>`	Dieser Parameter wird nur für die SAP-Authentifizierung verwendet.	Obligatorisch für die SAP-Authentifizierung.
`Destination_userName`	Freiformtext. Beispiel: `Destination_username=<Benutzername>`	Dieser Parameter gibt das Benutzerkonto an, über das sich das Tool mit dem BI-Plattform-CMS verbinden muss.	Obligatorisch, falls `action=promote`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Zulässige Werte	Beschreibung	Obligatorisch oder Optional
		Hinweis Delegierter Administrator wird unterstützt.	
`exportLocation`	Freiformtext. Muss eine `<.lcmbiar>`-Erweiterung aufweisen. Beispiel: `exportLocation=C:/Backup/New.lcmbiar`	Über diesen Parameter kann der Benutzer den Speicherort angeben, an dem die LCMBIAR-Datei abgelegt werden soll, nachdem die Objekte exportiert und gepackt wurden.	Obligatorisch, falls `action=export`
`exportDependencies`	False, True Beispiel: `exportDependencies=<true or false>`	Dieser Parameter gibt die von dem Tool für den Export gesammelten Objektabhängigkeiten an. Ist nur anwendbar, wenn er in Verbindung mit dem Kennzeichen `Source_CMS` verwendet wird.	Optional, falls `action=promote or export` Falls dieser Parameter nicht angegeben wird, ist der Standardwert "false".
`exportQuery`	Freiformtext. Verwenden Sie das CMS-Abfragesprachenformat. Beispiel: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi` **Hinweis** Sie können beliebig viele Abfragen in einer .properties-Datei verwenden, die Abfragen müssen jedoch exportQuery1, exportQuery2 usw. genannt werden.	Dies sind die Abfragen, die das Tool zum Abrufen der für den Export vorgesehenen Objekte ausführen soll.	Optional, falls `action=promote or export`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Zulässige Werte	Beschreibung	Obligatorisch oder Optional
exportQueriesTotal	Positive ganze Zahlen exportQueriesTotal=<Ganzzahl>	Über diesen Parameter kann der Benutzer die Anzahl der auszuführenden Exportabfragen angeben. Wenn Sie über x Exportabfragen verfügen und alle Abfragen ausführen möchten, muss dieser Parameter auf x festgelegt werden.	Optional, falls action=promote or export Wenn dieser Wert nicht angegeben wird, ist der Standardwert 1.
importLocation	Freiformtext. Muss eine **<.lcmbiar>**-Erweiterung aufweisen. Beispiel: importLocation=C:/Backup/New.lcmbiar	Über diesen Parameter kann der Benutzer den Speicherort der LCMBIAR-Datei angeben, die die hochzustufenden Objekte enthält.	Optional, falls action=promote
includeApplicationSecurity	false, true Beispiel: includeApplicationSecurity=<true or false>	Dieser Parameter weist das Tool an, die mit den ausgewählten Anwendungen assoziierte Sicherheit zu exportieren oder zu importieren.	Optional; falls dieser Parameter nicht angegeben wird, ist der Standardwert "False". Falls action=promote or export
includeSecurity	false, true Beispiel: includeSecurity=<True oder False>	Dieser Parameter weist das Tool an, die mit den ausgewählten Objekten und Benutzern assoziierte Sicherheit zu exportieren oder zu importierten. Wenn Zugriffsberechtigungen verwendet werden, werden diese hiermit ebenfalls exportiert bzw. importiert.	Optional; falls dieser Parameter nicht angegeben wird, ist der Standardwert "False". Falls action=promote or export
JOB_CUID	Die CUID des gespeicherten Hochstufverwaltungs-Auftrags.	Dieser Parameter weist das Tool an, alle Objekte im Auftrag in die LCMBIAR-Datei zu exportieren.	Optional, falls action=export or promote
lcmbiarpassword	Freiformtext Beispiel: java -cp lcm.jar com.businessobjects.lcm.cli.LCMCLI -lcmproperty lcm.properties -lcmbiarpassword "<testpassword>"	Dieser Parameter ermöglicht die Ver- und Entschlüsselung von BIAR-Dateien mithilfe eines Kennworts.	Optional, falls dies nicht angegeben oder die Zeichenfolge leer ist, ist keine Verschlüsselung vorhanden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Zulässige Werte	Beschreibung	Obligatorisch oder Optional
`lcmproperty`	Der vollständige Pfad zum Speicherort der Eigenschaftendatei `lcm_cli.bat -lcmproperty <Dateipfad der Eigenschaftendatei>`	Dieser Parameter bezieht sich auf die für die Ausführung eines Befehls erforderlichen Werte, die in einer Datei gespeichert sind.	Obligatorisch
`limitQueryBatchSize`	false, true Beispiel: `limitQueryBatchSize=<true or false>`	Dieser Parameter beschränkt die Anzahl der zurückgegebenen Objekte standardmäßig auf 1.000. Wenn dieser Parameter auf "false" gesetzt ist, werden alle abgefragten Objekte zurückgegeben. **Hinweis** Sie können den neuen Grenzwert für die Anzahl der von der Abfrage zurückgegebenen Objekte auch explizit mit folgendem Befehl festlegen: `select TOP <number>`	Optional, falls dieser Parameter nicht angegeben wird, ist der Standardwert "true".
`LCM_authentication`	secEnterprise, secWinAD, secLDAP,secSAPR3 Beispiel: `LCM_authentication=<Authentifizierung>`	Dieser Parameter gibt den zu verwendenden Authentifizierungstyp an.	Optional. Wenn der Authentifizierungstyp nicht angegeben ist, wird `secEnterprise` verwendet.
`LCM_clientID`	Client-ID Beispiel: `LCM_clientID=<Client-ID>`	Dieser Parameter wird für die SAP-Authentifizierung verwendet.	Obligatorisch für die SAP-Authentifizierung.
`LCM_CMS`	Freiformtext. Beispiel: `LCM_CMS=<CMS-Name:Portnr.>`	Über diesen Parameter kann der Benutzer den CMS für die Hochstufverwaltung angeben.	Obligatorisch, falls `action=promote or export`
`LCM_password`	Freiformtext. Beispiel: `LCM_password=<Kennwort>`	Über diesen Parameter kann der Benutzer das Kennwort für das Benutzerkonto angeben.	Obligatorisch, falls `action=promote or export`
`LCM_systemID`	System-ID Beispiel: `LCM_systemID=<System-ID>`	Dieser Parameter wird für die SAP-Authentifizierung verwendet.	Obligatorisch für die SAP-Authentifizierung.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Zulässige Werte	Beschreibung	Obligatorisch oder Optional
`LCM_userName`	Freiformtext. Beispiel: `LCM_user-Name=<Benutzername>`	Über diesen Parameter kann der Benutzer den Benutzernamen des Kontos angeben, den das Tool zum Herstellen einer Verbindung mit dem CMS der Hochstufverwaltung verwenden muss. **Hinweis** Delegierter Administrator wird unterstützt	Obligatorisch, falls `action=promote or export`
`Source_authen-tication`	secEnterprise, secWinAD, secLDAP,secSAPR3 Beispiel: `Source_authen-tication=<Authentifi-zierung>`	Dieser Parameter gibt den zu verwendenden Authentifizierungstyp an.	Optional. Wenn der Authentifizierungstyp nicht angegeben ist, wird `secEnterprise` verwendet.
`Source_clien-tID`	ID des SAP-Client Beispiel: `Source_clien-tID=<System-ID>`	Dieser Parameter wird nur für die SAP-Authentifizierung verwendet.	Obligatorisch für die SAP-Authentifizierung.
`Source_CMS`	Freiformtext. Beispiel: `Source_CMS=<CMSname:Portnr.>`	Über diesen Parameter kann der Benutzer angeben, mit welchem CMS das Tool eine Verbindung herstellen muss.	Obligatorisch, falls `action=export`
`Source_pass-word`	Freiformtext. Beispiel: `Source_pass-word=<Kennwort>`	Dieser Parameter gibt das zum Benutzerkonto gehörige Kennwort an.	Obligatorisch, falls `action=export`
`Source_syste-mID`	SAP-System-ID Beispiel: `Source_syste-mID=<System-ID>`	Dieser Parameter wird nur für die SAP-Authentifizierung verwendet.	Obligatorisch für die SAP-Authentifizierung.
`Source_user-Name`	Freiformtext. Beispiel: `Source_user-name=<Benutzername>`	Dieser Parameter gibt das Benutzerkonto an, über das sich das Tool mit dem BI-Plattform-CMS verbinden muss. **Hinweis** Delegierter Administrator wird unterstützt.	Obligatorisch, falls `action=export`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Zulässige Werte	Beschreibung	Obligatorisch oder Optional
stacktrace	True oder False Beispiel: stackt-race=<True oder False>	Mit diesem Parameter kann der Benutzer alle Aufrufe nachverfolgen.	Optional; falls dieser Parameter nicht angegeben wird, ist der Standardwert "False".

Hinweis

- Ähnlich wie bei der Erstellung eines Auftrags vor dem Export wird mit der Befehlszeilenoption dynamisch ein temporärer Auftrag erstellt. Dieser Auftragsname könnte eine Kombination von Query_<BENUTZER>_<Zeitstempel> sein. Dies trifft nur für **<exportQuery>** zu.
- Einen Rollback des Auftrags können Sie nur über die Hochstufverwaltung durchführen. Befehlszeilen zum Rollback der Aufträge werden nicht unterstützt.
- Wenn Sie mit einer großen Anzahl von Objekten arbeiten, ist es empfehlenswert, die maximale Java-Heapgröße mithilfe des Parameters -Xmx=8g im Script LCMCLI zu erhöhen.

15.7.4 Beispiel für eine Eigenschaftendatei

Nachfolgend wird ein Beispiel für eine Eigenschaften-Datei aufgeführt:

Beispiel

```
importLocation=C:/Backup/CR.lcmbiar

action=promote

LCM_CMS=<CMS-Name:Portnummer>

LCM_userName=<Benutzername>

LCM_password=<Kennwort>

LCM_authentication=<Authentifizierung>

LCM_systemID=<ID>

LCM_clientID=<Client-ID>

Destination_CMS=<CMS-Name:Portnummer>

Destination_userName=<Benutzername>

Destination_password=<Kennwort>

Destination_authentication=<Authentifizierung>

Destination_systemID=<ID>

Destination_clientID=<Client-ID>

lcmbiarpassword=<Kennwort>
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Enthält die `Eigenschaften`-Datei keine persönlichen Informationen, wird der Benutzer von der LCM-Befehlzeilenschnittstelle in der Konsole aufgefordert, diese einzugeben.

15.8 Verwenden des erweiterten Change and Transport System

Das Change and Transport System (CTS) organisiert Entwicklungsprojekte in der ABAP Workbench und passt diese an. Anschließend transportiert es diese Änderungen zu den einzelnen SAP-Systemen in Ihrer Systemlandschaft. Das erweiterte Change and Transport System (CTS+) ist ein Addon zu CTS, das ABAP-fremde Inhalte übergreifend über CTS+-aktivierte, ABAP-fremde Repositorys hochstuft.

BI-Plattform-InfoObjects können SAP-Business-Warehouse-Inhalte als Datenquelle verwenden. Die Integration von CTS+ mit der Hochstufverwaltung ermöglicht die Handhabung des BI-Plattform-Repositorys auf ähnliche Weise wie die des Repositorys von SAP Business Warehouse (BW), indem CTS-Transportanforderungen zum Hochstufen von Aufträgen verwendet werden. CTS+ bietet eine Option zum Transport von SAP-fremden Objekten innerhalb einer Systemlandschaft. Beispielsweise können im Entwicklungssystem erstellte Objekte an eine Transportanforderung angehängt und an andere Systeme innerhalb der Landschaft weitergeleitet werden.

Weitere Informationen zum Change and Transport System erhalten Sie unter *Change and Transport System - Overview (BC-CTS)*

Weitere Informationen über CTS+- und ABAP-fremde Transporte finden Sie unter *Transporting Non-ABAP Objects in Change and Transport System*

15.8.1 Voraussetzungen

Für die Übertragung von Business-Intelligence-Inhalt von einem System in ein anderes mittels CTS+ wird Folgendes vorausgesetzt:

1. BI-Plattform 4.0 (oder höher) ist installiert.
2. SAP Solution Manager 7.1 oder SAP Solution Manager 7.0 EHP1 (mindestens SP25) ist installiert und wird zumindest für die Konfiguration von SAP-BusinessObjects-Systemen als Domänencontroller für CTS+ verwendet.

   Weitere Informationen zum Konfigurieren der Transportdomäne finden Sie unter *Konfigurieren der Transportdomäne*.
3. Das CTS-Plugin ist unter SAP Solution Manager installiert. (Das CTS-Plugin stammt aus SL Toolset 1.0 SP02. Es empfiehlt sich, das neueste verfügbare CTS-Plugin zu verwenden.)

   Weitere Informationen zur Installation des erforderlichen CTS-Plugins finden Sie in folgendem SAP-Hinweis:

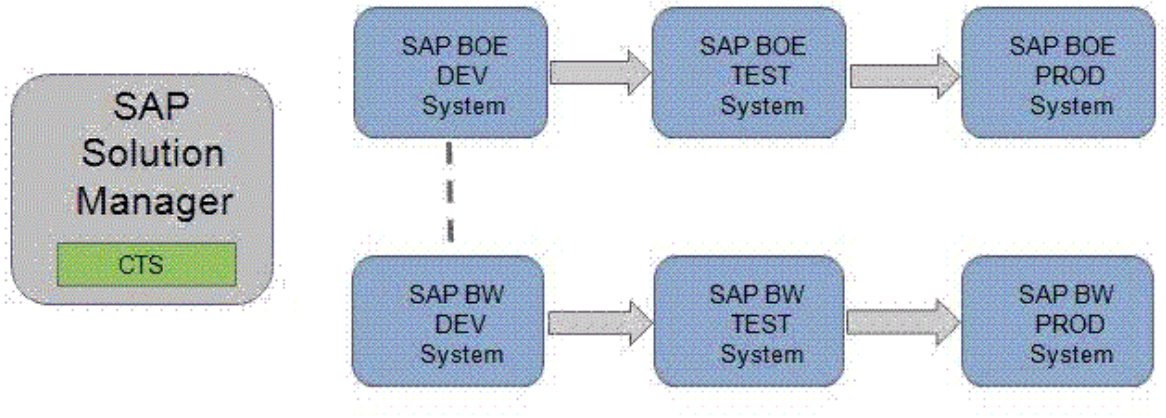
   SAP-Hinweis 1533059.
4. Systeme der Version *SAP Business Warehouse 7.0* (SPS 24 oder höher) wurden installiert. Weitere

   Informationen finden Sie im *SAP-Hinweis 1369301*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

5. Die SAP-Business-Warehouse-Transportlandschaft (SAP-BW-Transportlandschaft) wurde im Change and Transport System (CTS) konfiguriert.
6. *SAP-Hinweis 1692417* und *SAP-Hinweis 1860594* wurden auf dem Rechner implementiert, der als Host für den Webdienst CTS Deploy fungiert.

15.8.2 Konfigurieren der BI-Plattform und CTS+-Integration



Das Transport Management System (TMS), das Teil des Change and Transport System ist, wird zum Transport von Änderungen zwischen SAP-Systemen innerhalb einer Landschaft verwendet. Es verwaltet die verbundenen Systeme und ihre Routen sowie die Importe in die zugehörigen Systeme. Weitere Informationen zum Transport Management System finden Sie unter *Transport Management System (BC-CTS-TMS)*

CTS+ ermöglicht die Sammlung von Dateien von außerhalb und deren Verteilung in einer Transportlandschaft. Über die Web-Benutzeroberfläche des Transport Organizers, der Teil von CTS+ ist, werden die Transportanforderungen und die darin enthaltenen Objekte verwaltet. Weitere Informationen finden Sie unter *Transport Management System (BC-CTS-TMS)*.

Sie können die Hochstufverwaltung der BI-Plattform unter Verwendung von CTS-Transportanforderungen mit CTS+ und SAP BW integrieren.

> **Hinweis**
>
> Um die Integration der BI-Plattform in SAP Solution Manager zu ermöglichen, müssen Sie den Anwendungstyp BOLM in der SAP-Solution-Manager-Landschaft definieren.

Führen Sie die folgenden Schritte aus, um die BI-Plattform und CTS+ zu integrieren:

1. Aktivieren Sie den Webdienst für den CTS-Export.
2. Konfigurieren Sie CTS-Einstellungen in der Hochstufverwaltung.
3. Konfigurieren Sie das BI-Plattform-Importsystem in SAP Solution Manager.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Aktivieren des Webdiensts für den CTS-Export [Seite 570]
Konfigurieren von CTS+-Einstellungen im Hochstufverwaltungstool [Seite 570]
Konfigurieren der BI-Plattform und CTS+-Integration [Seite 569]

15.8.2.1 Aktivieren des Webdiensts für den CTS-Export

Zur Konfiguration der BI-Plattform muss der Webdienst für den CTS-Export im Webtool SOA Management aktiviert werden.

1. Um die Anwendung zu starten, geben Sie den Transaktionscode SOAMANAGER in SAP Solution Manager ein. Nachdem die erforderliche Authentifizierung erfolgt ist, wird die SOA Management Console in einem Webbrowser geöffnet.

   Weitere Informationen zu SOA Management und zur Konfiguration eines Dienst-Endpoints mithilfe von SAP Solution Manager 7.0 finden Sie unter *Configurieren eines Dienstproviders*. Informationen zu SAP Solution Manager 7.1 finden Sie in *Konfigurieren eines Dienstproviders*.
2. Klicken Sie auf der Registerkarte **Application and Scenario Communication** (Anwendungs- und Szenariokommunikation) auf **Single Service Configuration** (Einzeldienstkonfiguration).

   Der Webdienst für den CTS-Export heißt `EXPORT_CTS_WS`.
3. Erstellen oder Bearbeiten Sie auf der Registerkarte **Configuration** (Konfiguration) den Dienstendpunkt.
4. Konfigurieren Sie auf der Registerkarte **Security** (Sicherheit) das Transportprotokoll und die Authentifizierungsmethode.
5. Definieren Sie auf der Registerkarte **Transport Settings** (Transporteinstellungen) eine alternative Zugriffs-URL zum einfachen Zugriff auf den Dienstendpunkt.

15.8.2.2 Konfigurieren von CTS+-Einstellungen im Hochstufverwaltungstool

Im folgenden Abschnitt werden die in der CMC durchzuführenden Konfigurationsschritte beschrieben, um CTS+ für die Verwendung mit dem Hochstufverwaltungstool einzurichten.

1. Klicken Sie auf der Seite *Hochstufungsaufträge* auf **CTS-Einstellungen** und dann auf **BW-Systeme**.
2. Klicken Sie auf der Seite *BW-Systeme* auf **Hinzufügen**, um der Umgebung ein BW-System hinzuzufügen.
3. Geben Sie auf der Seite *System hinzufügen* die folgenden Details ein:
   - **Host-BW-SID**: Geben Sie die System-ID (SID) des Hostcomputers von SAP BW/ABAP an.
   - **Hostname**: Geben Sie die IP-Adresse des Hostcomputers an.
   - **Systemnummer**: Geben Sie die Systemnummer des Hostsystems ein.
   - **Client**: Bezieht sich auf die Systemdetails des Clientcomputers.
   - **Benutzer** und **Kennwort**: Geben Sie den Benutzernamen und das Kennwort für den Clientcomputer in diesen Feldern an.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- **Sprache**: Geben Sie die gewünschte Sprache in diesem Feld an.

4. Klicken Sie auf **OK**, um das System der Umgebung hinzuzufügen.

> **Hinweis**
>
> Nachdem Sie der Umgebung ein BW-System hinzugefügt haben, können Sie mit **Bearbeiten** oder **Löschen** auf der Seite *BW-Systeme* Änderungen an den Systemen in der Umgebung vornehmen.

5. Klicken Sie auf der Seite *Hochstufungsaufträge* auf **CTS-Einstellungen** und dann auf **Webdiensteinstellungen**.
6. Geben Sie auf der Seite *Webdiensteinstellungen* die Webdienst-URL und die Benutzerdetails ein.

> **Hinweis**
>
> Wenn Sie diese Details nicht kennen, holen Sie sie von der Solution-Manager-Systemverwaltung ein.

7. Klicken Sie auf **Speichern** und **Schließen**, um das Hinzufügen der Webdiensteinstellungen abzuschließen.
8. Erstellen Sie eine Zuordnungsdatei für das Hochstufverwaltungs-CMS der BI-Plattform.

   Führen Sie die folgenden Schritte im Entwicklungssystem der BI-Plattform aus, um eine Textdatei mit Konnektivitätsdetails zur Aktivierung der Zuordnung zu erstellen:

   a) Wechseln Sie im Hochstufverwaltungs-CMS der BI-Plattform in das Root-Verzeichnis, und erstellen Sie einen Ordner mit dem Namen **LCM** unter dem Pfad **<InstallVerz>**/SAP BusinessObjects Enterprise XI 4.0/.

   b) Erstellen Sie eine Textdatei mit dem Namen LCM_SOURCE_CMS_SID_MAPPING.properties, und nehmen Sie eine der folgenden Eingaben in der Datei vor:

      - **<Vollständiger Name des Quellsystems von SAP BI mit Domäne>@<CMS-Portnummer> = <logischer Name für das Quellsystem wie in der CTS-Konfiguration verwendet>**
      - **<IP-Nummer des Quellsystems von SAP BI>@<CMS-Portnummer> = <logischer Name für das Quellsystem wie in der CTS-Konfiguration verwendet>**

   Beispiel:

```
DEWDFTH04171S@6400=WJ3
10.208.112.177@6400=WJ3
DEWDFTH04171S.pgdev.sap.corp@6400=WJ3
```

> **Hinweis**
>
> Verfügen Sie über eine geclusterte Umgebung, dann kopieren Sie die Datei LCM_SOURCE_CMS_SID_MAPPING.properties auf das System, auf dem der Adaptive Processing Server ausgeführt wird.

Weitere Informationen zur Durchführung von Konfigurationsschritten für ABAP-fremde Systeme finden Sie unter *Transporteinstellungen in der Anwendung*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15.8.2.3 Konfigurieren des BI-Plattform-Importsystems im SAP Solution Manager

1. Melden Sie sich am SAP-Solution-Manager-System an.
2. Geben Sie Transaktion *stms* ein, und drücken Sie die *Eingabetaste*.
3. Konfigurieren Sie BOLM als Anwendungstyp.
   a) Wechseln Sie zu **Overview (Überblick)** > **Systems (Systeme)**.
   b) Wechseln Sie zu **Extras** > **Application Type (Anwendungstyp)** > **Configure (Konfigurieren)**.
   c) Wählen Sie **New Entries** (Neue Einträge) aus.
   d) Geben Sie in das Feld **Application Type** (Anwendungstyp) den Typ `BOLM` ein.
   e) Geben Sie eine Beschreibung ein.
   f) Geben Sie in das Feld **Support Details** (Unterstützungsdetails) den Wert `http://service.sap.com (ACH: BOJ-BIP-DEP)` ein.
   g) Klicken Sie auf **Table View (Tabellenansicht)** > **Save (Speichern)**.
   h) Bestätigen Sie die Eingabeaufforderung durch Auswahl von **Yes** (Ja).
4. Um mit verschiedenen Sprachen zu arbeiten, können Sie übersetzte Texte folgendermaßen pflegen:
   a) Wählen Sie **Goto (Gehe zu)** > **Translation (Übersetzung)**.
   b) Wählen Sie die Sprachen aus, in die der Text übersetzt werden soll.
   c) Geben Sie die übersetzten Werte in die Felder **Description** (Beschreibung) und **Support Details** (Unterstützungsdetails) ein.
   d) Bestätigen Sie das Dialogfeld.
   e) Wählen Sie **Continue** (Weiter) aus.
   f) Klicken Sie auf **Table View (Tabellenansicht)** > **Save (Speichern)**.
   g) Bestätigen Sie die Eingabeaufforderung.

   Die TMS-Domäne kann jetzt die Verwendung von Business-Intelligence-Inhalt in CTS unterstützen.
5. Definieren Sie in CTS+ das Quellsystem der BI-Plattform als Exportsystem.

   > **Hinweis**
   >
   > Weitere Informationen zum Erstellen eines ABAP-fremden Systems als Quellsystem finden Sie unter *Definieren und Konfigurieren von ABAP-fremden Systemen*.

6. Konfigurieren Sie in CTS+ das Importsystem der BI-Plattform, indem Sie folgende Schritte ausführen:

   > **Hinweis**
   >
   > Sie können eine SID als Verweis auf das Importsystem der BI-Plattform definieren.

   a) Erstellen Sie ein ABAP-fremdes System als Importsystem.
      Weitere Informationen finden Sie unter *Definieren und Konfigurieren von ABAP-fremden Systemen*.
   b) Legen Sie die Implementierungsmethode auf **Others** (Sonstige) fest, und heben Sie die Auswahl aller anderen Optionen auf.
   c) Wählen Sie **Speichern**.
   d) Bestätigen Sie das Verteilungs-Dialogfeld.
      Die Tabellenansicht zur Konfiguration der Importsystemeinstellungen wird angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

e) Wählen Sie **Edit (Bearbeiten)** > **New Entries (Neue Einträge)**.

f) Führen Sie auf dem Bildschirm "Change View CTS: System details for handling of application types" (Ansicht-CTS ändern: Details zu Behandlung von Anwendungstypen) folgende Schritte aus:

1. Wählen Sie im Feld **Deploy Method** (Implementierungsmethode) die Option **application-specific Deployer (EJB)** (Anwendungsspezifischer Implementierer (EJB)) aus.
2. Geben Sie in das Feld **Deploy-URI** folgende URI ein: `http://<BOE-Webservername>:<Webserver-Port>/BOE/LCM/CTSServlet?&cmsName=<BOE-Zielname>:<CMS-Port>&authType=<BOE-Authentifizierungstyp>`

   Dabei gilt:

   - Der "BOE-Webservername" ist der Name bzw. die IP-Adresse des Rechners, auf dem der Webserver der BI-Plattform ausgeführt wird.
   - Der "Webserver-Port" ist die Portnummer des Webservers der BI-Plattform.
   - Der "BOE-Zielname" ist der Name des Rechners, auf dem der Central Management Server (CMS) der BI-Plattform ausgeführt wird.
   - Der "CMS-Port" ist die Portnummer des Ziel-CMS.
   - Der "BOE-Authentifizierungstyp" ist der Typ der Benutzerauthentifizierung für den Import von Business-Intelligence-Inhalten. Es werden die Authentifizierungstypen secEnterprise, secLDAP, secWinAD und secSAPR3 unterstützt.
3. Geben Sie in das Feld **User** (Benutzer) den Benutzernamen der BI-Plattform ein.
4. Geben Sie in das Feld **Password** (Kennwort) das Kennwort der BI-Plattform ein.
5. Wählen Sie **Save** (Speichern), um die Einstellungen zu speichern.

Wenn mehr als ein Importsystem benötigt wird, wiederholen Sie die obigen Schritte, um alle erforderlichen Zielsysteme zu erstellen. Weitere Informationen zur Konfiguration von Transportrouten zwischen dem Quell- und Zielsystem nach der Erstellung der Zielsysteme erhalten Sie unter *Konfigurieren von Transportrouten*.

15.8.2.4 Exportieren von der BI-Plattform nach CTS+ mit SSL

15.8.2.4.1 Konfigurieren von SSL für CTS+

Um SSL für CTS+ zu konfigurieren, müssen Sie SSL auf dem Application Server ABAP konfigurieren. Weitere Informationen finden Sie unter *Configuring the SAP Web AS for Supporting SSL*.

15.8.2.4.2 Konfigurieren des clientseitigen SSL-Zertifikats

Um das clientseitige SSL-Zertifikat zu konfigurieren, müssen Sie entweder das Serverzertifikat oder das vertrauenswürdige CA-Zertifikat in den JVM-Keystore importieren.

1. Sichern Sie die `cacerts`-Dateien vom Verzeichnis `<INSTALLVERZ>\win64_x64\sapjvm\jre\lib\security6`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Importieren Sie das Zertifikat in die Tomcat-JVM, die die Datei `BOE.war` bereitstellt, unter Verwendung folgender Parameter:

```
<INSTALLVERZ>\win64_x64\sapjvm\jre\bin\keytool.exe -import -file server.cer -
keystore cacerts
```

3. Starten Sie Tomcat neu.

15.8.2.4.3 Konfigurieren des Exportwebdiensts CTS+

Um den HTTPS-fähigen Exportwebdienst CTS+ (`EXPORT_CTS_WS`) zu konfigurieren, können Sie einen neuen HTTPS-Endpoint erstellen.

> **Hinweis**
>
> Alternativ können Sie für den bestehenden HTTP-Endpoint die Verwendung von HTTPS konfigurieren.

1. Geben Sie den Transaktionscode **`soamanager`** ein, und wählen Sie auf der Registerkarte *Provider Security* (Providersicherheit) unter *Communication Security* (Kommunikationssicherheit) die Option **SSL over HTTP (Transport Channel Security)** (SSL über HTTP (Transportkanalsicherheit) und unter *Transport Channel Authentication* (Transportkanalauthentifizierung) die Option **User ID/Password** (Benutzer-ID/Kennwort).
2. Wählen Sie auf der Registerkarte *Transport settings* (Transporteinstellungen) unter *Transport Binding* (Transportbindung) die Option **HTTPS** für *Calculated Protocol* (Berechnetes Protokoll).

15.8.2.4.4 Konfigurieren der Hochstufverwaltung für SSL

> **Nicht vergessen**
>
> Importieren Sie das Serverzertifikat oder die vertrauenswürdige CA-Zertifikat in den JVM-Keystore.

1. Klicken Sie in der CMC auf der Registerkarte *Hochstufverwaltung* auf **Einstellungen** > **CTS-Einstellungen** > **Webdiensteinstellungen**.
2. Stellen Sie sicher, dass der Parameter *Web-Service-URL* mit `https://` beginnt und die oben konfigurierte Portnummer enthält.

> **Hinweis**
>
> Die Option **Hochstufen mit CTS** wird in der Liste **Job-Ziel** bzw. im Dialogfenster *Überschreibungen* nicht angezeigt, wenn die angegebene URL nicht erreichbar ist. Falls der SSL-Handshake zwischen der Hochstufverwaltung und CTS+ fehlschlägt, wird in der CMC-Protokolldatei ein Fehler erfasst.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15.8.2.5 Importieren von CTS+ zur BI-Plattform mit SSL

15.8.2.5.1 Konfigurieren von BI-Plattform-Tomcat zur Verwendung von HTTPS

Um BI-Plattform-Tomcat für die Verwendung von HTTPS zu konfigurieren, müssen Sie auf dem Rechner mit der installierten BI-Plattform folgende Schritte ausführen.

1. Erstellen Sie ein Serverschlüsselpaar, ein Zertifikat und einen Keystore.
   a) Führen Sie **<INSTALLDIR>**`\win64_x64\sapjvm\jre\bin\keytool.exe` mit den folgenden Parametern aus:

   ```
   keytool -genkey -alias server -keyalg RSA -keysize 1024 -keystore
   serverkeystore.jks -storetype JKS

   keytool -certreq -keyalg RSA -alias server -file server.csr -keystore
   serverkeystore.jks
   ```

   b) Geben Sie an der Eingabeaufforderung folgende Informationen ein:
      - Ihren Vor- und Nachnamen
      - Den Namen Ihrer Organisationseinheit
      - Den Namen Ihrer Organisation
      - Den Namen Ihrer Stadt oder Ihres Orts
      - Den Namen Ihres Bundesstaats oder Ihrer Provinz
      - Den aus zwei Buchstaben bestehenden Ländercode für diese Einheit

      Es wird eine formatierte Zeichenfolge angezeigt, z.B. `CN=Thomas Schmidt, OU=Rechnungswesen, O=SAP, L=Vancouver, ST=BC, C=CA`). Geben Sie **Ja** ein, und drücken Sie zur Bestätigung die *Eingabetaste*.
2. Senden Sie die Serverzertifikatsanforderung an eine Zertifizierungsstelle.
3. Importieren Sie das signierte Zertifikat mithilfe der folgenden Parameter in den Server-Keystore:

   ```
   keytool -import -alias server -keystore serverkeystore.jks -trustcacerts -file
   server.crt
   ```

4. Konfigurieren Sie die Tomcat-Konfigurationsdatei `server.xml`, um HTTPS zu aktivieren und den von Ihnen erstellten Server-Keystore zu verwenden.
5. Starten Sie Tomcat neu, und testen Sie die Verbindung, indem Sie folgende URL in einem Browser öffnen: `https://`**<SERVERNAME>:<SSLPORTNUMBER>**

Weitere Informationen

Konfigurieren von SSL für CTS+ [Seite 573]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

15.8.2.5.2 Konfigurieren von CTS+ für SSL

Um CTS+ für SSL zu konfigurieren, müssen Sie einen SSL-Client-PSE erstellen und ein Zertifikat importieren.

Weitere Informationen

Konfigurieren von SSL für CTS+ [Seite 573]

15.8.2.5.3 Aktualisieren der Test- und Produktionssysteme in CTS+ auf HTTPS-Verwendung

Um für die Test- und Produktionssysteme die Verwendung von HTTPS zu aktivieren, führen Sie folgende Schritte durch:

1. Starten Sie Transaktion STMS.
2. Klicken Sie auf **Überblick über das System**.
3. Wählen Sie Ihr Test- oder Produktionssystem aus, und klicken Sie **Springen** > **Anwendungstypen** > **Implementierungsmethode**.
4. Stellen Sie sicher, dass der Parameter *Deploy-URI* mit `https://` beginnt und eine korrekte HTTPS-Portnummer enthält.

15.8.3 Hochstufen von Aufträgen über CTS

In diesem Abschnitt wird der Workflow beschrieben, den das Hochstufverwaltungs-Tool unterstützt, um BI-Plattform-CMS-Objekte (Central Management Server) unter Verwendung des Change Transport Systems aus dem Quellsystem in das Zielsystem hochzustufen. Führen Sie folgende Schritte aus, um CTS zum Hochstufen von Aufträgen zu verwenden:

1. Starten Sie das Hochstufverwaltungs-Tool über die SAP-Authentifizierung, und erstellen Sie einen Auftrag.

   Weitere Informationen über das Erstellen eines neuen Auftrags finden Sie im Abschnitt "Erstellen von Aufträgen" über die zugehörigen Links weiter unten.

   > **Hinweis**
   >
   > Stellen Sie sicher, dass Sie auf dem Anmeldebildschirm des Quellsystems den Authentifizierungstyp "SAP" auswählen.

2. Wählen Sie aus der Dropdown-Liste **Ziel** die Option **Hochstufen mit CTS** aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Klicken Sie auf **Erstellen**.
   Der Bildschirm *Objekte aus dem System hinzufügen* wird angezeigt. Hier werden die Ordner und Unterordner in einer Baumstruktur angezeigt.
4. Navigieren Sie zu dem Ordner, aus dem Sie ein InfoObject wählen möchten.
5. Wählen Sie das dem Auftrag hinzuzufügende InfoObject, und klicken Sie auf **Hinzufügen**. Wenn Sie ein InfoObject hinzufügen und das Dialogfeld *Objekte hinzufügen* schließen möchten, klicken Sie auf **Hinzufügen & Schließen**.
   Das InfoObject wird an den Auftrag angehängt, und der Bildschirm *Hochstufungsaufträge* wird angezeigt.

   > **Hinweis**
   >
   > Im Bildschirm "Hochstufungsaufträge" können Sie folgende Aktionen durchführen:
   >
   > - Sie können dem Job mit der Option **Objekte hinzufügen** weitere InfoObjects hinzufügen. Weitere Informationen finden Sie unter "Hinzufügen eines InfoObjects zu einem Auftrag".
   > - Mit der Option **Abhängigkeiten verwalten** können Sie die Abhängigkeiten des ausgewählten InfoObjects verwalten. Die SAP BW-Abhängigkeiten des Objekts werden auf der Benutzeroberfläche angezeigt und stehen dort für den Benutzer zur Auswahl.
   >
   > Weitere Informationen finden Sie unter "Verwalten von Auftragsabhängigkeiten".

6. Klicken Sie auf **Hochstufen**.
   Der Bildschirm *Hochstufen* wird mit der ID, dem Eigentümer und einer kurzen Beschreibung der aktuell eingerichteten Transportanforderung angezeigt.
7. Sie können den Hyperlink **Transportanforderungen** verwenden, um:
   - Details der Transportanforderung anzuzeigen.
   - Einstellungen der Standardtransportanforderung zu ändern.
   - Eine andere Transportanforderung auszuwählen.
   - Eine Transportanforderung zu erstellen.

   1. Klicken Sie auf den Hyperlink **Transportanforderungen**, um die Web-Benutzeroberfläche des *Transport Organizers* zu öffnen.
   2. Wenn Sie zur Eingabe von Anmeldedaten aufgefordert werden, melden Sie sich mit den gültigen Anmeldedaten für das CTS-Domänencontroller-System an.
   3. Regenerieren Sie den Bildschirm *Hochstufen*, um die Updates anzuzeigen.

   Weitere Informationen zur Verwendung der Web-Benutzeroberfläche des *Transport Organizers* erhalten Sie unter *Web-Benutzeroberfläche des Transport Organizers*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8. Klicken Sie auf den Hyperlink **Abhängigkeiten auf zweiter Ebene**, um die Details zu den Abhängigkeiten der SAP BW-Objekte anzuzeigen.

> **Hinweis**
>
> Wenn Sie auf den Hyperlink **Abhängigkeiten auf zweiter Ebene** klicken, werden nur die Objekte angezeigt, die in einer Anforderung gesperrt sind. Wenn die Anforderung freigegeben wurde, können Sie keine Abhängigkeiten anzeigen. Außerdem ist dieser Hyperlink ausgegraut, wenn keine aktiven Abhängigkeiten auf zweiter Ebene vorhanden sind.

9. Klicken Sie auf **Hochstufen**.
10. Schließen Sie den Auftrag.
    Der Hauptbildschirm der Hochstufverwaltung wird angezeigt. Der Status des erstellten Auftrags lautet jetzt **In CTS+ exportiert**.
11. Gehen Sie zum Freigeben des BI-Plattformobjekts an das Zielsystem wie folgt vor:
    a) Klicken Sie auf den Hyperlink in der Spalte "Status" des Auftrags, den Sie hochstufen möchten.
    Das Fenster *Hochstufungsstatus* wird angezeigt.
    b) Klicken Sie auf **Anforderungsstatus**.
    Die Web-Benutzeroberfläche des *Transport Organizers* wird angezeigt.
    c) Wenn der Status der Anforderung **Modifiable** (Modifizierbar) lautet, klicken Sie auf **Release** (Freigeben), um die Transportanforderung des BI-Plattformobjekts freizugeben. Weitere Informationen zur Freigabe von Transportanforderungen mit ABAP-fremden Objekten finden Sie unter *Freigabe von Transportanforderungen mit ABAP-fremden Objekten*.
    d) Schließen Sie die Web-Benutzeroberfläche des *Transport Organizers*.
12. Klicken Sie zum Anzeigen der Abhängigkeiten des SAP BW-Objekts auf den Hyperlink **Liste der BW-Abhängigkeiten**.

> **Hinweis**
>
> Es wird empfohlen, in Kontakt mit dem SAP BW-Team zu bleiben, um hinsichtlich der SAP BW-Abhängigkeiten und ihrer Freigabe informiert zu sein, da das Team für diese Objekte zuständig ist.

13. Schließen Sie das Fenster *Hochstufungsstatus*.
14. Gehen Sie zum Importieren des BI-Plattformobjekts in das Zielsystem wie folgt vor:
    a) Melden Sie sich am CTS+-Domänencontroller an.
    b) Rufen Sie die Transaktion `STMS` auf, um das Transport Management System zu öffnen.
    c) Klicken Sie auf das Symbol **Importübersicht**.
    Der Bildschirm *Importübersicht* wird angezeigt. Hier können Sie die Elemente in der Importqueue von allen Systemen einsehen.
    d) Wählen Sie die System-ID des Ziel-Hochstufverwaltungssystems aus.
    Es wird eine Liste der Transportanforderungen angezeigt, die in das System importiert werden können.
    e) Klicken Sie auf **Regenerieren**.
    f) Importieren Sie die relevanten Transportanforderungen. Weitere Informationen finden Sie unter *Importieren von Anforderungen*.

    Allgemeine Informationen zum Importieren von Transportanforderungen mit BOLM-Inhalt finden Sie unter *Importieren von Transportanforderungen mit ABAP-fremden Objekten*.
15. Wenn das ausgewählte Objekt SAP BW-Abhängigkeiten aufweist, führen Sie folgende Schritte durch:
    a) Gehen Sie zum Freigeben der SAP BW-Abhängigkeiten an das Zielsystem wie folgt vor:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Melden Sie sich beim SAP BW-Quellsystem an.
2. Rufen Sie die SE09-Transaktion auf. Der Bildschirm *Transport Organizer* wird angezeigt.
3. Klicken Sie auf **Anzeigen**. Die SAP BW-Anforderung wird angezeigt.
4. Klicken Sie auf die SAP BW-Anforderung, und klappen Sie sie auf, um die für die Abhängigkeiten erstellen Aufgaben anzuzeigen.
5. Klicken Sie mit der rechten Maustaste auf die Anforderung, die mit dem primären SAP BW-Objekt verknüpft ist, und wählen Sie **Direkt freigeben** aus. Wiederholen Sie diesen Schritt, um alle mit den einzelnen abhängigen Objekten verknüpften Aufgaben separat freizugeben.
6. Klicken Sie mit der rechten Maustaste auf die Anforderung, die mit dem primären BW-Objekt verknüpft ist, und wählen Sie **Direkt freigeben** aus.
7. Regenerieren Sie den Bildschirm, bis alle Anforderungen freigegeben wurden.

> **Hinweis**
>
> Sie können die Protokolle einer Anforderung anzeigen, indem Sie auf diese doppelklicken.

b) Gehen Sie zum Importieren der SAP BW-Abhängigkeiten in das Zielsystem wie folgt vor:

1. Melden Sie sich beim SAP BW-Zielsystem an.
2. Rufen Sie die STMS-Transaktion auf, um das Transport Management System zu öffnen.
3. Klicken Sie auf das Symbol **Importübersicht**. Der Bildschirm *Importübersicht* wird angezeigt.
4. Doppelklicken Sie auf die System-ID für das SAP BW-Ziel. Es wird eine Liste der Transportanforderungen angezeigt, die in das System importiert werden können.
5. Importieren Sie die relevanten Transportanforderungen. Weitere Informationen finden Sie unter *Importieren von Anforderungen*.

   Weitere Informationen zu Transporten mit Importqueues erhalten Sie unter *Transporte mit Importqueues*.

16. Melden Sie sich am Zielsystem an, um den Status des hochgestuften Auftrags anzuzeigen.

Weitere Informationen zum Generic CTS finden Sie unter *Konfigurieren von Zielsystemen für weitere Anwendungen*.

Weitere Informationen

Einen Auftrag erstellen [Seite 534]
Verwalten der Abhängigkeiten eines Auftrags [Seite 540]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

16 Versionsverwaltung

16.1 Verwalten mehrerer Versionen von BI-Ressourcen

Mit der Versionsverwaltung können Sie mehrere Versionen von BI-Ressourcen verwalten, die sich im Repository der BI-Plattform befinden. Um diese Funktion zu vereinfachen, enthält das Tool das Versionsverwaltungssystem Subversion.

> **Hinweis**
>
> Das System ClearCase ist nicht Teil der Installation der BI-Plattform. Wenn Sie es zur Versionsverwaltung nutzen möchten, müssen Sie es installieren.

Um mehrere Versionen von Aufträgen oder InfoObjects zu verwalten, führen Sie folgende Schritte aus:

1. Melden Sie sich bei der CMC-Anwendung an und wählen **Versionsverwaltung**.
2. Wählen Sie im linken Bereich des Fensters *Versionsverwaltung* den Ordner mit den Aufträgen bzw. InfoObjects, deren Versionen Sie verwalten möchten.
3. Wählen Sie die InfoObjects, und klicken Sie auf **Zu VM hinzufügen**.

   > **Hinweis**
   >
   > Durch Klicken auf *Zu VM hinzufügen* wird eine Basisversion des Objekts im Repository des Versionsverwaltungssystems angelegt. Die Basisversion wird zum anschließenden Einchecken benötigt.

4. Klicken Sie bei nachfolgenden Änderungen am Dokument und zur Versionierung des inkrementell geänderten Dokuments auf **Einchecken**. Dadurch wird das im VMS-Repository enthaltene Dokument aktualisiert.

   Das Dialogfeld *Eincheck-Kommentare* wird angezeigt.
5. Geben Sie Ihre Kommentare ein, und klicken Sie auf **OK**.
   Die geänderte Versionsnummer des ausgewählten InfoObjects wird in den Spalten *VMS-Version* und *CMS-Version* (Central Management Server) angezeigt.
6. Zum Abrufen der aktuellen Version des Dokuments vom VMS wählen Sie das betreffende InfoObject, und klicken Sie auf **Aktuelle Version abrufen**.
   Die letzte Version des VMS-Repositorys wird in den CMS importiert.
7. Zum Erstellen einer Kopie der aktuellen Version klicken Sie auf **Kopie erstellen**.
   In den VMS- und CMS-Repositorys wird eine Kopie der ausgewählten Version erstellt.
8. Wählen Sie **Verlauf**, um alle für das ausgewählte InfoObject verfügbaren Versionen anzuzeigen.
   Das Fenster *Verlauf* wird angezeigt. Folgende Optionen werden angezeigt:
   - **Version abrufen** – Falls mehrere Versionen vorhanden sind und Sie eine bestimmte Version der BI-Ressource benötigen, können Sie das benötigte InfoObject auswählen und auf **Version abrufen** klicken.
   - **Kopie von Version abrufen** – Mit dieser Option können Sie eine Kopie der ausgewählten Version abrufen.
   - **Kopie von Version exportieren** – Mit dieser Option können Sie eine Kopie der ausgewählten Version in Ihrem lokalen System speichern.
   - **Vergleichen** – Mit dieser Option können Sie die Metadateninformationen von zwei Versionen eines Auftrags vergleichen. Weitere Informationen finden Sie unter “Vergleichen von verschiedenen Versionen desselben Auftrags”.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

9. Wählen Sie ein InfoObject aus, und klicken Sie auf **Sperren**, um das InfoObject zu sperren, oder auf **Sperrung aufheben**, um das InfoObject zu entsperren, oder auf **Löschen**, um alle versionierten Inhalte aus dem VMS-Repository zu löschen. Inhalte in der CMS sind nicht davon betroffen.

> **Hinweis**
>
> Wenn Sie das InfoObject sperren, können Sie keine Aktionen für dieses InfoObject ausführen.

10. Wenn die Version im CMS neuer ist als die Version im VMS, wird ein Kennzeichen neben dem aktualisierten InfoObject angezeigt. Wenn Sie den Cursor auf das Kennzeichen bewegen, erscheint die QuickInfo `Auf dem CMS befindet sich eine aktuellere Version`.
11. Um eine Liste mit allen eingecheckten Ressourcen, die im VMS, jedoch nicht im CMS vorhanden sind, anzuzeigen, klicken Sie auf **Gelöschte Ressourcen anzeigen**
    Klicken Sie auf eine gelöschte Ressource, um ihren Verlauf anzuzeigen. Sie können die gelöschte Ressource auswählen und auf **Version abrufen** klicken, um diese spezifische Version der Ressource anzuzeigen.

    Klicken Sie auf **Löschen**, um das Objekt auch dauerhaft aus dem VMS-Repository zu löschen.

> **Hinweis**
>
> Wenn Sie **Version abrufen** wählen, wird die Ressource aus der Liste fehlender Dateien des VMS in das CMS verschoben.

12. Wählen Sie ein InfoObject, und klicken Sie auf , um die Eigenschaften des InfoObjects anzuzeigen.
    Alternativ können Sie auch mit der rechten Maustaste auf das InfoObject klicken und die Schritte 3 bis 12 ausführen.

16.2 Manuelles Starten und Stoppen von Subversion unter Unix

Unter Unix kann es sein, dass Subversion nicht autmatisch startet, nachdem der Rechner neu gestartet wurde. Von der BI-Plattform 4.1 SP2 aus können Subversion über den Befehl **`<INSTALLVERZ>`**`/svn_startup.sh` starten und über **`<INSTALLVERZ>`**`/svn_shutdown.sh` stoppen.

> **Hinweis**
>
> Der Befehl `svn_shutdown.sh` funktioniert nur, wenn `svnserve` über `svn_startup.sh` gestartet worden ist.

> **Einschränkung**
>
> Falls der Subversion-Prozess vor der SP2-Patch-Installation läuft, funktioniert der Befehl `svn_shutdown.sh` nach der Installation des Patch nicht. Um Subversion neu zu starten, muss der Prozess `svnserve` manuell beendet und anschließend `svn_startup.sh` ausgeführt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

16.3 Erforderliche Dateien für Subversion unter Solaris 10 und RedHat Linux 5

Die folgenden Dateien sind erforderlich, um Subversion verwenden zu können.

> **Hinweis**
>
> Falls eine der folgenden ausführbaren Dateien vor der Installation der BI-Plattform 4.1 SP1 nicht vorhanden ist, muss der Benutzer den Befehl **<INSTALLVERZ>**/sap_bobj/lcm_installer.sh **<SUBVERSION_PASSWORT> <CMS_PASSWORT>** ausführen und anschließend den Adaptive Processing Server neu starten, damit die Versionsverwaltung korrekt funktioniert.

- Unter Solaris 10 müssen die Pakete `CSWlibiconv2` und `CSWlibgcc-s1` installiert werden, die die Dateien `libiconv.so.2` und `libgcc_s.so.1` enthalten.

  > **Nicht vergessen**
  >
  > Stellen Sie im Anschluss an die Installation dieser Pakete sicher, dass der Pfad zu den Bibliotheken in der Benutzer-Umgebungsvariablen `LD_LIBRARY_PATH` enthalten ist.

- Unter RedHat Linux 5 muss die Datei `libexpat.so.1` installiert werden.

16.4 Verwenden der Option „Versionsverwaltungseinstellungen“

Von der Central Management Console aus können Sie Einstellungen zum Versionsverwaltungssystem und den Subversion- und ClearCase-Parametern vornehmen.

1. Klicken Sie in der CMC auf **Anwendungen**.
2. Doppelklicken Sie auf **VMS**.
   Das Bild „Versionsverwaltungseinstellungen“ wird angezeigt.
3. Wählen Sie **VMS-Einstellungen**.
4. Wählen Sie in der Liste **Versionsverwaltungssysteme** das System **Subversion** aus.
   Die bei der Installation der Hochstufverwaltung eingegebene Portnummer, das Kennwort, der Repository-Name, der Servername, der Benutzername, der Name des Arbeitsbereichsverzeichnisses und der Pfad zum Installationsverzeichnis werden in den entsprechenden Feldern angezeigt.
5. Ändern Sie gegebenenfalls die Werte in den Feldern.

   > **Hinweis**
   >
   > Stellen Sie sicher, dass Sie den Installationspfad bis zur `.exe`-Datei eingeben.

   Unter Windows: **<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\Subversion

   Unter Unix: **<INSTALLVERZ>**/sap_bobj/enterprise_40/subversion/bin

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6. Wählen Sie **SVN**, **HTTP** oder **HTTPS**.

> **Hinweis**
>
> Weitere Informationen zu HTTPS-Verbindungen zu Subversion erhalten Sie in der *Apache Subversion Documentation*.

7. (Optional) Um Ihre VMS-Einstellungen zu überprüfen, klicken Sie auf **VMS testen**.
8. Klicken Sie auf **Speichern**.

> **Hinweis**
>
> - Wenn Sie Subversion als Standard-VMS festlegen möchten, wählen Sie **Als Standard-VMS verwenden**.
> - Wenn Sie Änderungen an Werten der Felder vorgenommen haben, starten Sie den Adaptive Processing Server neu.

16.4.1 Standardeinstellungen für das Versionsverwaltungssystem

Nach Neuinitialisierung des CMS werden alle Anwendungseinstellungen zurückgesetzt. Die Standardeinstellungen für das Versionsverwaltungssystem lauten:

Parameter	Wert
Servername	`localhost`
Server-Port	`3690`
Benutzername	`LCM`
Kennwort	Während der Installation eingegeben
Installationspfad	Unter Windows: `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\Subversion` Unter Unix: `<INSTALLVERZ>/sap_bobj/enterprise_xi40/subversion/bin`
Repository Name	Unter Windows: `svn_repository` Unter Unix: `LCM_repository`
Arbeitsbereichsverzeichnis	Unter Windows: `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\CheckOut` Unter Unix: `<INSTALLVERZ>/sap_bobj/enterprise_xi40/CheckOut`
Protokoll	`SVN`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

16.4.2 Einrichten des Versionsverwaltungssystems ClearCase in Windows

Führen Sie folgende Schritte aus, um das ClearCase-Versionsverwaltungssystem in Windows festzulegen:

1. Klicken Sie im Fenster *Verwaltungsoptionen* auf die Option **VMS-Einstellungen**.
2. Wählen Sie in der Dropdownliste **Versionsverwaltungssysteme** das System **ClearCase**.
3. Geben Sie folgende Informationen ein:
   - ClearCase-Laufwerk zuordnen – Geben Sie den Laufwerksnamen ein. Standardmäßig ist dies das Laufwerk "M". Beispiel: `M:`
   - VOB-Tag-Name – Geben Sie den Versioned Object Base-(VOB-)Namen ein. Beispiel: FreitagVB
   - Verzeichnis zur Ansichtsspeicherung – Geben Sie den Pfad zu dem freigegebenen Ordner ein. Beispiel: `\\Hostname\Ordnername`

   Hinweis

   Der Hostname darf nicht als "localhost" geschrieben werden.
4. Klicken Sie auf **Speichern**.
5. Um ClearCase als Standard-Versionsverwaltungssystem festzulegen, wählen Sie **Als Standard-VMS verwenden**.

16.4.3 Einrichten des Versionsverwaltungssystems ClearCase in Unix

Führen Sie folgende Schritte aus, um das ClearCase-Versionsverwaltungssystem in Unix festzulegen:

1. Klicken Sie im Fenster "Verwaltungsoptionen" auf die Option **VMS-Einstellungen**.
2. Wählen Sie in der Dropdownliste "Versionsverwaltungssysteme" das System **ClearCase**.
3. Geben Sie folgende Informationen ein:
   - ClearCase-Laufwerk zuordnen – Geben Sie den Namen des Ordners an, in dem das MVFS enthalten ist. Die Standardeinstellung ist `/view`.
   - VOB-Tag-Name – Geben Sie den VOB-Namen und den Ordner an, in dem das VOB enthalten ist. Beispiel: `VOB-Ordner/VOB-Name`
   - Verzeichnis zur Ansichtsspeicherung: Geben Sie den Pfad des Verzeichnisses ein, in dem die Ansichten erstellt werden.
4. Klicken Sie auf **Speichern**.
5. Um ClearCase als Standard-Versionsverwaltungssystem festzulegen, wählen Sie **Als Standard-VMS verwenden**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

16.5 Vergleichen von verschiedenen Versionen desselben Auftrags

Sie können die Unterschiede zwischen zwei Versionen desselben Auftrags anzeigen, indem Sie folgende Schritte ausführen:

1. Melden Sie sich bei der CMC-Anwendung an.
2. Wählen Sie auf der CMC-Startseite **Versionsverwaltung**.
3. Wählen Sie auf dem Bildschirm „Versionsverwaltung“ den Auftrag aus, dessen Versionen verwaltet werden sollen.
4. Klicken Sie auf **Verlauf**.
   Die Seite "Verlauf" wird geöffnet und zeigt alle Versionen des ausgewählten InfoObjects an.
5. Wählen Sie zwei zu vergleichende Versionen aus.
6. Klicken Sie auf **Vergleichen**.
   Der Vergleichsprozess wird gestartet. Die Unterschiede werden in Orange und die fehlenden Objekte werden in Rot hervorgehoben.
7. Klicken Sie auf **Speichern**, um den Vergleichsbericht zu speichern.

16.6 Aktualisieren von Subversion-Inhalten

Falls Sie über alte Subversion-Inhalte verfügen, die in einer früheren Version der BI-Plattform erstellt wurden, können Sie für diese Inhalte ein Upgrade auf die aktuelle Version durchführen:

1. Melden Sie sich auf dem Computer mit SAP BusinessObjects Enterprise 3.x am VMS an.
2. Checken Sie ein Objekt ein. Sie können beispielsweise das Administrator- und das Guest-Objekt zweimal einchecken.
3. Klicken Sie in der CMC auf **Benutzer**, und prüfen Sie, ob `2` in der VMS- und CMS-Versionsnummer angezeigt wird.
4. Melden Sie sich vom VMS ab.
5. Rufen Sie die Befehlszeileneingabe auf, navigieren Sie zu `C:\Programme\Subversion\bin`, und führen Sie den Export-Befehl aus: `svnadmin dump c:/LCM_repository/svn_repository > dumrepo`
6. Kopieren Sie die Datei `dumrepo` auf den BI-Plattform-Rechner.
7. Wechseln Sie in die Befehlszeileneingabe auf dem BI-Plattform-Rechner, navigieren zu `C:\Programme (x86)\SAP`, und führen Sie die folgenden Befehle aus:

   ```
   svnadmin.exe load "C:/Programme (x86)/SAP BusinessObjects/SAPBusinessObjects
   Enterprise XI 4.0/LCM_repository/svn_repository" < c:/dumrepo
   ```

   ```
   svnadmin.exe upgrade "C:/Programme (x86)/SAP BusinessObjects/SAP BusinessObjects
   Enterprise XI 4.0/LCM_repository/svn_repository"
   ```
8. Nachdem die Befehle erfolgreich ausgeführt wurden, starten Sie den SIA neu.
9. Melden Sie sich an der CMC an und klicken auf **Versionsverwaltung**.
10. Klicken Sie auf **Benutzer**, und überprüfen Sie, ob die VMS-Version `2` ist.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

11. Wählen Sie das Objekt **Administrator** aus, und klicken Sie anschließend auf **Aktuelle Version abrufen**.
12. Der VMS und der CMS haben nun dieselbe Versionsnummer.

16.7 Unterversionen für geclusterte Processing Job Server konfigurieren

16.7.1 Option A: Konfigurieren des Subversion-Hauptrechners, bevor das Versionsverwaltungssystem verwendet wird

1. Stellen Sie sicher, dass das Verzeichnis der Arbeitskopie unter `<INSTALLATIONSVERZEICHNIS>\CheckOut` noch nicht erstellt worden ist.
2. Erstellen Sie ein Verzeichnis für die Arbeitskopie-Dateien von Subversion und geben Sie es für andere Rechner mit Schreibzugriff frei.
3. Ändern Sie in der CMC bei den Einstellungen für das Versionsverwaltungssystem den **Servernamen** von `localhost` auf die Adresse Ihres Hauptrechners.
4. Ändern Sie das **Arbeitsbereichsverzeichnis** auf den Namen der Freigabe Ihrer Arbeitskopie, in folgendem Format: `\\<HOST-NAME>\<NAME DER FREIGABE>`
5. Halten Sie den Server Intelligence Agent (SIA) an, und wechseln Sie das Konto von LocalSystem auf den Betriebssystem-Administrator.

   > **Hinweis**
   >
   > Das Konto LocalSystem verfügt nicht über die Berechtigung zum Netzwerkzugriff auf das freigegebene Verzeichnis.

6. Starten Sie den SIA.

   > **Hinweis**
   >
   > Falls der SIA bereits von einem anderen Konto mit Netzwerkzugriff auf das freigegebene Verzeichnis aus gestartet wurde, müssen Sie nur alle Processing Job Server neu starten, die das VMS hosten, damit die Schritte 3 und 4 wirksam werden.

16.7.2 Option B: Konfigurieren von Subversion, nachdem das Versionsverwaltungssystem das Verzeichnis der Arbeitskopie erstellt hat

1. Stellen Sie sicher, dass Subversion als Teil der BI-Plattform installiert worden ist.
2. Geben Sie das Verzeichnis der Arbeitskopie frei, das sich unter `<INSTALLATIONSVERZEICHNIS>\CheckOut` befindet, und vergeben Sie Leserechte für andere Rechner.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Richten Sie den Namen des Arbeitsbereichs auf eine der folgenden Arten ein:
   - Führen Sie einen VMS-Vorgang (Versionsverwaltungssystem) auf dem Hauptrechner aus. Öffnen Sie dann das Verzeichnis der Arbeitskopie von Subversion, um den Namen des Arbeitsbereichs herauszufinden.
   - Ermitteln Sie den Namen, indem Sie das @ entfernen und alle Doppelpunkte durch das Zeichen *B* ersetzen. Wenn beispielsweise das Cluster den Namen `ABCD-LCM:6400` hat, wird das VMS den Arbeitsbereich-Namen `ABCD-LCMB6400` verwenden.

> **Hinweis**
>
> Subversion speichert sein Repository im Verzeichnis der Arbeitskopie.

4. Ändern Sie die Standard-URL von **`localhost`** auf eine URL, die beliebige Rechner aufrufen können. Verwenden Sie dazu folgenden Befehl:

```
svn switch --relocate svn://localhost:3690/svn_repository svn://<SUBVERSION-
RECHNER>:3690/svn_repository \\<SUBVERSION-FREIGABE>\CheckOut\<ARBEITSBEREICH-
NAME>-LCMB6400\WORKSPACE
```

5. Geben Sie bei Aufforderung das Kennwort des Betriebssystem-Administrators ein, den Benutzernamen und dessen Kennwort.

> **Hinweis**
>
> Der Standard-Benutzername lautet LCM, und das Kennwort wurde während der Installation ausgewählt.

6. Ändern Sie in der CMC bei den Einstellungen für das Versionsverwaltungssystem den **Servernamen** von **`localhost`** auf die Adresse Ihres Hauptrechners.
7. Ändern Sie das **Arbeitsbereichsverzeichnis** von **`localhost`** auf den Namen der Freigabe Ihrer Arbeitskopie: `\\<SUBVERSION-FREIGABE>\CheckOut`
8. Halten Sie den Server Intelligence Agent (SIA) an, und wechseln Sie das Konto von LocalSystem auf den Betriebssystem-Administrator.
9. Starten Sie den SIA.

> **Hinweis**
>
> Falls der SIA bereits von einem anderen Konto mit Netzwerkzugriff auf das freigegebene Verzeichnis aus gestartet wurde, müssen Sie nur alle Processing Job Server neu starten, die das VMS hosten.

16.7.3 Konfigurieren anderer Subversion-Rechner

Um andere Subversion-Rechner zu konfigurieren, stoppen Sie den Server Intelligence Agent (SIA) und wechseln Sie das Konto von LocalSystem auf den ein Konto mit Netzwerkzugriffsrechten, damit der Processing Job Server auf das freigegebene Verzeichnis zugreifen kann (z. B. das Konto des Betriebssystem-Administrators). Starten Sie danach den SIA neu.

> **Hinweis**
>
> Falls der SIA bereits von einem anderen Konto mit Netzwerkzugriff auf das freigegebene Verzeichnis aus gestartet wurde, müssen Sie nur alle Processing Job Server neu starten, die das VMS hosten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

16.8 Zugriff auf dieselbe ClearCase-Sicht von verschiedenen Versionsverwaltungsservern aus

1. Richten Sie den ClearCase-Hauptrechner ein.

   Auf diesem Rechner werden die internen Dateien und Metadaten für ClearCase verwaltet. Andere Rechner werden sich mit diesem Rechner verbinden.

2. Richten Sie den ClearCase-Slave-Rechner ein.

   Dieser Rechner dient zum Herstellen einer Verbindung und der Freigabe der Sichten des ClearCase-Hauptrechners.

   > **Nicht vergessen**
   >
   > Installieren Sie zusammen mit den ClearCase-Paketen keine Server-Komponenten, wie den Versioned Object Base (VOB) Server oder den View Server.

3. Fügen Sie den Namen des ClearCase-Rechners hinzu, um ihn als Registry-Server zu verwenden.
4. Überspringen Sie die Schritte im Abschnitt "VOB erstellen". Starten Sie die Hauptsicht lokal, und stellen Sie VOB bereit.
   a) Richten Sie den Namen des Arbeitsbereichs auf eine der folgenden Arten ein:
      - Führen Sie einen VMS-Vorgang (Versionsverwaltungssystem) auf dem Hauptrechner aus. Öffnen Sie dann das Verzeichnis der Arbeitskopie von Subversion, um den Namen des Arbeitsbereichs herauszufinden.
      - Ermitteln Sie den Namen, indem Sie das @ entfernen und alle Doppelpunkte durch das Zeichen *B* ersetzen. Wenn beispielsweise das Cluster den Namen `ABCD-LCM:6400` hat, wird das VMS den Arbeitsbereich-Namen `ABCD-LCMB6400` verwenden.

   b) Starten Sie die Sicht lokal über folgenden Befehl: **`cleartool startview <NAME_DER_SICHT>`**
      Die Sicht öffnet sich auf dem ClearCase-Slave-Rechner.
   c) Stellen Sie VOB über folgenden Befehl bereit: **`cleartool mount \<VOB_TAG>`**

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

17 Grafischer Vergleich

17.1 Grafischer Vergleich in der Hochstufverwaltung

Mit dem grafischen Vergleich können Sie die Unterschiede zwischen zwei Versionen eines unterstützten Dateityps (LCMBIAR) oder Objekttyps (LCM-Auftrag) oder beiden anzeigen. Mit dieser Funktion können Sie Unterschiede zwischen Dateien oder Objekten ermitteln, um verschiedene Berichtstypen zu entwickeln und zu pflegen. Diese Funktion liefert einen Vergleichsstatus für Quell- und Zielversion. Wenn z. B. eine frühere Version des Benutzerberichts genau ist und die aktuelle Version ungenau, können Sie die Dateien vergleichen und analysieren, um das konkrete Problem zu ermitteln.

> **Hinweis**
>
> Um den grafischen Vergleich verwenden zu können, müssen Sie Adobe Flash Viewer installieren.

Im Folgenden sind drei Arten des grafischen Vergleichs dargestellt, aus dem Sie die Datei oder ein Objekt ermitteln können:

- Entfernt - Wenn in einem Bericht in einer der Dateiversionen ein Element fehlt, wird die Art des Unterschieds als "Entfernt" dargestellt. Das Element könnte z.B. eine Zeile, ein Abschnitt oder sogar ein Block sein.
- Geändert - Wenn sich in einem Bericht Werte der Quell- und der Zielversion unterscheiden, wird die Art des Unterschieds als "Geändert" angezeigt. Der Wert könnte z.B. der Zelleninhalt oder das Ergebnis einer lokalen Variable sein.
- Eingefügt - Wenn in einem Bericht ein Element in der Zielversion vorhanden ist, das in der Quellversion nicht vorhanden ist, wird die Art des Unterschieds als "Eingefügt" angezeigt.

Folgende Objekttypen unterstützen grafische Vergleiche:

- LCMBIAR
- Hochstufverwaltungsauftrag

Sie können folgende Kombinationen vergleichen:

- einen Hochstufverwaltungsauftrag mit einem anderen Hochstufverwaltungsauftrag
- einen Hochstufverwaltungsauftrag mit einer LCMBIAR-Datei
- eine LCMBIAR-Datei mit einer anderen LCMBIAR-Datei
- eine LCMBIAR-Datei mit einem Hochstufverwaltungsauftrag

Einstellungen

Auf der Startseite des grafischen Vergleichs können Sie Einstellungen wie z. B. Produktgebietsschema, bevorzugtes Anzeigegebietsschema, maximale Anzahl von Objekten pro Seite, Zeitzone und Eingabeaufforderung für ungespeicherte Daten festlegen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Startseite

Die Startseite des grafischen Vergleichs besteht aus folgenden Registerkarten und Bereichen:

- "Neuer Vergleich" - Mit dieser Registerkarte können Sie neue Vergleiche von Objekten erstellen.
- "Nach Vergleichen suchen" - Mit diesem Feld können Sie nach bereits verglichenen Objekten suchen.
- Bereich "Vergleiche" - In diesem Bereich sind die Registerkarten für Filter und Unterschiede aufgelistet
- "Vergleiche": Bereich "Unterschiede" - In diesem Bereich werden die verglichenen Objekte mit Name, Datum und Uhrzeit des Vergleichs sowie den Status der Unterschiede aufgelistet.

17.1.1 Vergleich von Objekten oder Dateien mittels des Grafischen Vergleichs

Mit der Option des Grafischen Vergleichs können Sie die BIAR-Dateien und Objekte vergleichen.

Um den Grafischen Vergleich von Dateien durchzuführen, gehen Sie folgendermaßen vor:

1. Melden Sie sich bei der CMC-Anwendung an.
2. Klicken Sie auf der CMC-Startseite auf der Registerkarte *Verwalten* auf die Verknüpfung **Grafischer Vergleich**.
   Die Seite "Grafischer Vergleich" wird angezeigt. Die verglichenen Dateien werden im Ordner "Unterschiede" oder in einem der vom Benutzer erstellten Unterordner abgelegt.

   > **Hinweis**
   >
   > Zum Erstellen eines neuen Unterordners klicken Sie auf das Ordnersymbol.

3. Klicken Sie auf **Neuer Vergleich**.
   Der Bildschirm *Vergleiche* wird angezeigt.
4. Wählen Sie das Referenzsystem über **System auswählen** unter "Referenz" aus.
   Sie können eine Verbindung zu einem der folgenden Referenzsysteme herstellen:
   - CMS
   - VMS
   - Lokales Dateisystem
5. Klicken Sie auf **Durchsuchen**, um ein Objekt oder eine Datei im lokalen System für den Vergleich auszuwählen.
6. Wählen Sie das Zielsystem aus **System auswählen** unter "Ziel" aus.
   Sie können eine Verbindung zu einem der folgenden Referenzsysteme herstellen:
   - CMS
   - VMS
   - Lokales Dateisystem

   > **Hinweis**
   >
   > Wenn Sie sich am CMS oder VMS anmelden, kann das im Referenzsystem ausgewählte Objekt auch automatisch mit einem Objekt gleichen Namens im Referenzsystem verglichen werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7. Klicken Sie auf **Durchsuchen**, um ein Objekt oder einen Auftrag im lokalen System für den Vergleich auszuwählen.
8. Klicken Sie auf **Hinzufügen**.
   Die für den Vergleich ausgewählten Objekte werden in den Einkaufswagen aufgenommen.

   Wenn mehr als ein Objektpaar in den Einkaufswagen aufgenommen wird, können die Objekte zu einem späteren Zeitpunkt für den Vergleich eingeplant werden. Wenn der Einkaufswagen nur ein Objektpaar enthält, können Sie diese Objekte jedoch vergleichen.

   Fahren Sie mit dem nächsten Schritt fort, um die Dateien zu vergleichen. Um den Vergleich zeitgesteuert zu verarbeiten, siehe *Zeitgesteuerte Verarbeitung des Vergleichs* [Seite 592]
9. Klicken Sie auf **Vergleichen**, um die Objekte bzw. Ordner zu vergleichen.

   > **Hinweis**
   >
   > Zum Vergleich der Auftragsdatei LCMBIAR/Hochstufverwaltung gehören:
   >
   > - LCMBIAR-Metadaten: Vergleich der Auftragsdetails wie Name, Erstellt von, Uhrzeit.
   > - Primäre Objekte: Vergleich aller explizit in LCMBIAR ausgewählten Objekte mit den gleichen Objekten in der LCMBIAR-Zieldatei nach CUID.
   > - Abhängige Objekte: Vergleich des in der Datei ausgewählten abhängigen Objekts mit einen gleichen Objekt in der Zeildatei nach CUID.
   >
   > Wenn andere Objekte als LCMBIAR oder ein Hochstufverwaltungs-Auftrag ausgewählt werden, wird die folgende Fehlermeldung angezeigt: `Plugin nicht gefunden.`

   Der Vergleichsprozess wird sofort gestartet, und die Unterschiede werden ggf. im Viewer des *Grafischen Vergleichs* angezeigt. Die Unterschiede werden in Orange hervorgehoben, und die fehlenden Objekte sind rot markiert.

   Um die verglichenen Objekte nach Typ und mit Unterschieden oder gemeinsamen Attributen anzuzeigen, können Sie auch die Filteroption verwenden.
10. Klicken Sie auf **Speichern**, um den Vergleichsbericht zu speichern.
11. Geben Sie den Speicherort an, an dem Sie den Bericht speichern möchten, und klicken Sie auf **OK**.

17.1.2 Vergleichen von Objekten oder Dateien mithilfe des Versionsverwaltungssystems

Sie können Aufträge oder Ordner der Hochstufverwaltung in einem Versionsverwaltungssystem anhand der Option "Grafischer Vergleich" vergleichen.

Führen Sie die folgenden Schritte aus, um Objekte in einem Versionsverwaltungssystem zu vergleichen:

1. Melden Sie sich an der CMC an.
2. Klicken Sie auf der CMC-Startseite auf der Registerkarte *Verwalten* auf die Verknüpfung **Grafischer Vergleich**.

   Die Seite "Grafischer Vergleich" wird angezeigt. Die verglichenen Dateien werden im Ordner "Unterschiede" oder in einem der vom Benutzer erstellten Unterordner abgelegt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Zum Erstellen eines neuen Unterordners klicken Sie auf das Ordnersymbol.

3. Klicken Sie auf **Neuer Vergleich**.

   Der Bildschirm *Vergleiche* wird angezeigt.
4. Wählen Sie **Anmeldung am VMS** aus **System auswählen** unter "Referenz" aus.
5. Geben Sie die Anmeldedaten für den VMS ein, und klicken Sie auf **Anmelden**.

   Das Dialogfeld *Grafischer Vergleich - Zielsystem automatisch auswählen* wird angezeigt.
6. Klicken Sie auf **Nein**, um ein anderes Zielsystem festzulegen, oder auf **Ja**, wenn das Zielsystem das Referenzsystem sein soll.
7. Klicken Sie auf **Durchsuchen**, um im Referenz- und im Zielsystem Objekte und Aufträge auszuwählen, die Sie vergleichen möchten.
8. Klicken Sie auf **Hinzufügen**.

   Die für den Vergleich ausgewählten Objekte werden im Bereich *Neuer Vergleich* aufgelistet.

   Sie können die Dateien sofort vergleichen oder den Vergleich zu einem späteren Zeitpunkt zeitgesteuert verarbeiten. Fahren Sie mit dem nächsten Schritt fort, um die Dateien zu vergleichen. Um den Vergleich zeitgesteuert zu verarbeiten, siehe *Zeitgesteuerte Verarbeitung des Vergleichs* [Seite 592]
9. Klicken Sie auf **Vergleichen**, um Aufträge bzw. Ordner zu vergleichen.

   Der Vergleichsprozess wird sofort gestartet, und die Unterschiede werden ggf. im Viewer des *Grafischen Vergleichs* angezeigt. Die Unterschiede werden in Orange hervorgehoben, und die fehlenden Objekte sind rot markiert.

   Um die verglichenen Objekte nach Typ und mit Unterschieden oder gemeinsamen Attributen anzuzeigen, können Sie auch die Filteroption verwenden.
10. Klicken Sie auf **Speichern**, um den Vergleichsbericht zu speichern.
11. Geben Sie den Speicherort an, an dem Sie den Bericht speichern möchten, und klicken Sie auf **OK**.

17.1.3 Zeitgesteuerte Verarbeitung des Vergleichs

Um den Vergleich von Dateien oder Objekten zeitgesteuert zu verarbeiten, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf **Zeitgesteuert verarbeiten**.
   Das Fenster *Grafischer Vergleich – Zeitgesteuert verarbeiten* wird angezeigt.
2. Wählen Sie die Frequenz für die zeitgesteuerte Verarbeitung des Vergleichs aus der Liste **Vergleich ausführen** aus.
3. Geben Sie die Anzahl und das Intervall der zulässigen Neuversuche in den entsprechenden Feldern an.

   > **Hinweis**
   >
   > Sie können das Intervall nur festlegen, wenn Sie die Anzahl der Neuversuche festgelegt haben.

4. Geben Sie den Berichtsnamen an, und klicken Sie auf **Durchsuchen**, um den Speicherort für den Bericht zu finden.
   Das Fenster *Auftrag speichern in* wird angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

5. Wählen Sie den Ordner, in dem Sie den Bericht ablegen möchten, und klicken Sie auf **OK**.

> **Hinweis**
>
> Abhängig von der Option, die Sie in der Liste **Vergleich ausführen** auswählen, müssen Sie das Datum und/oder die Uhrzeit für den Vergleich festlegen.

6. Klicken Sie auf **Zeitgesteuert verarbeiten**.

   Der Benutzer kann das Vergleichsobjekt oder den Vergleichsbericht zu einem späteren Zeitpunkt im Viewer des Grafischen Vergleichs anzeigen. Die Seite *Verglichen: Unterschiede* wird mit einer Liste von Ordnern und Dateien oder Vergleichsberichten angezeigt.

   Die Seite "Verglichen: Unterschiede" enthält darüber hinaus die folgenden Optionen:

   - **Verlauf** – Mittels dieser Option können Sie den Verlauf des Vergleichs anzeigen.
   - **Erneut ausführen** – Mittels dieser Option wird der Vergleich nochmals ausgeführt.
   - **Zeitgesteuert verarbeiten** – Mittels dieser Option können Sie den Vergleich zeitlich einplanen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18 Verwalten von Anwendungen

18.1 Verwalten von Anwendungen über die CMC

18.1.1 Übersicht

Im Verwaltungsbereich *Anwendungen* der CMC können Sie die Darstellung und Funktionalität von Webanwendungen wie CMC und BI-Launchpad ohne Programmieraufwand ändern. Sie können auch den Zugriff auf Anwendungen für Benutzer, Gruppen und Administratoren ändern, indem Sie die jeweils zugewiesenen Rechte bearbeiten.

In diesem Abschnitt finden Sie Kontextinformationen, Verfahren und Anleitungen zur Verwaltung verschiedener Einstellungen. Die folgenden Anwendungen haben Einstellungen, die über die CMC geändert werden können:

- Analysis, Edition für OLAP
- Warnungsanwendung
- BI-Launchpad
- BI-Arbeitsbereiche
- Central Management Console
- Zusammenarbeit (mit SAP Jam oder SAP StreamWork)
- Crystal-Reports-Konfiguration
- Dashboards
- Diskussionsforum
- Information Designer
- Überwachungstool
- Multitenancy
- OpenDocument
- Plattformsuchanwendung
- Hochstufverwaltung
- Berichtskonvertierungstool
- SAP BusinessObjects Mobile
- Übersetzungsmanagement-Tool
- Universe-Design-Tool
- Upgrade-Management-Tool
- Grafischer Vergleich
- Web Intelligence
- Webdienst
- Widgets

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18.1.2 Gemeinsame Einstellungen für Anwendungen

18.1.2.1 Festlegen von Benutzerrechten für Anwendungen

Sie können mithilfe von Rechten den Benutzerzugriff auf bestimmte Funktionen in Anwendungen steuern. Im Bereich *Anwendungen* der CMC können Sie Prinzipale zu der Zugriffskontrollliste für eine Anwendung zuordnen, die Rechte eines Prinzipals anzeigen und die Rechte, die der Prinzipal für eine Anwendung hat, ändern. Weitere Informationen über die Verwaltung von Rechten finden Sie im *Administratorhandbuch für SAP BI*.

18.1.2.2 Einstellen der Ablaufverfolgungsprotokollierungsebene der Webanwendung in der CMC

Um andere Webanwendungen zu verfolgen, müssen Sie die entsprechende `BO_trace.ini`-Datei manuell konfigurieren.

1. Klicken Sie im Bereich *Anwendungen* der CMC mit der rechten Maustaste auf eine Anwendung und wählen **Ablaufverfolgungsprotokoll-Einstellungen**.

   > **Hinweis**
   >
   > Diese Anwendungen verfügen über Ablaufverfolgungsprotokoll-Einstellungen: BI-Launchpad, CMC, Open Document, Hochstufverwaltung, Versionsverwaltung, Grafischer Vergleich und Webdienst.

   Das Dialogfeld *Ablaufverfolgungsprotokoll-Einstellungen* wird angezeigt.
2. Wählen Sie in der Liste **Protokollierungsebene** eine Einstellung aus.
3. Klicken Sie auf **Speichern und schließen**.

Die neue Ablaufverfolgungsprotokollierungsebene wird nach der nächsten Anmeldung an der Webanwendung wirksam.

Weitere Informationen

Ablaufverfolgungsprotokollierungsebenen [Seite 595]

18.1.2.2.1 Ablaufverfolgungsprotokollierungsebenen

Folgende Ablaufverfolgungsprotokollierungsebenen stehen für BI-Plattform-Komponenten zur Verfügung:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ebene	Beschreibung
Nicht angegeben	Die Ablaufverfolgungsprotokollierungsebene wird über einen anderen Mechanismus angegeben (normalerweise eine `.ini`-Datei).
Keine	Es erfolgt keine Ablaufverfolgung.
Niedrig	Der Filter für die Ablaufverfolgungsprotokollierung ermöglicht die Protokollierung von Fehlermeldungen, während Warn- und Statusmeldungen ignoriert werden. Wichtige Statusmeldungen werden für Meldungen für Start, Herunterfahren, Start- und Endanforderung für Komponenten protokolliert. Diese Ebene wird für Debuggingzwecke nicht empfohlen.
Mittel	Der Ablaufverfolgungsprotokollfilter ist so eingestellt, dass Fehler-, Warn- und die meisten Statusmeldungen berücksichtigt werden. Weniger wichtige oder sehr umfangreiche Statusmeldungen werden herausgefiltert. Diese Ebene ist nicht ausreichend ausführlich für das Debugging.
Hoch	Es werden keine Meldungen gefiltert. Diese Ebene wird für Debuggingzwecke empfohlen. **Achtung** Diese Ablaufverfolgungsprotokollierungsebene wirkt sich in hohem Maße auf die Systemressourcen aus, indem die Prozessorauslastung erhöht und mehr Speicherplatz belegt wird.

18.1.3 Anwendungsspezifische Einstellungen

18.1.3.1 Verwalten von CMC-Anwendungseinstellungen

18.1.3.1.1 Authentifizierung und Programmobjekte

Sie können die zum Ausführen von Programmobjekten erforderlichen Informationen konfigurieren, und Sie können steuern, welche Arten von Programmobjekten von Benutzern ausgeführt werden können.

Beachten Sie die mit dem Hinzufügen von Programmobjekten zum Repository verbundenen potenziellen Sicherheitsrisiken. Für das Konto, unter dem das Programmobjekt ausgeführt wird, wird anhand der Ebene der Dateiberechtigungen bestimmt, ob durch das Programm überhaupt Änderungen an Dateien vorgenommen werden können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Aktivieren und Deaktivieren bestimmter Arten von Programmobjekten

Als erste Sicherheitsmaßnahme können Sie konfigurieren, welche Arten von Programmobjekten verwendet werden können.

Authentifizierung auf allen Plattformen

Im Verwaltungsbereich *Ordner* der CMC geben Sie die Anmeldedaten für das Konto an, unter dem das Programm ausgeführt wird. Mit dieser Funktion können Sie ein spezifisches Benutzerkonto für das Programm einrichten und ihm die entsprechenden Berechtigungen zuweisen, damit das Programmobjekt unter diesem Konto ausgeführt werden kann.

Benutzer, die den Informationsplattformdiensten Programmobjekte hinzufügen, können einem Programmobjekt auch ihre eigenen Anmeldedaten zuweisen, um dem Programm Zugriff auf das System zu gewähren. Das Programm wird dann unter diesem Benutzerkonto ausgeführt, wobei die Berechtigungen des Programms auf die des Benutzers begrenzt sind. Wenn Sie kein Benutzerkonto für ein Programmobjekt angeben, wird es unter dem Standardsystemkonto ausgeführt, das im Allgemeinen mit lokalen, aber nicht mit Netzwerkberechtigungen ausgestattet ist.

> **Hinweis**
>
> In der Standardeinstellung treten nach der zeitgesteuerten Verarbeitung eines Programmobjekts Fehler bei der Ausführung von Aufträgen auf, wenn keine Anmeldedaten angegeben wurden. Um Standardanmeldedaten anzugeben, wählen Sie **CMC** im Verwaltungsbereich *Anwendungen*. Klicken Sie im Menü **Aktionen** auf **Programmobjektrechte**. Klicken Sie auf **Mit den folgenden Anmeldedaten für das Betriebssystem einplanen**, und geben Sie einen Standardbenutzernamen und ein Standardkennwort ein.

Authentifizierung für Java-Programme

In den Informationsplattformdiensten können Sie Sicherheitseinstellungen für alle Programmobjekte vornehmen. Bei Java-Programmen erzwingen die Informationsplattformdienste die Verwendung einer Java-Richtliniendatei (Java Policy File), deren Standardeinstellung mit der Java-Standardeinstellung für unsicheren Code übereinstimmt. Verwenden Sie nach Bedarf das (mit dem Java Development Kit erhältliche) Java Policy Tool zum Ändern der Java-Richtliniendatei.

Das Java Policy Tool enthält zwei Basiseinträge für Code. Der erste Eintrag verweist auf das SAP-BusinessObjects-Enterprise-Java-SDK und gewährt Programmobjekten vollständige Berechtigungen für alle SAP-BusinessObjects-Enterprise-JAR-Dateien. Der zweite Basiseintrag für Code gilt für alle lokalen Dateien. Für unsicheren Code werden die gleichen Sicherheitseinstellungen wie beim Java-Standard für unsicheren Code verwendet.

> **Hinweis**
>
> Die Einstellungen für die Java-Richtlinie gelten universell für alle Program Job Server, die auf demselben Rechner ausgeführt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Die Java-Richtliniendatei wird standardmäßig im Root-Verzeichnis der Informationsplattformdienste-Installation im Java-SDK-Verzeichnis installiert. Ein typischer Speicherort unter Windows ist z. B.: `C:\Programme\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\conf\crystal-program.policy`

18.1.3.1.1.1 Aktivieren und Deaktivieren bestimmter Programmobjekttypen

1. Wählen Sie im Bereich *Anwendungen* die Option **Central Management Console** aus.
2. Klicken Sie auf **Aktionen** > **Programmobjektrechte**.
   Das Dialogfeld *Programmobjektrechte* wird angezeigt.
3. Wählen Sie im Bereich *Benutzer dürfen* die Programmobjekttypen aus, die von den Benutzern ausgeführt werden dürfen.

   Sie können **Skritpte/Binärdateien ausführen** oder **Java-Programme ausführen** auswählen.

   Wenn Sie **Java-Programme ausführen** ausgewählt haben, können Sie das Kontrollkästchen **Identitätsmaskierung verwenden** aktivieren oder deaktivieren. Durch diese Option wird dem Java-Programm ein Token bereitgestellt, mit dem es sich bei den Informationsplattformdiensten anmelden kann.
4. Klicken Sie auf **Speichern und schließen**.

18.1.3.1.2 Registrieren von Verarbeitungserweiterungen im System

> **Hinweis**
>
> Diese Funktion kann nicht für Web Intelligence-Dokumente verwendet werden.

Damit Ihre Verarbeitungserweiterungen einzelnen Objekten zugewiesen werden können, müssen Sie zunächst die Codebibliothek auf allen Rechnern bereitstellen, auf denen die jeweiligen Zeitsteuerungs- oder Anzeigeanforderungen verarbeitet werden. Bei der Installation der BI-Plattform wird auf jedem Job Server, Processing Server und Report Application Server (RAS) ein Standardverzeichnis für Verarbeitungserweiterungen angelegt. Es empfiehlt sich, eigene Verarbeitungserweiterungen in die Standardverzeichnisse auf den einzelnen Servern zu kopieren. Unter Windows lautet das Standardverzeichnis `C:\Programme\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86\ProcessExt`. Unter UNIX heißt das Verzeichnis `sap_bobj/ProcessExt`.

> **Tipp**
>
> Die Dateien für Verarbeitungserweiterungen können auch von mehreren Servern aus genutzt werden.

Kopieren Sie die Erweiterungen je nach enthaltenem Funktionsumfang auf die folgenden Rechner:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Bei Verarbeitungserweiterungen, die ausschließlich Zeitsteuerungsanforderungen abfangen, ist die Bibliothek auf jeden Rechner zu kopieren, der als Adaptive Job Server betrieben wird.
- Bei Verarbeitungserweiterungen, die ausschließlich Anzeigeanforderungen abfangen, ist die Bibliothek auf jeden Rechner zu kopieren, der als Crystal Reports Processing Server oder RAS ausgeführt wird.
- Bei Verarbeitungserweiterungen, die Zeitsteuerungs- und Anzeigeanforderungen abfangen, ist die Bibliothek auf jeden Rechner zu kopieren, der als Adaptive Job Server, Crystal Reports Processing Server oder RAS ausgeführt wird.

> **Hinweis**
>
> Wenn die Verarbeitungserweiterung nur für Zeitsteuerungs- oder Anzeigeanforderungen an eine bestimmte Servergruppe benötigt wird, genügt es, die Bibliothek auf die einzelnen Verarbeitungsserver in der Gruppe zu kopieren.

18.1.3.1.2.1 So registrieren Sie eine Verarbeitungserweiterung im System

1. Wechseln Sie in den Verwaltungsbereich *Anwendungen* der CMC.
2. Wählen Sie **Central Management Console**.
3. Klicken Sie auf **Aktionen** > **Verarbeitungserweiterungen**.
   Das Dialogfeld *Verarbeitungserweiterungen: CMC* wird angezeigt.
4. Geben Sie im Feld **Name** einen Anzeigenamen für die Verarbeitungserweiterung ein.
5. Tragen Sie im Feld **Speicherort** den Dateinamen Ihrer Verarbeitungserweiterung sowie ggf. zusätzliche Pfadangaben ein.
   - Wenn Sie Ihre Verarbeitungserweiterung in das Standardverzeichnis auf den einzelnen Rechnern kopiert haben, brauchen Sie nur den Dateinamen (ohne Erweiterung) einzugeben.
   - Wenn Sie eine Verarbeitungserweiterung in einen Unterordner unterhalb des Standardverzeichnisses kopiert haben, geben Sie den Speicherort wie folgt ein:: `<Unterordner>/<Dateiname>`
6. Im Feld **Beschreibung** können Sie weitere Angaben zur Verarbeitungserweiterung eintragen.
7. Klicken Sie auf **Hinzufügen**.

   > **Tipp**
   >
   > Um eine Verarbeitungserweiterung zu löschen, wählen Sie sie aus der Liste **Vorhandene Erweiterungen** aus und klicken auf **Löschen**. (Sorgen Sie dafür, dass auf dieser Verarbeitungserweiterung keine wiederkehrenden Jobs basieren, weil zukünftige, auf dieser Verarbeitungserweiterung basierende Jobs fehlschlagen müssen.)

8. Klicken Sie auf **Speichern und schließen**.
   Die Verarbeitungserweiterung wird bei der CMC registriert.

Sie können diese Verarbeitungserweiterung jetzt auswählen und ihre Logik bestimmten Objekten zuweisen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18.1.3.1.2.2 Nutzen von Verarbeitungserweiterungen von mehreren Servern aus

> **Hinweis**
>
> Diese Funktion ist nicht auf Web Intelligence-Dokumente oder in SAP Crystal Reports für Enterprise erstellte Berichte anwendbar.

Die Verarbeitungserweiterungen müssen sich nicht unbedingt im Standardverzeichnis der einzelnen Adaptive Job Server, Crystal Reports Processing Server und RAS befinden, sondern können auch alle am selben Speicherort abgelegt werden. Kopieren Sie zunächst Ihre Verarbeitungserweiterungen in ein im Netzwerk freigegebenes Verzeichnis, auf das alle Job Server und Page Server Zugriff haben. Ordnen Sie das Netzwerklaufwerk aller Server-Rechner zu (bzw. melden Sie es in UNIX an).

> **Hinweis**
>
> Zugeordnete Laufwerke unter Windows sind nur gültig, bis Sie Ihren Rechner neu starten.

Wenn in Ihrem Netzwerk Windows- und UNIX-Server parallel eingesetzt werden, müssen Sie für jede Verarbeitungserweiterung eine .dll-Datei und eine .so-Datei in das freigegebene Verzeichnis kopieren. Außerdem muss das im Netzwerk freigegebene Verzeichnis für Windows- und UNIX-Rechner sichtbar sein (über Samba oder eine andere Software für die gemeinsame Dateinutzung).

Anschließend ändern Sie auf jedem Server das Standardverzeichnis für die Verarbeitungserweiterungen in der Befehlszeile. Um die Befehlszeile zu ändern, navigieren Sie in der CMC zur Registerkarte "Server", wählen Sie einen Server und öffnen die Seite "Eigenschaften". Fügen Sie `-report_ProcessExtPath` **`<Absoluter Pfad>`** zur Befehlszeile hinzu. Tragen Sie für **`<<absoluter Pfad>>`** den Pfad des neuen Ordners ein. Verwenden Sie dabei das unter dem Betriebssystem des jeweiligen Servers übliche Format (z.B. `M:\code\extensions`, `/home/shared/code/extensions` usw.).

Um das Standardverzeichnis für Verarbeitungserweiterungen zu ändern, stoppen Sie den Server mithilfe der CMC. Öffnen Sie die Eigenschaften des Servers, und ändern Sie hier die Befehlszeile. Starten Sie den Server anschließend neu.

18.1.3.1.3 Verwalten des CMC-Registerkartenzugriffs

18.1.3.1.3.1 Delegierte(r) Verwaltung und Zugriff auf CMC-Registerkarten

In der Regel verwaltet der Administrator eines BI-Plattformsystems eine große Anzahl von Dokumenten, Ordnern, Benutzern, Servern und anderen Objekten. Jedoch können große Unternehmensumgebungen die Kapazitäten eines einzelnen Administrators überfordern. Ein Systemadministrator, der sich nur auf Aufgaben mit hoher Priorität konzentrieren möchte, kann delegierte Administratoren erstellen und ihnen Teile von Verwaltungsaufgaben zuweisen (z.B. Verwaltung einer Abteilung oder von Tenant-Inhalten). Im Gegensatz zu Systemadministratoren können delegierte Administratoren nur bestimmte Aufgaben ausführen und haben weniger Berechtigungen für Objekte im System.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Die Standardkonfiguration der Central Management Console ermöglicht Benutzern den Zugriff auf alle verfügbaren CMC-Registerkarten. Der Systemadministrator kann den Zugriff auf CMC-Registerkarten verwalten, um festzulegen, welche Registerkarten den Prinzipalen (Benutzern oder Benutzergruppen) angezeigt werden. Zur Optimierung der Benutzererfahrung und des Workflows des delegierten Administrators kann der Systemadministrator die CMC-Registerkarten ausblenden, die er wahrscheinlich nicht verwenden wird.

> **Achtung**
>
> Die Verwaltung des Zugriffs auf CMC-Registerkarten wirkt sich nur auf die grafische Darstellung der CMC-Benutzeroberfläche aus. Das Ausblenden von CMC-Registerkarten ist keine Sicherheitsmaßnahme, da dadurch keine Sicherheitsberechtigungen für Objekte innerhalb der Registerkarten festgelegt oder geändert werden. Um sicherzustellen, dass Benutzer keine nicht autorisierten Vorgänge für nicht autorisierte Objekte (z.B. Verwalten von Servern über den Central Configuration Manager oder Drittanbieter-Software basierend auf dem BI-Plattform-SDK) ausführen können, müssen Sie die entsprechenden Sicherheitsberechtigungen für Objekte (wie Serverobjekte) festlegen.

Weitere Informationen

Verwalten des Zugriffs auf CMC-Registerkarten für andere Benutzer [Seite 602]
Verwalten von Rechten zur Konfiguration des Zugriffs auf die Registerkarte "CMC" für andere Benutzer oder Benutzergruppen [Seite 605]

18.1.3.1.3.2 Arbeiten mit dem CMC-Registerkartenzugriff

18.1.3.1.3.2.1 Verwalten des Zugriffs auf CMC-Registerkarten für andere Benutzer

Systemadministratoren haben immer Zugriff auf alle CMC-Registerkarten. Halten Sie sich zur Verwaltung von CMC-Registerkarten, auf die Prinzipale Zugriff haben, an die folgenden Richtlinien:

- Für einen vereinfachten Verwaltungsprozess und einen verringerten Wartungs- und Fehlerbehebungsaufwand sollten die Administratoren den Zugriff auf CMC-Registerkarten auf Benutzergruppenebene (anstatt auf Benutzerebene) verwalten.
- Für CMC-Registerkarten, die Ordner der obersten Ebene enthalten, müssen Administratoren den Zugriff auf eine Registerkarte sowie *Ansichtsrechte* für den Ordner der obersten Ebene der Registerkarte gewähren. Folgende CMC-Registerkarten unterstützen Ordner der obersten Ebene:
  - **Zugriffsberechtigungen**
  - **Kalender**
  - **Kategorien**
  - **(Universums-)Verbindungen**
  - **Kryptografieschlüssel**
  - **Ereignisse**
  - **Föderation**

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- **Ordner**
- **Posteingänge**
- **OLAP-Verbindung**
- **Persönliche Kategorien**
- **Persönliche Ordner**
- **Profile**
- **Replikationslisten**
- **Server und Gruppen**
- **Temporärer Speicher**
- **Universen**
- **Benutzer und Gruppen**
- **Webdienstabfrage**

- Zur verbesserten Systemsicherheit haben nur Mitglieder der Administratorgruppe Zugriff auf die folgenden CMC-Registerkarten. Als Systemadministratoren können Mitglieder der Administratorgruppe unabhängig von den Zugriffsberechtigungen für CMC-Registerkarten auf alle CMC-Registerkarten zugreifen. Die Zugriffsberechtigungen für CMC-Registerkarten dienen der Kontrolle des Zugriffs auf CMC-Registerkarten für delegierte Administratoren, das heißt, für Benutzer, die keine Mitglieder der Administratorgruppe sind.
  - **Überwachung**
  - **Authentifizierung**
  - **Kryptografieschlüssel**
  - **Lizenzschlüssel**
  - **Überwachen**
  - **Sitzungen**
  - **Einstellungen**
  - **Benutzerattributverwaltung**

> ⚠ Achtung
>
> Die Verwaltung des Zugriffs auf CMC-Registerkarten wirkt sich nur auf die grafische Darstellung der CMC-Benutzeroberfläche aus. Das Ausblenden von CMC-Registerkarten ist keine Sicherheitsmaßnahme, da dadurch keine Sicherheitsberechtigungen für Objekte innerhalb der Registerkarten festgelegt oder geändert werden. Um sicherzustellen, dass Benutzer keine nicht autorisierten Vorgänge für nicht autorisierte Objekte (z.B. Verwalten von Servern über den Central Configuration Manager oder Drittanbieter-Software basierend auf dem BI-Plattform-SDK) ausführen können, müssen Sie die entsprechenden Sicherheitsberechtigungen für Objekte (wie Serverobjekte) festlegen.

18.1.3.1.3.2.1.1 Verwalten des Zugriffs auf CMC-Registerkarten für andere Benutzer

1. Melden Sie sich an der CMC an.
2. Klicken Sie auf der Registerkarte *Benutzer und Gruppen* mit der rechten Maustaste auf einen Prinzipal und wählen **Konfiguration der CMC-Registerkarte**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Wenn der Zugriff auf CMC-Registerkarten uneingeschränkt ist, wird folgende Meldung angezeigt: `Warnung: Der Zugriff auf die Registerkarte "CMC" ist momentan nicht eingeschränkt. Um den CMC-Zugriff einzuschränken, klicken Sie auf die Registerkarte "Anwendung", wählen Sie "CMC" und setzen den Zugriff auf die Registerkarte "CMC" auf eingeschränkt. Diese Einstellungen werden wirksam, nachdem der Zugriff auf die Registerkarte "CMC" eingeschränkt wurde.` Sie können den Zugriff auf CMC-Registerkarten weiterhin konfigurieren. Die Konfiguration wird jedoch erst wirksam, nachdem Sie den Zugriff auf CMC-Registerkarten eingeschränkt haben.

Im Dialogfeld *CMC-Registerkarten konfigurieren* wird eine Tabelle angezeigt:

- ✓ oder ✗ zeigt an, auf welche CMC-Registerkarte der Prinzipal Zugriff hat.
- *Übernommen* zeigt an, dass der Registerkartenzugriff von ihren übergeordneten Benutzergruppen übernommen wurde.
- *Explizit* zeigt an, dass der Registerkartenzugriff explizit auf der Prinzipalebene festgelegt wurde.

3. Überprüfen Sie die Zugriffsberechtigungen für die CMC-Registerkarte. Um die Berechtigungen zu ändern, können Sie die Schaltflächen auf der Symbolleiste verwenden:
   - Klicken Sie auf **Gewähren**, um den Zugriff auf die Registerkarte explizit zu gewähren.
   - Klicken Sie auf **Verweigern**, um den Zugriff auf die Registerkarte explizit zu verweigern.
   - Klicken Sie auf **Übernehmen**, um ein übernommenes Zugriffsrecht zu verwenden.

   > **Hinweis**
   >
   > Durch Klicken auf die Schaltflächen werden die Änderungen sofort auf den Prinzipal angewendet.

4. Wenn Sie fertig sind, klicken Sie auf **Schließen**.

Der neue wirksame Zugriff auf die Registerkarten wird in der Spalte *Berechtigung* der Tabelle angezeigt.

Weitere Informationen

Einschränken des Zugriffs auf CMC-Registerkarten [Seite 606]

18.1.3.1.3.2.1.2 Übernahme des Zugriffs auf eine CMC-Registerkarte

Berechtigungen für den Zugriff auf CMC-Registerkarten sowie die Berechtigung zur Konfiguration des Zugriffs auf CMC-Registerkarten für andere Benutzer und Benutzergruppen werden genauso angewendet und übernommen wie andere Sicherheitsberechtigungen der BI-Plattform. Wenn der Registerkartenzugriff für Prinzipale nicht explizit festgelegt wurde, übernehmen Sie den Registerkartenzugriff von den Benutzergruppen, deren Mitglied sie sind.

Wenn ein Benutzer Mitglied von zwei Benutzergruppen ist, wird der Registerkartenzugriff auf die gleiche Weise berechnet wie alle anderen BI-Plattform-Berechtigungen. Wenn der Zugriff auf eine CMC-Registerkarte in einer

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

der Gruppen gewährt und in einer anderen verweigert wird, kann der Prinzipal nicht auf die CMC-Registerkarte zugreifen.

> **Hinweis**
>
> - Durch Änderung der Zugriffsberechtigung auf eine CMC-Registerkarte einer Benutzergruppe wird die Zugriffsberechtigung auf diese Registerkarte für alle Benutzer oder Benutzergruppen geändert, die Berechtigungen von der Benutzergruppe übernehmen, wenn ihr Zugriff auf die CMC-Registerkarte auf **Übernommen** gesetzt wird.
> - Der auf Benutzerebene festgelegte Registerkartenzugriff setzt stets den von Benutzergruppen übernommenen Registerkartenzugriff außer Kraft.

18.1.3.1.3.2.1.3 Benutzergruppen von delegierten Administratoren

Sie können einen Satz Benutzergruppen von delegierten Administratoren erstellen, um die Verwaltung von CMC-Registerkarten zu vereinfachen. Um nicht den Zugriff auf einzelne CMC-Registerkarten konfigurieren zu müssen, können Sie einen vorhandenen Benutzer oder eine vorhandene Benutzergruppe zum Mitglied einer Benutzergruppe eines delegierten Administrators machen. Folgende Konfiguration wird empfohlen, sie kann jedoch an spezifische Geschäftsanforderungen angepasst werden.

> **Hinweis**
>
> Die Mitgliedschaft in mehreren Gruppen resultiert in zusätzlichen Berechtigungen, wenn die Berechtigungen auf **Übernommen** gesetzt werden.

Benutzergruppe von delegierten Administratoren	Empfohlene Berechtigungen
Systemadministratoren	Gewähren des Zugriff auf alle Registerkarten.
Benutzeradministratoren	Gewähren des Zugriffs auf **Zugriffsberechtigungen**, **Folders**, **Posteingänge**, **Persönliche Ordner**, **Persönliche Kategorien**, **Abfrageergebnisse**, **Sitzungen** und **Benutzer und Gruppen**. Alle anderen Registerkarten auf **Übernommen** setzen.
Inhaltsadministratoren	Gewähren des Zugriffs auf **Kalender**, **Kategorien**, **Ereignisse**, **Ordner**, **Instanzenmanager**, **Persönliche Kategorien**, **Persönliche Ordner**, **Profile**, **Abfrageergebnisse** und **Universen**. Alle anderen Registerkarten auf **Übernommen** setzen.
Serveradministratoren	Gewähren des Zugriffs auf **Server** und **Anwendungen.** Alle anderen Registerkarten auf **Übernommen** setzen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18.1.3.1.3.2.1.4 Verwalten von Rechten zur Konfiguration des Zugriffs auf die Registerkarte "CMC" für andere Benutzer oder Benutzergruppen

In einer großen Unternehmensumgebung müssen Systemadministratoren u.U. die Verwaltung des Zugriffs auf CMC-Registerkarten an einen anderen Administrator übertragen. Alternativ kann in einem System mit mehreren Tenants jeder Tenant einen delegierten Administrator haben, der für die Verwaltung des Zugriffs auf CMC-Registerkarten für andere Benutzer und Benutzergruppen verantwortlich ist.

1. Melden Sie sich bei der CMC an.
2. Klicken Sie auf der Registerkarte *Benutzer und Gruppen* mit der rechten Maustaste auf einen Prinzipal und wählen **Konfiguration der CMC-Registerkarte**.
   Im Dialogfeld *CMC-Registerkarten konfigurieren* wird die Option **Berechtigung zur Konfiguration des Zugriffs auf die CMC-Registerkarte für andere Benutzer oder Benutzergruppen:** für den Prinzipal angezeigt.

   > **Hinweis**
   >
   > Falls die Berechtigung erteilt wird, kann der Prinzipal den Zugriff auf CMC-Registerkarten (nur auf Registerkarten, auf die der Prinzipal Zugriff hat) für Benutzer verwalten, für die der Prinzipal die Berechtigung *Sicher Rechte ändern* hat. Darüber hinaus kann der Prinzipal die Verwaltung des Zugriffs auf CMC-Registerkarten weiter an andere Benutzer delegieren, indem er Benutzern die **Berechtigung zur Konfiguration des Zugriffs auf die CMC-Registerkarte für andere Benutzer oder Benutzergruppen** erteilt, für die der Prinzipal die Berechtigung *Sicher Rechte ändern* hat.

   - ✓ oder ✗ zeigt an, ob der Prinzipal die Berechtigung zur Konfiguration von CMC-Registerkarten für andere Benutzer oder Benutzergruppen hat.
   - *Übernommen* zeigt an, dass die Berechtigung von ihren übergeordneten Benutzergruppen übernommen wurde.
   - *Explizit* zeigt an, dass die Berechtigung explizit auf der Prinzipalebene festgelegt wurde.
3. Überprüfen Sie die Berechtigungen zur Konfiguration des Zugriffs auf CMC-Registerkarten für andere Benutzer oder Benutzergruppen. Um die Berechtigungen zu ändern, wählen Sie eine der folgenden Einstellungen aus der Liste aus:
   - Klicken Sie auf **Gewähren**, um die Berechtigung zur Verwaltung des Zugriffs auf CMC-Registerkarten für andere Benutzer oder Benutzergruppen explizit zu gewähren.
   - Klicken Sie auf **Verweigern**, um die Berechtigung zur Verwaltung des Zugriffs auf CMC-Registerkarten für andere Benutzer oder Benutzergruppen explizit zu verweigern.
   - Klicken Sie auf **Übernehmen**, um die Berechtigung zur Verwaltung des Zugriffs auf CMC-Registerkarten für andere Benutzer oder Benutzergruppen zu übernehmen.

   > **Hinweis**
   >
   > Durch Auswahl einer Einstellung aus der Liste wird die Berechtigung des Prinzipals sofort geändert.
4. Wenn Sie fertig sind, klicken Sie auf **Schließen**.

Die neue wirksame Berechtigung wird angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Delegierte(r) Verwaltung und Zugriff auf CMC-Registerkarten [Seite 600]
Übernahme des Zugriffs auf eine CMC-Registerkarte [Seite 603]

18.1.3.1.3.2.1.5 Hinzufügen einer Registerkarte "Anpassung" für einen Benutzer oder eine Gruppe

Bevor Sie eine Registerkarte “Anpassung” für einen Benutzer oder eine Gruppe hinzufügen können, muss der CMC-Registerkartenzugriff auf **Eingeschränkt** gesetzt werden.

1. Wählen Sie in der CMC den Verwaltungsbereich **Benutzer und Gruppen** aus.
2. Klicken Sie mit der rechten Maustaste auf einen Benutzer oder eine Benutzergruppe und wählen **CMC-Registerkartenkonfiguration**.

   Das Dialogfeld *CMC-Registerkarten konfigurieren* wird mit einer Auflistung der einzelnen CMC-Registerkartentitel und ihren Zugriffsberechtigungen für die Benutzergruppe angezeigt.

   Wenn die folgende Warnmeldung oben im Dialogfeld in rot angezeigt wird, müssen Sie den CMC-Registerkartenzugriff auf eingeschränkt setzen, bevor Sie eine Registerkarte **Anpassung** hinzufügen können:

   ```
   Warnung: Der Zugriff auf die Registerkarte "CMC" ist momentan nicht eingeschränkt.
   Um den Zugriff auf die Registerkarte "CMC" einzuschränken, wählen Sie "CMC", und
   setzen Sie den Zugriff auf die Registerkarte "CMC" auf eingeschränkt. Diese
   Einstellungen werden wirksam, nachdem der Zugriff auf die Registerkarte "CMC"
   eingeschränkt wurde:
   ```
3. (Falls erforderlich) So setzen Sie den Zugriff auf die Registerkarte "CMC" auf eingeschränkt:
   a) Klicken Sie im Verwaltungsbereich **Anwendungen** der CMC mit der rechten Maustaste auf **Central Management Console** und wählen **Konfiguration des Zugriffs auf die CMC-Registerkarte**.
   b) Wählen Sie unter **Konfiguration des Zugriffs auf die CMC-Registerkarte** die Option **Eingeschränkt** und klicken auf **Speichern & schließen**.
4. Wählen Sie im Dialogfeld *CMC-Registerkarten konfigurieren* für die Benutzergruppe für jede CMC-Registerkarte **Gewährt**, **Verweigert** oder **Übernommen** in der Liste aus.
   Jedes Mal, wenn Sie die Berechtigung für eine Registerkarte ändern, aktualisiert das Dialogfeld "CMC-Registerkarten konfigurieren" die Berechtigung der Benutzergruppe zum Konfigurieren des Registerkartenzugriffs für andere Benutzer oder Benutzergruppen.
5. Klicken Sie auf **Schließen**.

18.1.3.1.3.2.2 Einschränken des Zugriffs auf CMC-Registerkarten

Es wird empfohlen, zuerst den Zugriff auf CMC-Registerkarten für Prinzipale zu konfigurieren und anschließend den Zugriff auf CMC-Registerkarten einzuschränken. Wenn Sie den Registerkartenzugriff vor der Konfiguration

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

einschränken, können Ihre Benutzer erst auf CMC-Registerkarten zugreifen, nachdem ihnen ein Administrator Zugriff darauf gewährt hat.

Um die Konsistenz mit früheren Versionen der BI-Plattform sicherzustellen, ist der Zugriff auf CMC-Registerkarten anfänglich nach der Installation der BI-Plattform uneingeschränkt, und alle Benutzer, die Zugriff auf die CMC haben, haben Zugriff auf alle verfügbaren Registerkarten. Um Benutzer daran zu hindern, auf Registerkarten zuzugreifen, für die sie keine Zugriffsberechtigung besitzen, können Systemadministratoren den Zugriff auf die CMC-Registerkarten einschränken.

In dringenden Fällen kann die Einschränkung des Zugriffs auf eine CMC-Registerkarte aufgehoben werden oder zur Fehlerbehebung der Konfiguration des Zugriffs auf CMC-Registerkarten (z.B. wenn ein delegierter Administrator nicht auf eine wichtige CMC-Registerkarte zugreifen kann).

1. Melden Sie sich bei der CMC an.
2. Klicken Sie auf der Registerkarte *Anwendungen* mit der rechten Maustaste auf **Central Management Console** und wählen **Konfiguration des Zugriffs auf die CMC-Registerkarte**.
   Das Dialogfeld *CMC-Registerkartenzugriff* wird angezeigt.
3. Konfigurieren Sie die Regeln für den Zugriff auf CMC-Registerkarten.
   - Um den Zugriff Ihrer Benutzer auf Registerkarten einzuschränken, für die sie Berechtigungen haben, wählen Sie **Eingeschränkt**.
   - Um Ihren Benutzern den Zugriff auf alle Registerkarten zu gewähren, wählen Sie **Nicht eingeschränkt**.
4. Klicken Sie abschließend auf **Speichern und schließen**.

Die Regel für den Zugriff auf die CMC-Registerkarten wird auf das System angewendet.

Weitere Informationen

Fehlerbehebung des Zugriffs auf CMC-Registerkarten [Seite 607]

18.1.3.1.3.2.3 Fehlerbehebung des Zugriffs auf CMC-Registerkarten

Zur Verhinderung von unberechtigtem Zugriff oder zur Fehlerbehebung des eingeschränkten Zugriffs eines Benutzers auf CMC-Registerkarten, können Sie die Zugriffsberechtigungen für CMC-Registerkarten eines Benutzers ändern.

1. Melden Sie sich als Administrator bei der CMC an.

   > **Hinweis**
   >
   > Stellen Sie sicher, dass Sie Zugriff auf die Registerkarte haben, für die Sie eine Fehlerbehebung durchführen möchten, und dass Sie über die Berechtigung *Sicher Rechte ändern* für den Benutzer verfügen.

2. Klicken Sie auf der Registerkarte *Benutzer und Gruppen* mit der rechten Maustaste auf einen Prinzipal und wählen **Konfiguration der CMC-Registerkarte**.
   Das Fenster *CMC-Registerkarten konfigurieren* wird angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Überprüfen Sie den festgelegten CMC-Registerkartenzugriff. Sie können Zugriff auf die verfügbaren Registerkarten explizit gewähren oder verweigern.

   Wenn der Zugriff auf CMC-Registerkarten übernommen wird, der Registerkartenzugriff jedoch nicht den Anforderungen des Benutzers genügt:

   a) Stellen Sie eine Liste aller Benutzergruppen zusammen, bei denen der ausgewählten Prinzipal Mitglied ist.
   b) Wiederholen Sie die Schritte 1 bis 3 für jede Gruppe, von der der Benutzer den Registerkartenzugriff übernimmt.
   c) Korrigieren Sie den CMC-Registerkartenzugriff nach Bedarf auf Prinzipalebene oder Gruppenebene.

   > **Hinweis**
   >
   > Wenn diese Aufgabe auf Gruppenebene ausgeführt wird, wirkt sich der CMC-Registerkartenzugriff auf alle Benutzer aus, die Mitglieder dieser Benutzergruppe sind, sowie alle Benutzer, die Mitglieder der von dieser Benutzergruppe übernommenen Benutzergruppen sind, sofern der CMC-Registerkartenzugriff für die Benutzer auf **Übernommen** gesetzt ist.

4. Wenn Sie fertig sind, klicken Sie auf **Schließen**.

Weitere Informationen

Verwalten des Zugriffs auf CMC-Registerkarten für andere Benutzer [Seite 602]
Übernahme des Zugriffs auf eine CMC-Registerkarte [Seite 603]

18.1.3.2 Verwalten der Einstellungen von Diskussionsforen

Im Bereich *Anwendungen* der CMC in der BI-Plattform können Sie die Einstellungen für Diskussions-Threads auf Systemebene festlegen.

Sie können für die Anwendung *Diskussionsforen* Diskussions-Threads verwalten und mit ihnen auf verschiedene Arten interagieren, z.B.:

- Suchen von Diskussions-Threads nach angegebenen Suchkriterien.
- Sortieren von Suchergebnissen von Diskussions-Threads.
- Löschen von Diskussions-Threads.

> **Hinweis**
>
> Für die Anwendung Discussions sind keine Einstellungen für Benutzerrechte verfügbar. Sie können jedoch Rechte für einzelne Berichte festlegen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18.1.3.2.1 Suchen nach Diskussionsthreads

Standardmäßig werden auf der Seite *Diskussionsforum* die Titel aller Diskussionsthreads angezeigt. Es werden ausschließlich Threads auf der Stammebene angezeigt.

Um durch eine Liste der Diskussionsthreads zu blättern, verwenden Sie die Schaltflächen "Zurück" und "Weiter". Sie können auch einen bestimmten Thread oder eine Gruppe von Threads suchen.

1. Wechseln Sie zum Bereich *Anwendungen* der CMC, und wählen Sie **Diskussionsforum**.
2. Klicken Sie auf **Verwalten** > **Threads verwalten**.
   Das Dialogfeld **Notizenverwaltung** wird angezeigt.
3. Wählen Sie in der Liste **Feldname** eine Option aus.

Option	Beschreibung
Thread-Titel	Sucht nach Thread-Titel
Erstellungsdatum	Sucht nach Erstellungsdatum
Letztes Änderungsdatum	Sucht nach dem letzten Änderungsdatum
Autor	Sucht nach Autor

4. In der zweiten Liste können Sie Ihre Suche eingrenzen.

> **Hinweis**
>
> Bei der Suche wird die Groß-/Kleinschreibung nicht berücksichtigt.

   - Wenn Sie nach **Thread-Titel** oder **Autor** suchen, wählen Sie aus den folgenden Optionen im zweiten Feld aus.

Option	Beschreibung
ist	Sucht alle Diskussionsthreads, deren Titel oder Autor exakt mit der Schreibweise des von Ihnen im dritten Feld eingegebenen Texts übereinstimmt.
ist nicht	Sucht alle Diskussionsthreads, deren Titel oder Autor nicht exakt mit der Schreibweise des von Ihnen im dritten Feld eingegebenen Texts übereinstimmt.
enthält	Sucht alle Diskussionsthreads, bei denen der Suchtext in einem beliebigen Teil des Threadtitels oder Autornamens vorkommt.
enthält nicht	Sucht alle Diskussionsthreads, bei denen der Suchtext in keinem Teil des Threadtitels oder Autornamens vorkommt.

   - Falls Sie **Erstellungsdatum** oder **Letztes Änderungsdatum** ausgewählt haben, wählen Sie eine der folgenden Optionen und geben dann ein Suchdatum an.

Option	Beschreibung
vor	Sucht alle Diskussionsthreads, die vor dem Suchdatum erstellt oder geändert wurden.
nach	Sucht alle Diskussionsthreads, die nach dem Suchdatum erstellt oder geändert wurden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung
zwischen	Sucht alle Diskussionsthreads, die zwischen den beiden Suchdatumsangaben erstellt oder geändert wurden.

5. Verwenden Sie das dritte Textfeld, um die Suche weiter einzugrenzen.
   - Wenn Sie in den ersten beiden Feldern eine textbasierte Suche ausgewählt haben, geben Sie die Textzeichenfolge ein.
   - Bei Auswahl einer datumsbasierten Suche geben Sie eine bzw. zwei Datumsangaben in die entsprechenden Felder ein.
6. Klicken Sie auf **Suchen**.

18.1.3.2.2 So sortieren Sie Suchergebnisse in Diskussionsthreads

Wenn Sie Diskussionsthreads suchen, können Sie auswählen, wie die Suchergebnisse angezeigt werden sollen. So können Sie die Ergebnisse beispielsweise in aufsteigender alphabetischer Reihenfolge ordnen und auswählen, wie viele Ergebnisse pro Seite angezeigt werden.

1. Wechseln Sie zum Bereich *Anwendungen* der CMC, und wählen Sie **Diskussionsforum**.
2. Klicken Sie auf **Verwalten** > **Threads verwalten**.
   Das Dialogfeld *Notizenverwaltung* wird angezeigt.
3. Wählen Sie in der Liste **Sortieren nach** eine Sortieroption.

Option	Beschreibung
Thread-Titel	Sortiert nach dem Titel eines Diskussionsthreads.
Erstellungsdatum	Sortiert nach dem Datum, zu dem der Diskussionsthread erstellt wurde.
Letztes Änderungsdatum	Sortiert nach dem Datum, zu dem ein Diskussionsthread zuletzt geändert wurde.
Autor	Sortiert nach dem Autor eines bestimmten Diskussionsthreads.

4. In der zweiten Liste wählen Sie aus, ob die Datensätze in auf- oder absteigender Reihenfolge angezeigt werden sollen.
5. Im dritten Textfeld geben Sie ein, wie viele Ergebnisse für den Diskussionsthread auf jeder Seite angezeigt werden sollen.

   Der Standardwert beträgt 10 Ergebnisse pro Seite.
6. Klicken Sie auf **Suchen**.

18.1.3.2.3 So löschen Sie einen Diskussionsthread

Sie können beliebige Diskussionsthreads im Bereich *Anwendungen* der CMC in der BI-Plattform löschen.

1. Wechseln Sie zum Bereich *Anwendungen* der CMC, und wählen Sie **Diskussionsforum**.
2. Klicken Sie auf **Verwalten** > **Threads verwalten**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Das Dialogfeld *Notizenverwaltung* wird angezeigt.

3. Suchen Sie den zu löschenden Diskussionsthread in der Ergebnisliste, und wählen Sie ihn aus.
4. Klicken Sie auf **Löschen**.

18.1.3.3 Verwalten der BI-Launchpad-Einstellungen

Wählen Sie im CMC-Bereich **Anwendungen** der BI-Plattform ▶ **Verwalten** > **Eigenschaften** ▶ aus, um Anzeigeoptionen für BI-Launchpad anzuzeigen.

Sie können Benutzern oder Gruppen für BI-Launchpad das Ausführen folgender Aktionen ermöglichen:

- Ändern von Einstellungen
- Organisieren von Ordnern
- Suchen
- Filtern von Objektlisten nach Objekttyp
- Anzeigen des Ordners `Favoriten`

Wenn Sie beispielsweise für Benutzer Ordner gemäß einer Standardnamenskonvention erstellt haben, können Sie den Benutzern das Recht verweigern, ihre Ordner selbst zu organisieren.

> **Hinweis**
>
> In der Standardeinstellung haben alle Benutzer Zugriff auf diese Funktionen.

18.1.3.3.1 Ändern der Anzeigeeinstellungen von BI-Launchpad

1. Wechseln Sie in den Bereich **Anwendungen** der CMC, und doppelklicken Sie auf **BI-Launchpad**.
   Das Dialogfeld *BI-Launchpad-Eigenschaften* wird angezeigt.
2. Zum Aktivieren eines Diskussionsforums für BI-Launchpad-Benutzer aktivieren Sie das Kontrollkästchen **Diskussionsforum aktivieren**.
3. Zum Aktivieren von Filtern für die zeitgesteuerte Verarbeitung aktivieren Sie das Kontrollkästchen **Registerkarte "Filter" auf der Seite "Zeitgesteuert verarbeiten" anzeigen**.

   Diese Einstellung steuert, ob Benutzer beim Planen eines Crystal-Reports-Berichts Datensatz- oder Gruppenauswahlformeln eingeben können.
4. Klicken Sie auf **Speichern und schließen**.

18.1.3.4 Verwalten von Web-Intelligence-Einstellungen

Sie können steuern, auf welche Funktionen die Benutzer für Web Intelligence-Dokumente zugreifen können, indem Sie Eigenschaften für die Web Intelligence-Anwendung festlegen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18.1.3.4.1 Ändern der Anzeigeeinstellungen in Web Intelligence

1. Wechseln Sie zum Bereich *Anwendungen* der CMC, und wählen Sie **Web Intelligence**.
2. Klicken Sie auf **Verwalten** > **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
3. Legen Sie eine der folgenden Anzeigeoptionen fest:

Option	Beschreibung
Dimensionen und Informationen	Verwenden Sie die Optionen in diesem Bereich, um festzulegen, wie hinzugefügte Daten in Berichten angezeigt werden und um Schriftschnitt, Textfarbe und Hintergrundfarbe zu ändern. Bei einer Vorschau der Zelle werden die Änderungen automatisch angezeigt. Klicken Sie auf **OK**, sobald Sie fertig sind.
Schwankungswerte (numerische Kennzahlen)	Verwenden Sie die Optionen in diesem Bereich, um Seitenüberschriften zu ändern und zu formatieren und um Schriftschnitt, Textfarbe und Hintergrundfarbe zu ändern. Bei einer Vorschau der Zelle werden die Änderungen automatisch angezeigt. Klicken Sie auf **OK**, sobald Sie fertig sind.
Eigenschaften eingebetteter Bilder	Geben Sie die Maximalgröße eingebetteter Bilder ein.
Eigenschaften des schnellen Anzeigemodus	Legen Sie in den entsprechenden Feldern die maximale Anzahl vertikaler Datensätze und horizontaler Datensätze, die Mindestbreite und Mindesthöhe der Seite sowie den Füllen rechts-Wert und Füllen unten-Wert fest.
Einstellungen für das automatische Speichern	Legen Sie das Intervall fest, in dem Dokumente automatisch gespeichert werden. Dieses Intervall wird jedes Mal zurückgesetzt, wenn ein Dokument manuell oder automatisch gespeichert wird. Das automatisch gespeicherte Dokument wird zudem gelöscht, wenn Sie ein Dokument manuell speichern.
Automatisch regenerieren	Aktiviert die automatische Regenerierung von Web-Intelligence-Dokumenten, wenn die Web-Intelligence-Dokumenteigenschaft **Automatische Regenerierung** ausgewählt wurde. Ausführliche Informationen finden Sie im *Benutzerhandbuch für SAP BusinessObjects Web Intelligence*.
Automatische Zusammenführung	Aktiviert die automatische Zusammenführung von Dimensionen, wenn die Web-Intelligence-Dokumenteigenschaft **Dimensionen automatisch zusammenführen** ausgewählt wurde. Ausführliche Informationen finden Sie im *Benutzerhandbuch für SAP BusinessObjects Web Intelligence*.
Automatische Dokumentregenerierung beim Öffnen der Sicherheitsberechtigungseinstellung	Entfernen Sie diese Option, damit Web Intelligence Dokumente beim Öffnen automatisch regenerieren kann, ohne dass **Beim Öffnen regenerieren** in den Web-Intelligence-Dokumenteigenschaften aktiviert wurde. Durch die Auswahl dieser Option wird die Sicherheitsberechtigung **Dokumente: Automatische Regenerierung beim Öffnen deaktivieren** ausgewählt.
SmartView	Diese Option bestimmt, welche Dokumentversion angezeigt wird, wenn Benutzer Dokumente in Web Intelligence öffnen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung
	○ Letzte Instanz anzeigen Die letzte Instanz des Objekts wird geöffnet. Wenn beispielsweise ein Dokument stündlich regeneriert werden soll und das Dokument zuletzt vor fünf Stunden gespeichert und geschlossen wurde, wird die letzte Instanz geöffnet. Wenn ein Benutzer diese Instanz speichert, wird das ursprüngliche Dokument entsprechend aktualisiert. ○ Objekt anzeigen Das Dokument wird in demselben Status geöffnet, in dem es zuletzt gespeichert wurde, unabhängig von jeglichen eingeplanten Regenerierungen, die u.U. durchgeführt wurden.

4. Klicken Sie auf **Speichern und schließen**.

> **Hinweis**
>
> Um mit Ihrer Auswahl zu den standardmäßigen Anzeigevariablen zurückzukehren, klicken Sie auf **Zurücksetzen**.

18.1.3.5 Verwalten von Warnmeldungseinstellungen

Im Bereich *Anwendungen* der CMC in der BI-Plattform können Sie die Einstellungen für Warnmeldungen auf Systemebene festlegen.

Für die *Warnungsanwendung* können Sie folgendermaßen steuern und festlegen, wie Systembenutzer auf Warnmeldungen zugreifen:

- Aktivieren des Ordners **Meine Warnmeldungen** für Warnmeldungsabonnenten
- Aktivieren und Formatieren von per E-Mail gesendeten Warnmeldungen
- Begrenzen der Anzahl an Warnmeldungen im System
- Festlegen einer Gültigkeitsdauer für Warnmeldungen

Weitere Informationen

Festlegen von Benutzerrechten für Anwendungen [Seite 595]

18.1.3.5.1 Ändern der Zieleigenschaften von Warnmeldungen

1. Doppelklicken Sie im Bereich **Anwendungen** der CMC auf **Warnungsanwendung**.
2. Klicken Sie auf **Verwalten** > **Eigenschaften**.
   Das Dialogfeld *Warnmeldungen* wird angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. (Erforderlich) Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie **Meine Warnmeldungen aktivieren** aus, wenn Abonnenten von Warnmeldungen Benachrichtigungen im Bereich **Meine Warnmeldungen** im BI-Launchpad erhalten sollen.
   - Wählen Sie **E-Mail aktivieren** aus, wenn Abonnenten Benachrichtigungen per E-Mail erhalten sollen.

     Es werden globale E-Mail-Optionen für Warnmeldungen angezeigt.
4. Wenn Sie **E-Mail aktivieren** ausgewählt haben, führen Sie folgende Schritte durch:
   - Geben Sie im Feld **Von** die E-Mail-Adresse des Benutzers ein, von dem die Warnungsbenachrichtigungen aus gesendet werden.

     Die Abonnenten erhalten Warnmeldungs-E-Mails dieser E-Mail-Adresse. Verwenden Sie eine gültige E-Mail-Adresse, die vom System erkannt wird.
   - Geben Sie im Feld **An** die E-Mail-Adresse des Warnmeldungsabonnenten ein.

     Alle Systemwarnmeldungen werden standardmäßig an diese E-Mail-Adresse gesendet.

     > **Tipp**
     >
     > Geben Sie keine E-Mail-Adresse oder keinen -Empfänger ein. Verwenden Sie den Platzhalter **%SI_EMAIL_ADDRESS%**.
   - Geben Sie im Feld **cc** die Empfänger-E-Mail-Adresse ein, an die eine Kopie der Warnmeldungen gesendet werden soll.
   - Geben Sie im Feld **Betreff** eine Standardbetreffzeile für E-Mails, die Warnmeldungen enthalten, ein.
   - Geben Sie im Feld **Nachricht** eine Standardnachricht für E-Mails, die Warnmeldungen enthalten, ein.
   - Wählen Sie **Anlage hinzufügen**, um standardmäßig Anlagen für E-Mails, die Warnmeldungen enthalten, zu aktivieren.

     Diese Option können Sie beispielsweise auswählen, um zugehörige Crystal-Reports-Berichte an ausgelöste Warnmeldungen anzuhängen.
   - Wenn Sie **Anlage hinzufügen**ausgewählt haben, wählen Sie unter **Dateiname** die Option**Automatisch generierten Namen verwenden** oder **Spezifischen Namen verwenden**, um anzugeben, welcher Name für Anlagen in E-Mails verwendet werden soll.
5. Klicken Sie auf **Speichern und schließen**.

Weitere Informationen

Festlegen von Benutzerrechten für Anwendungen [Seite 595]
Verwalten von Warnmeldungseinstellungen [Seite 613]

18.1.3.5.2 Ändern der Standardeigenschaften von Warnmeldungen

1. Wechseln Sie in den Bereich *Anwendungen* der CMC, und wählen Sie **Warnungsanwendung** aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Klicken Sie auf **Verwalten** > **Eigenschaften** > **Standardeinstellungen**.
3. Legen Sie für die folgenden Eigenschaften geeignete Werte fest.

Option	Beschreibung
Gültigkeitsdauer	Legt fest, wie lange Warnmeldungen im System gespeichert werden, bevor sie gelöscht werden.
Maximale Anzahl an Warnmeldungen	Gibt die maximale Anzahl von Warnmeldungen an, die im System unterstützt werden. Wenn der Schwellenwert erreicht ist, entfernt das System 20 % der Warnmeldungen und beginnt dabei mit den ältesten.

4. Klicken Sie auf **Speichern und schließen**.

Weitere Informationen

Verwalten von Warnmeldungseinstellungen [Seite 613]

18.1.3.6 Verwalten von Widget-Einstellungen

Widgets für SAP BusinessObjects ist eine Desktopanwendung, mit deren Hilfe Benutzer Minianwendungen zu ihrem Desktop hinzufügen können, um auf einfache Weise auf Business-Intelligence-Inhalt in BI-Plattform- und Web Dynpro-Anwendungen auf SAP NetWeaver Application Servern zuzugreifen.

Über den Bereich "Anwendungen" der CMC können Sie den Zugriff der Benutzer zum Erstellen und Verwenden von Widgets auf ihrem Desktop sowie die Fähigkeit, das BI-Plattform-Repository aus der Widget-Anwendung auf dem Desktop heraus zu durchsuchen, steuern.

Sie können Benutzern oder Gruppen das Ausführen folgender Aktionen ermöglichen:

- Widgets verwenden
- Von Widgets erstellte Objekte bearbeiten
- Benutzerrechte für den Zugriff auf Objekte ändern

> **Hinweis**
>
> In der Standardeinstellung haben alle allgemeinen Benutzer Zugriff auf diese Funktionen.

18.1.3.7 Verwalten der SAP BusinessObjects Explorer-Einstellungen

Sie können für SAP BusinessObjects Explorer festlegen, auf welche Funktionen Benutzer Zugriff haben, indem Sie die zugehörigen Sicherheitsberechtigungen im Bereich "Anwendungen" der CMC festlegen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18.1.3.7.1 Ändern der SAP BusinessObjects Explorer-Anwendungseigenschaften

1. Wechseln Sie zum Bereich *Anwendungen* der CMC.
2. Klicken Sie auf **Verwalten** > **Eigenschaften**.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
3. Legen Sie folgende SAP BusinessObjects Explorer-Einstellungen fest:
   - Gültigkeit von Lesezeichen
   - Erweiterte Konfiguration
4. Klicken Sie auf **Speichern und schließen**.

18.1.3.8 Verwalten der Integration von Anwendungen für die Zusammenarbeit

Dieses Handbuch ist für BI-Plattform-Administratoren vorgesehen, die die BI-Plattform mit den Anwendungen für Zusammenarbeit SAP Jam oder SAP StreamWork integrieren.

Im Bereich **Anwendungen** der Central Management Console (CMC) auf der BI-Plattform können Sie die Zusammenarbeit aktivieren und konfigurieren.

Im Enterprise-Agent der Anwendung für die Zusammenarbeit sind folgende zusätzlichen Konfigurationseinstellungen vorzunehmen:

- Einrichten der HTTPS-Verbindung mit einem Dienstprovider
- Erfüllen der Voraussetzungen für die Authentifizierung

Nachdem SAP Jam oder SAP StreamWork konfiguriert wurde, stehen Feeds aus der Anwendung für die Zusammenarbeit im BI-Launchpad zur Verfügung.

Microsoft Internet Explorer 11 wird von SAP Jam nicht unterstützt.

18.1.3.8.1 Voraussetzungen für die Zusammenarbeit

Bevor Sie die BI-Plattform mit einer Zusammenarbeitsplattform integrieren, müssen die Voraussetzungen für die Zusammenarbeit erfüllt sein.

- Die BI-Plattform muss mit mindestens einem Central Management Server (CMS) installiert werden.
- Die Zusammenarbeitsanwendung (SAP Jam oder SAP StreamWork) muss in der Central Management Console (CMC) werden.
- Für die Zusammenarbeitsanwendung (SAP Jam oder SAP StreamWork) muss eine Enterprise-Organisation festgelegt werden.
- SAP-Jam- oder SAP-StreamWork-Benutzer müssen der Enterprise-Organisation angehören.
- Ein SAP StreamWork Enterprise Agent ist nur erforderlich, um Benutzer bereitzustellen, die einen lokalen LDAP/AD-Verzeichnisdienst verwenden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18.1.3.8.2 BI-Plattformkonfiguration

18.1.3.8.2.1 Konfigurationsoptionen für die Zusammenarbeit

Die Optionen für die Zusammenarbeit werden im Dialogfeld *Eigenschaften: Zusammenarbeit* in der Central Management Console (CMC) der BI-Plattform angezeigt.

Um das Dialogfeld *Eigenschaften: Zusammenarbeit* aufzurufen, wählen Sie auf der Registerkarte **Anwendungen** in der CMC die Option **Zusammenarbeit** und dann **Verwalten** > **Eigenschaften**.

Option	Beschreibung	
Zusammenarbeit aktivieren	Aktivieren Sie dieses Kontrollkästchen, und wählen Sie **SAP Jam** oder **SAP StreamWork** aus.	
Verbindungs-URL	Geben Sie die URL zur Anwendung für die Zusammenarbeit ein.	
Eindeutige ID des Identitätsproviders	Geben Sie einen eindeutigen Wert für Ihre BI-Plattform-Implementierung ein. Dieser Wert ist mit dem Zertifikat zu verknüpfen, das zur Konfiguration der Integration in der Administrationskonsole der Anwendung für die Zusammenarbeit verwendet wird. Die Anwendung, die eine Identität für die Einzelanmeldung sicherstellt, muss als administrative OAuth-Anwendung konfiguriert sein.	
Base64-Zertifikat des Identitätsproviders	Wenn Sie **Generieren** wählen, wird in diesem Feld ein Zertifikat generiert. Verwenden Sie dieses Zertifikat in der Administrationskonsole der Anwendung für die Zusammenarbeit, um einen OAuth-Consumer-Schlüssel zu generieren. Dieses Zertifikat stellt eine Vertrauensbeziehung zwischen der Anwendung für die Zusammenarbeit und der BI-Plattform her. Der externe Identitätsprovider selbst wird mit einem X509-Zertifikat identifiziert, mit dem alle Identitätssicherstellungen signiert werden. Das Zertifikat muss Base64-codiert sein.	
OAuth-Consumer-Schlüssel	Geben Sie den in der Administrationskonsole der Anwendung für die Zusammenarbeit generierten OAuth-Consumer-Schlüssel ein.	
Herstellen einer Verbindung über Proxy	Aktivieren Sie dieses Kontrollkästchen, um die Verbindung über Proxy herzustellen, und geben Sie die Informationen zum Proxy-Host in den Feldern **HTTP-Proxy-Host** und **Port** ein. Um eingehende Verbindungen von den Servern der Anwendung für die Zusammenarbeit mit dem Unternehmensnetzwerk zuzulassen, muss in der DMZ ein Reverse Proxy vorhanden sein. Um ein vertrauenswürdiges Zertifikat von einem SSL-Zertifikatprovider dem Reverse Proxy hinzuzufügen, muss der Reverse Proxy über einen Domänen- oder Unterdomänennamen verfügen.	
	HTTP-Proxy-Host	Geben Sie in der Reverse-Proxy-Konfiguration eine externe Adresse ein, die für die Anwendung für die Zusammenarbeit zugänglich ist. Verwenden Sie z. B. `https://<ReverseProxy>/`, wobei `<ReverseProxy>` der Domänen- oder Unterdomänenname des Reverse Proxy ist.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung	
		Die Anwendung für die Zusammenarbeit verwendet diese Adresse, um Informationen an die BI-Plattform zu senden. Der Reverse Proxy verwendet diese Adresse, um die von der Anwendung für die Zusammenarbeit empfangenen Informationen an den Rechner umzuleiten, der den Enterprise-Agent der Anwendung für die Zusammenarbeit enthält.
	Port	Der Enterprise-Agent der Anwendung für die Zusammenarbeit ist so konfiguriert, dass er den Port 8443 überwacht.

18.1.3.8.2.2 Aktivieren und Konfigurieren der Zusammenarbeit in der CMC

Für diese Aufgabe ist eine gültige Verbindung mit der Administrationskonsole der Anwendung für die Zusammenarbeit (SAP Jam oder SAP StreamWork) erforderlich. Sie müssen Sicherheitsdetails an die Konsole übergeben und dort abrufen.

Aus Sicherheitsgründen können die folgenden Standardkonten keinen Inhalt an SAP Jam oder SAP StreamWork senden oder zeitgesteuert verarbeiten:

- Guest
- SMAdmin
- Administrator
- WaaWSServletPrincipal

1. Gehen Sie in der Central Management Console (CMC) der BI-Plattform zum Bereich **Anwendungen**, und doppelklicken Sie auf **Zusammenarbeit**.
2. Aktivieren Sie im Dialogfeld *Eigenschaften: Zusammenarbeit* das Kontrollkästchen **Zusammenarbeit aktivieren**, und wählen Sie **SAP Jam** oder **SAP StreamWork** aus.
3. Geben Sie im Feld **Verbindungs-URL** die URL zur Anwendung für die Zusammenarbeit ein.
4. Geben Sie im Feld **Eindeutige ID des Identitätsproviders** einen eindeutigen Wert des Identitätsproviders für die BI-Plattform-Implementierung ein.

   Notieren Sie sich den Wert des Identitätsproviders. Diesen Wert werden Sie zur Konfiguration der Anwendung für die Zusammenarbeit verwenden.
5. Klicken sie auf **Generieren** (oder **Regenerieren**, falls bereits ein Zertifikat erstellt wurde).
   Im Feld **Base64-Zertifikat des Identitätsproviders** wird das Zertifikat angezeigt. Das Zertifikat wird zur Konfiguration der Anwendung für die Zusammenarbeit verwendet.
6. Geben Sie im Feld **OAuth-Consumer-Schlüssel** einen gültigen OAuth-Consumer-Schlüssel ein.
7. Falls Sie über einen Proxy mit dem Server, der SAP Jam oder SAP StreamWork ausführt, verbunden sind, führen Sie folgende Aktionen aus:
   a) Aktivieren Sie das Kontrollkästchen **Herstellen einer Verbindung über Proxy**.
   b) Geben Sie im Feld **HTTP-Proxy-Host** den Proxy-Host-Namen des Servers ein.
   c) Geben Sie im Feld **Port** die Portnummer des Servers ein.
8. Klicken Sie auf **Speichern und schließen**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18.1.3.8.3 SAP-Jam-Konfiguration

18.1.3.8.3.1 Registrieren eines neuen vertrauenswürdigen SAML-IDP für SAP Jam

Jeder Benutzer muss mit einer eindeutigen E-Mail-Adresse registriert sein, die der Enterprise-E-Mail-Adresse des Benutzers im BI-Launchpad entspricht. Die E-Mail-Adressen werden zwischen der BI-Plattform und dem SAP-System zugeordnet.

Stellen Sie vor dem Registrieren eines neuen vertrauenswürdigen SAML-Identitätsproviders Folgendes sicher:

- Ihr Unternehmen ist dem SAP hinzugefügt und darin konfiguriert.
- Sie verfügen über ein gültiges SAP-Benutzerkonto, das mit Ihrem Unternehmen im SAP-System verknüpft ist.
- Sie verfügen über Unternehmensadministratorrechte für Ihr Unternehmen im SAP-System und die vollständigen Administratorrechte auf der BI-Plattform und im BI-Launchpad.
- Das BI-Launchpad muss im SAP-System als OAuth-Client registriert sein, der als Vertreter von BI-Launchpad im SAP-System fungiert.

Microsoft Internet Explorer 11 wird von SAP Jam nicht unterstützt.

1. Wählen Sie rechts oben in der Central Management Console (CMC) in der BI-Plattform **Administrator** und dann **Admin**.
   Es werden Informationen über Ihr Unternehmen, einschließlich Ihrer SAP-Lizenz, angezeigt. Notieren Sie sich diese Informationen.
2. Wählen Sie **Vertrauenswürdige SAML-IDs** im **Admin**-Menü, und klicken Sie auf **Identitätsprovider registrieren**.

   Sie müssen den Identitätsprovider registrieren, den Sie im BI-Launchpad erstellt haben.
3. Geben Sie im Feld **IDP ID** den Wert des eindeutigen Identitätsproviders ein, der bei der Konfiguration von SAP auf der BI-Plattform erstellt wurde.

   Wenn Ihnen der Wert nicht vorliegt, wenden Sie sich an die Systemadministration für externe Anwendungen.

   Geben Sie z. B. `<Firmenname>_<SystemID>_<Client>` ein.
4. Geben Sie im Feld **Single Sign-On URL** (Einzelanmeldungs-URL) die URL ein, die direkt auf das SAP-System zugreift.

   Das SAP-System verwendet diese URL für die Einzelanmeldung am eindeutigen Identitätsprovider.
5. Geben Sie im Feld **Single Log-Out URL** (Einzelabmeldungs-URL) die URL ein, die nach der Abmeldung vom SAP-System angezeigt werden soll.

   Das SAP-System verwendet diese URL für die Einzelabmeldung vom eindeutigen Identitätsprovider.
6. Geben Sie in das Feld **Default Name ID Format** (Format der Standardnamens-ID) das Format der Namens-ID ein, das bei Authentifizierungsanforderungen verwendet werden soll.
7. Geben Sie in das Feld **Default Name ID Policy SP Name Qualifier** (DP-Namensqualifizierer der Richtlinien für die Standardnamens-ID) den SP-Namensqualifizierer ein, der bei Authentifizierungsanforderungen verwendet werden soll.
8. Wählen Sie aus der Liste **Allowed Assertion Scope** (Zulässiger Assertionsumfang) die Option **Users in my company** (Benutzer in meiner Organisation) aus.

   Mit dieser Option wird die Gruppe der Benutzer festgelegt, für die das SAP-System Assertionen vom Identitätsprovider akzeptiert.
9. Geben Sie im Feld **X509 Certificate (Base64)** den Wert des Base64-Zertifikats ein, der bei der Konfiguration vom SAP-System auf der BI-Plattform generiert wurde.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wenn Ihnen der Wert nicht vorliegt, wenden Sie sich an die Systemadministration für externe Anwendungen.

10. Klicken Sie auf **Registrieren**.

18.1.3.8.3.2 Erstellen eines OAuth-Clients für SAP Jam

Stellen Sie vor dem Erstellen eines OAuth-Consumer-Schlüssels Folgendes sicher:

- Ihr Unternehmen ist SAP Jam hinzugefügt und darin konfiguriert.
- Sie verfügen über ein gültiges SAP-Jam-Benutzerkonto, das mit Ihrem Unternehmen in SAP Jam verknüpft ist.
- Sie verfügen über Unternehmensadministratorrechte für Ihr Unternehmen in SAP Jam und die vollständigen Administratorrechte auf der BI-Plattform und im BI-Launchpad.
- Das BI-Launchpad muss bei SAP Jam als OAuth-Client registriert sein, der als Vertreter von BI-Launchpad in SAP Jam fungiert.
- Jeder Benutzer muss bei SAP Jam mit einer eindeutigen E-Mail-Adresse registriert sein, die der Enterprise-E-Mail-Adresse des Benutzers im BI-Launchpad entspricht. Die E-Mail-Adressen werden zwischen der BI-Plattform und SAP Jam zugeordnet.

Microsoft Internet Explorer 11 wird von SAP Jam nicht unterstützt.

1. Wählen Sie in SAP Jam aus dem Menü **Administrator** in der oberen rechten Ecke **Admin** aus.
   Es werden Informationen über Ihr Unternehmen, einschließlich Ihrer SAP-Jam-Lizenz, angezeigt.
2. Wählen Sie **OAuth Clients** im Menü **Admin** aus, und klicken Sie auf **Add OAuth Client**.
3. Geben Sie im Dialogfeld *Register a new OAuth Client* im Feld **Name** den Wert der eindeutigen Identitätsprovider-ID ein, die bei der Konfiguration von SAP Jam in der BI-Plattform erstellt wurde.

   Wenn Ihnen der Wert nicht vorliegt, wenden Sie sich an die Systemadministration für externe Anwendungen.

   In SAP Jam wird der Anwendungsname als Hyperlink (zu der von Ihnen eingegebenen URL) angezeigt, wenn für den Benutzer eine Aktion ausgeführt wird.

   Geben Sie z. B. `<Firmenname>_<SystemID>_<Client>_<Anwendung>` ein.
4. Im Feld **Integration URL** geben Sie die URL für das BI-Launchpad ein.

   In SAP Jam wird der Anwendungsname als Hyperlink zu dieser URL angezeigt, wenn für den Benutzer eine Aktion ausgeführt wird.
5. Geben Sie im Feld **X509 Certificate (Base64)** den Wert des Base64-Zertifikats ein, der bei der Konfiguration von SAP Jam in der BI-Plattform generiert wurde.

   Wenn Ihnen der Wert nicht vorliegt, wenden Sie sich an die Systemadministration für externe Anwendungen.

   Wenn Sie dieses Feld leer lassen, stellt SAP Jam einen geheimen Consumer-Schlüssel bereit.
6. Klicken Sie auf **Speichern**.

Der OAuth-Consumer-Schlüssel wird generiert. Notieren Sie sich den Wert des OAuth-Consumer-Schlüssels, damit die BI-Plattform-Systemadministration ihn verwenden kann.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18.1.3.8.4 SAP-StreamWork-Konfiguration

18.1.3.8.4.1 Abbildung der SAP-StreamWork-Integration

Dieses Diagramm zeigt die erforderlichen BI-Plattform-, SAP-StreamWork- und SAP-StreamWork-Enterprise-Agent-Komponenten, die für die Integration mit SAP StreamWork erforderlich sind.

Der Workflow beschreibt die Schritte zur Integration der Systeme und enthält einen Überblick über die Aktionen, die Benutzer nach der Integration ausführen können:

- Im SAP StreamWork Enterprise Agent können Benutzer Enterprise-Benutzer aus LDAP in SAP StreamWork bereitstellen.
- In der Central Management Console (CMC) der BI-Plattform können Administratoren Benutzer erstellen und diese Enterprise-Benutzern zuzuordnen.
- In BI-Launchpad können Benutzer Aktivitäten erstellen und in einem Browser anzeigen, ohne ein Konto zu erstellen oder sich bei SAP StreamWork anzumelden.
- Außerdem können Benutzer im BI-Launchpad SAP-StreamWork-Feeds anzeigen und darauf reagieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

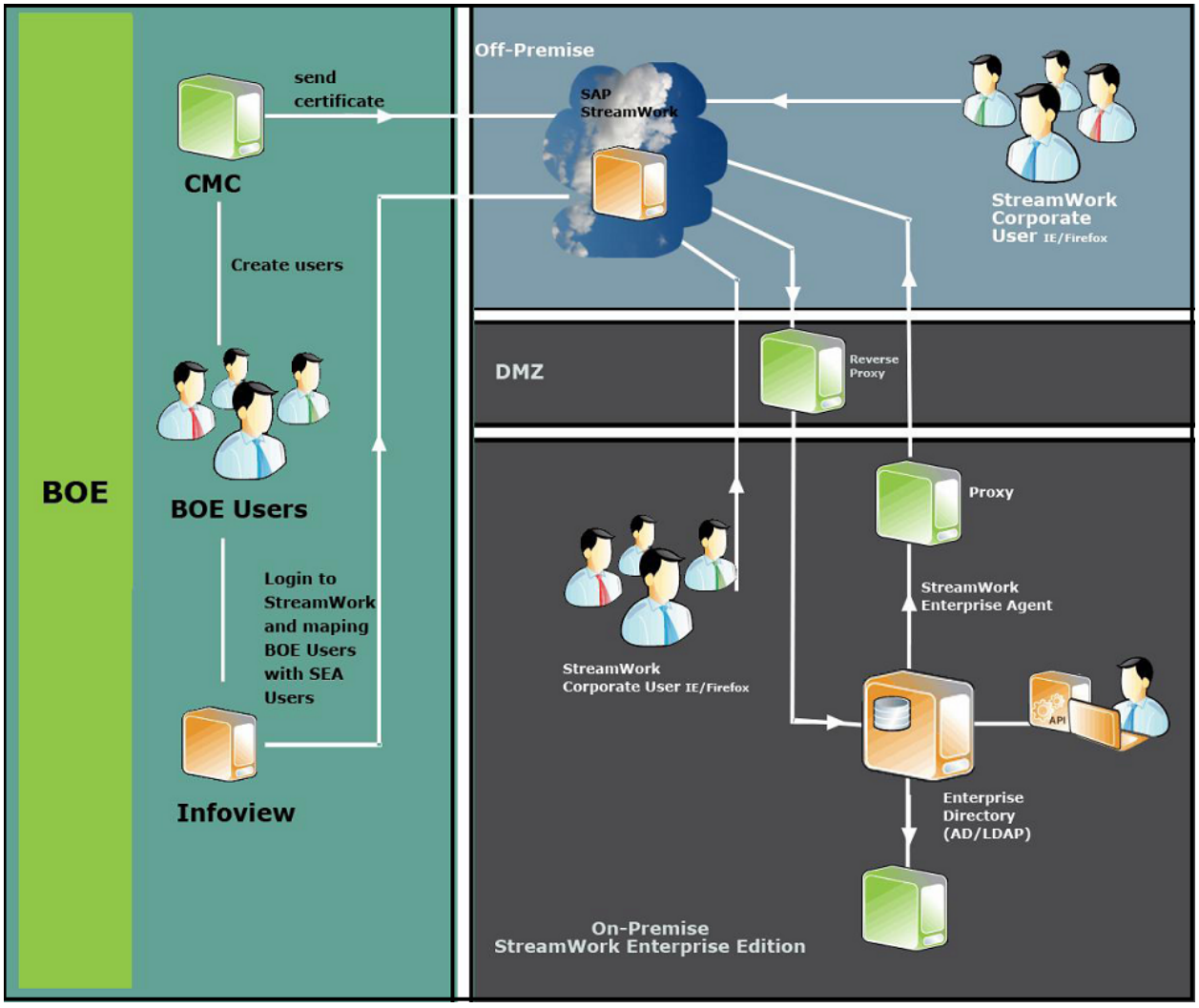


Abbildung 12: Systemlandschaft

18.1.3.8.4.2 Erstellen eines OAuth-Consumer-Schlüssels für SAP StreamWork

Zum Erstellen eines OAuth-Comsumer-Schlüssels benötigen Sie Administratorrechte für die SAP-StreamWork-Enterprise-Organisation.

1. Wählen Sie in der SAP-StreamWork-Administrationskonsole auf der Registerkarte **Admin** die Option **Vertrauenswürdige SAML-IDPs** aus, und melden Sie sich an SAP StreamWork mit einem Konto für einen Administrator der Enterprise-Organisation an.
2. Klicken Sie auf **Identitätsprovider registrieren**.
3. Wählen Sie **Hier klicken, um eine neue administrative OAuth-Anwendung zu erstellen** aus, und stimmen Sie den Nutzungsbedingungen zu.
4. Führen Sie im Fenster **Neue Anwendung registrieren** folgende Aktionen aus:
   a) Geben Sie in das Feld **Anwendungsname** den Namen der in der Integration zu verwendenden Anwendungsinstanz ein.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Diese Information gibt über die Anwendung Aufschluss, die zum Ausführen von Aktionen für einen Benutzer benötigt wird, zum Beispiel zum Posten von SAP-StreamWork-Feeds für einen Benutzer. Benutzer müssen diesen Anwendungsnamen erkennen können.

b) Im Feld **Integration URL** geben Sie die URL für das BI-Launchpad ein.

c) Geben Sie im Feld **Base64 X509 Certificate** den Wert des Base64-Zertifikats ein, der bei der Konfiguration von SAP StreamWork in der Central Management Console (CMC) in der BI-Plattform generiert wurde.

   Wenn Ihnen der Wert nicht vorliegt, wenden Sie sich an die Systemadministration für externe Anwendungen.

5. Klicken Sie auf **Registrieren**.
   Der OAuth-Consumer-Schlüssel wird generiert. Notieren Sie sich den Wert des OAuth-Consumer-Schlüssels, damit die BI-Plattform-Systemadministration ihn verwenden kann.
6. Klicken Sie auf **Zurück**, um die vertrauenswürdigen SAML-Identitätsprovider anzuzeigen.
7. Führen Sie im Fenster *Neuen vertrauenswürdigen SAML-Identitätsprovider registrieren* folgende Aktionen aus:

   a) Geben Sie in das Feld **Anzeigename** einen Namen für die BI-Plattform-Implementierung ein.
   Dieser Name wird Benutzern in SAP StreamWork angezeigt.

   b) Geben Sie im Feld **IDP ID** den Wert des eindeutigen Identitätsproviders ein, der bei der Konfiguration von SAP StreamWork in der BI-Plattform erstellt wurde.

   Wenn Ihnen der Wert nicht vorliegt, wenden Sie sich an die Systemadministration für externe Anwendungen.

   c) Geben Sie im Feld **Base64 X509 Certificate** den Wert des Base64-Zertifikats ein, der bei der Konfiguration von SAP StreamWork in der BI-Plattform generiert wurde.

   Wenn Ihnen der Wert nicht vorliegt, wenden Sie sich an die Systemadministration für externe Anwendungen.

8. Klicken Sie auf **Registrieren**.

18.1.3.8.4.3 Hinzufügen von SAP StreamWork zu einem BI-Arbeitsbereich

SAP StreamWork ist ausgeblendet und muss manuell in der Liste der BI-Launchpad-Module, die Sie zu einem BI-Arbeitsbereich hinzufügen können, eingeblendet werden.

1. Suchen Sie die Datei `C:\BusinessObjects\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.PerformanceManagement\web\WEB-INF\lib\aasdk-ivdm_ext.jar\conf-syst\conf-syst\home-analyticlist.xml`.

   Der Dateiinhalt sollte mit dem folgenden Text beginnen:

```
<?xml version="1.0" encoding="UTF-8"?>
<CHOICE>
<!--<SW_ACTIVITIES NAME="$MSG_SW_ACTIVITIES$" DESCRIPTION="$MSG_SW_ACTIVITIESDESC
$"/>-->
<!--SW_FEED NAME="$MSG_SW_FEED$" DESCRIPTION="$MSG_SW_ACTIVITIESDESC$"/-->
<HOMEINBOX NAME="$MSG_HOMEINBOX$" DESCRIPTION="$MSG_HOMEINBOXDESC$"/>
<HOMEAPPLICATIONS NAME="$MSG_HOMEAPPLICATIONS$"
DESCRIPTION="$MSGHOMEAPPLICATIONSDESC$"/>
<HOMERECENTLYRUNDOCS NAME="$MSG_HOMERECENTLYRUNDOCS$"
DESCRIPTION="$MSG_HOMERECENTLYRUNDOCSDESC$"/>
<HOMERECENTDOCS NAME="$MSG_HOMERECENTDOCS$" DESCRIPTION="$MSG_HOMERECENTDOCSDESC
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
$"/>
<HOMEALERTS NAME="$MSG_ALERTNOTIFICATIONS$"
DESCRIPTION="$MSG_ALERTNOTIFICATIONSDESC$"/>
</CHOICE>
```

2. Entfernen Sie `!--` aus den Zeilen `SW_ACTIVITIES NAME=` und `SW_FEED NAME=`.
3. Starten Sie den Tomcat-Server neu.

In der Liste **BI-Launchpad-Module** in der Modulbibliothek für BI-Arbeitsbereiche in BI-Launchpad wird **SAP-StreamWork-Feed** angezeigt.

18.1.3.9 Verwalten der Einstellungen für die Plattformsuche

Im Bereich *Anwendungen* der CMC in der BI-Plattform können Sie für die Plattformsuchanwendung Einstellungen auf Systemebene festlegen.

Weitere Informationen

Liste der Indizierungsfehler [Seite 743]
Konfigurieren von Anwendungseigenschaften in der CMC [Seite 624]

18.1.3.9.1 Konfigurieren von Anwendungseigenschaften in der CMC

Zum Konfigurieren der Anwendungseigenschaften der Plattformsuche führen Sie die folgenden Schritte aus:

1. Wechseln Sie zum Bereich *Anwendungen* der CMC.
2. Wählen Sie **Anwendung zur Plattformsuche**.
3. Klicken Sie auf **Verwalten** > **Eigenschaften**. Das Dialogfeld *Eigenschaften* wird angezeigt.
4. Konfigurieren Sie die Plattformsucheinstellungen:

Option	Beschreibung
Suchstatistiken	Die Plattformsuche bietet die folgenden Suchstatistiken: ○ Indizierungsstatus: zeigt den Status des Indizierungsvorgangs an. ○ Anzahl der indizierten Dokumente: zeigt die Anzahl der Dokumente an, die indiziert wurden. ○ Zeitstempel der letzten Indizierung: zeigt den Zeitstempel des Zeitpunkts an, an dem das Dokument zum letzten Mal indiziert wurde.
Indizierung starten/Indizierung stoppen	Mit den Optionen "Indizierung starten" und "Indizierung stoppen" können Sie Indizierungsprozesse zu Wartungszwecken starten bzw. stoppen oder wenn Sie vom kontinuierlichen Crawling zum zeitgesteuert verarbeiteten Crawling wechseln möchten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung
	Um die Indizierung zu stoppen, klicken Sie auf **Indizierung stoppen**.
Standardindexgebiets-schema	Die Plattformsuche verwendet das in der CMC angegebene Gebietsschema für die Indizierung aller nicht lokalisierten BI-Dokumente. Nach der Lokalisierung des Dokuments wird die entsprechende Sprachanalyse für die Indizierung verwendet. Die Suche basiert auf dem Produktgebietsschema des Clients, und die Gewichtung wird dem Produktgebietsschema des Clients zugewiesen. Sie können die Gewichtung in den Konfigurationseigenschaften der CMC konfigurieren.
Crawling-Frequenz	Sie können das gesamte BI-Plattform-Repository mithilfe der folgenden Optionen indizieren: ○ Kontinuierliches Crawling: Mit dieser Option wird kontinuierlich indiziert. Das Repository wird jedes Mal indiziert, wenn ein Objekt hinzugefügt, geändert oder gelöscht wird. Die Option bietet Ihnen die Möglichkeit, den aktuellen Inhalt der BI-Plattform anzuzeigen bzw. damit zu arbeiten. Das standardmäßig aktivierte fortlaufende Crawling aktualisiert ständig das Repository mit den von Ihnen ausgeführten Aktionen. Das kontinuierliche Crawling erfordert keinen Benutzereingriff und verkürzt die zur Indizierung eines Dokuments benötigte Zeit. ○ Zeitgesteuert verarbeitetes Crawling: Mit dieser Option wird auf der Grundlage eines Zeitplans indiziert, der durch die Optionen der zeitgesteuerten Verarbeitung festgelegt wird. Weitere Informationen darüber, wie Objekte zeitgesteuert verarbeitet werden, finden Sie im Abschnitt *Zeitgesteuertes Verarbeiten eines Objekts* unter "Plattformsuche" in der *Onlinehilfe für die CMC von SAP BusinessObjects Business Intelligence*. Hinweis ○ Wenn Sie **Zeitgesteuert verarbeitetes Crawling** auswählen und **Wiederholung** auf eine andere Option als **Jetzt** setzen, zeigt die Plattformsuche das Datum und den Zeitstempel für die nächste zeitgesteuerte Indizierung des Dokuments an. ○ Wenn Sie **Kontinuierliches Crawling** auswählen, wird die Schaltfläche **Indizierung starten** aktiviert und die Schaltfläche **Indizierung stoppen** deaktiviert. ○ Nach Abschluss der zeitgesteuerten Verarbeitung ist die Schaltfläche **Indizierung stoppen** deaktiviert.
Index-Speicherort	Die Indizes werden in freigegebenen Ordnern an den folgenden Speicherorten abgelegt:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung
	○ Speicherort des Hauptindex (Indizes, Rechtschreibprüfungen): An diesem Speicherort werden der Hauptindex und der Rechtschreibprüfungsindex gespeichert. Bei einer Suche werden die anfänglichen Ergebnisse mit dem Hauptindex und die Vorschläge mit den Rechtschreibprüfungsindizes abgerufen. In einer geclusterten Implementierung der BI-Plattform sollte sich dieser Speicherort in einem freigegebenen Dateisystem befinden, das für alle Knoten im Cluster zugänglich ist. ○ Speicherort für persistente Daten (Inhaltsspeicher): Der Inhaltsspeicher befindet sich an diesem Speicherort. Er wird auf Basis des Speicherorts des Hauptindex erstellt und bleibt mit diesem synchronisiert. Der Inhaltsspeicher dient zum Generieren von Facetten und zur Verarbeitung der anfänglichen Treffer, die aus dem Speicherort des Hauptindex generiert wurden. In einer geclusterten BI-Plattform-Implementierung werden Inhaltsspeicher auf jedem Knoten generiert. Der Speicherort für persistente Daten ist der einzige Indexspeicherort, der von der geclusterten Umgebung betroffen ist, da er die Inhaltsspeicherordner enthält. Wenn ein Rechner nur über einen Suchdienst verfügt, gibt es auch nur einen Speicherort für den Inhaltsspeicher. Zum Beispiel: {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores. Wenn jedoch in einer geclusterten Umgebung mehrere Suchdienste vorhanden sind, gibt es für jeden Suchdienst einen Speicherort für den Inhaltsspeicher. Sollten Sie zwei Instanzen eines Servers ausführen, lauten die Speicherorte für den Inhaltsspeicher: 1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores. 2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name 1>\ContentStores. ○ Kein persistenter Datenspeicherort (temporäre Ersatzdateien, Delta-Indizes): An diesem Speicherort werden die Delta-Indizes erstellt und temporär gespeichert, bevor sie mit dem Hauptindex zusammengeführt werden. Die Indizes von diesem Speicherort werden nach dem Zusammenführen mit dem Hauptindex gelöscht. Außerdem werden an diesem Speicherort Ersatzdateien (Ausgabe der Extraktoren) erstellt und temporär gespeichert, bis sie in Delta-Indizes konvertiert werden. **Hinweis** ○ Alle Speicherorte von Indizes müssen freigegeben sein. ○ Sie müssen auf **Indizierung stoppen** klicken, um den Indexspeicherort zu ändern. ○ Wenn Sie einen Indexspeicherort ändern, kopieren Sie den Inhalt an einen neuen Speicherort, sonst gehen die vorhandenen Indexinformationen verloren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung

Indizierungsebene	Sie könne den Suchinhalt abstimmen, indem Sie die Indizierungsebene wie folgt festlegen:
	○ Plattform-Metadaten: Ein Index wird ausschließlich für die Plattform-Metadateninformationen wie Titel, Schlüsselwörter und Beschreibungen von Dokumenten erstellt.
	○ Plattform- und Dokument-Metadaten: Dieser Index beinhaltet sowohl die Plattform- als auch die Dokument-Metadaten. Zu den Dokument-Metadaten gehören Erstellungsdatum, Änderungsdatum und Name des Autors.
	○ Gesamter Inhalt: Dieser Index beinhaltet die Plattform-Metadaten, Dokument-Metadaten und andere Inhalte wie:
	  ○ den tatsächlichen Inhalt des Dokuments
	  ○ den Inhalt von Eingabeaufforderungen und Wertelisten
	  ○ Diagramme, Grafiken und Beschriftungen
	Hinweis
	Wenn Sie die Indizierungsebene ändern, wird die Indizierung für die Regenerierung des gesamten BI-Plattform-Repositorys initialisiert.

Inhaltstypen	Für die Indizierung stehen folgende Inhaltstypen zur Auswahl: ○ Crystal Reports ○ Web Intelligence ○ Universum ○ BI-Arbeitsbereich ○ Microsoft PowerPoint ○ Adobe Acrobat ○ Rich Text ○ Text ○ Microsoft Word ○ Microsoft Excel
Index neu erstellen	Mit dieser Option wird der gesamte Index gelöscht und das gesamte Repository neu indiziert. Sie können die Option **Index neu erstellen** unabhängig davon auswählen, ob die Indizierung ausgeführt wird oder gestoppt wurde. Der vorhandene Index wird gelöscht, wenn Sie Ihre Änderungen auf der Eigenschaftenseite speichern. Wenn die Indizierung jedoch derzeit gestoppt ist, wird der Index erst dann wieder neu erstellt, wenn Sie die Indizierung erneut starten. Falls die Dokumente nicht mit der Plattformsuche neu indiziert werden sollen, heben Sie die Auswahl der Option **Index neu erstellen** auf, bevor Sie auf **Indizierung starten** klicken.
Von der Indizierung ausgeschlossene Dokumente	Die Option **Von der Indizierung ausgeschlossene Dokumente** schließt Dokumente von der Indizierung aus. Es könnte z. B. sein, dass Sie extrem große Crys-

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung
	tal-Reports-Berichte von der Suche ausschließen möchten, um die Report-Application-Server-Ressourcen nicht zu überlasten. Außerdem möchten Sie möglicherweise Veröffentlichungen mit Hunderten von personalisierten Berichten indizieren. Durch Ausschließen bestimmter Dokumente können Sie den Zugriff auf diese Dokumente über die Plattformsuche verhindern. Wenn ein Dokument jedoch indiziert wurde, bevor es dieser Gruppe zugewiesen wurde, kann es weiterhin durchsuchbar sein. Damit sichergestellt ist, dass die Dokumente in der Gruppe **Von der Indizierung ausgeschlossene Dokumente** nicht durchsuchbar sind, müssen Sie den Index neu erstellen. Das Administratorkonto hat standardmäßig vollständige Kontrolle über die Option **Von der Indizierung ausgeschlossene Dokumente**. Andere Benutzer mit den folgenden Rechten können lediglich Dokumente zu der Gruppe **Von der Indizierung ausgeschlossene Dokumente** hinzufügen: ○ Ansichts- und Bearbeitungsrechte für die Kategorie ○ Direkte Bearbeitung des Dokuments

5. Klicken Sie auf **Speichern und schließen**.

> **Hinweis**
>
> Wenn ein Benutzer die Option **Index neu erstellen** nicht auswählt und die Indizierungsebene ändert oder Extraktoren aktiviert oder deaktiviert, wird der Index schrittweise aktualisiert, ohne dass der vorhandene Index gelöscht wird.

18.1.3.10 Konfigurieren der BEx-Webintegration

BEx Web Applications sind webbasierte Anwendungen aus Business Explorer (BEx) von SAP NetWeaver Business Warehouse (BW) für die Datenanalyse, Berichterstellung und analytische Verwendung im Web.

Business Explorer ist die Business-Intelligence-Suite von SAP NetWeaver, die flexible Berichterstellungs- und Analysetools zur besseren strategischen Analyse und Entscheidungsfindung bietet. Diese Tools stellen Abfrage-, Berichterstellungs- und Analysefunktionen bereit. Als Mitarbeiter mit Zugriffsrechten können Sie historische oder aktuelle Daten auf verschiedenen Detailebenen und aus unterschiedlichen Blickwinkeln auswerten, sowohl im Web als auch in Microsoft Excel.

Der Zugriff auf die Daten erfolgt über das SAP NetWeaver Portal oder über das BI-Launchpad von SAP BI. Autoren von BEx Web Applications können die Web Applications direkt im BI-Launchpad aus BEx Web Application Designer öffnen.

Zur Integration von BEx Web Applications in die BI-Plattform sind die folgenden Konfigurationsschritte auszuführen:

1. Richten Sie einen Server für die BEx Web Applications in der Central Management Console (CMC) ein.

   Sie können entweder einen allgemeinen oder eigenständigen Server für die BEx Web Applications verwenden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Tipp**
>
> Es empfiehlt sich, einen eigenständigen Server für die BEx Web Applications einzurichten, da der allgemeine Server normalerweise von vielen anderen Diensten verwendet wird.

2. Konfigurieren Sie die Servereinstellungen.
3. Überprüfen Sie die Verbindung zum BW-System.
4. Um sicherzustellen, dass Autoren BEx Web Applications direkt im BI-Launchpad aus dem BEx Web Application Designer ausführen können, nehmen Sie die entsprechenden Einstellungen in der Tabelle **Connected Portals** (Angeschlossene Portale) (`RSPOR_T_PORTAL`) im BW-System vor.

Nach der Konfiguration des BI-Servers können Benutzer BEx Web Applications in BI-Launchpad öffnen. Dort haben sie die Möglichkeit, durch die Daten zu navigieren und die BEx Web Applications als Lesezeichen in den Webbrowser-Favoriten zu speichern.

> **Einschränkung**
>
> Die Integration wird ab den unten aufgeführten Releases von SAP NetWeaver unterstützt:
>
> SAP NetWeaver 7.0 Enhancement Package 1 Support Package Stack 8
>
> SAP NetWeaver 7.3 Support Package Stack 1
>
> Da der SAP NetWeaver Java-Stack für diese Integration nicht erforderlich ist, gelten die folgenden Einschränkungen:
>
> Information Broadcasting wird nicht unterstützt.
>
> Da das Portal und Knowledge Management von SAP NetWeaver nicht benötigt werden, werden die Dokumentintegration und die Verwendung von Portalmotiven in BEx Web Applications nicht unterstützt.
>
> Das Web Item **Bericht** wird nicht unterstützt. Es wird empfohlen, SAP Crystal Reports für die formatierte Berichterstellung zu verwenden.
>
> Um Druckversionen von BEx Web Applications zu erstellen, wird die Exportbibliothek für SAP Business Explorer verwendet. Adobe Document Services (ADS) stehen nicht zur Verfügung.
>
> Die BEx Web Applications, die in die BI-Plattform integriert sind, können nur Datenquellen enthalten, die im BW-Mastersystem gespeichert sind. In der Systemverwaltung definieren Sie, welches System als BW-Mastersystem in der BI-Plattform konfiguriert ist.
>
> Die Einzelanmeldung zwischen der BI-Plattform und dem SAP-NetWeaver-BW-System ist nicht aktiviert. Benutzer von BEx Web Applications werden bei jeder BI-Plattform-Sitzung aufgefordert, sich bei dem entsprechenden SAP BW-Mastersystem anzumelden.
>
> Bericht-Berichtschnittstelle von und zu BEx Web Applications wird nicht unterstützt. Entsprechende Befehle werden nicht ausgeführt.
>
> Auf BEx-Querys oder Abfrageansichten basierende und mit SAP BusinessObjects Dashboards erstellte Dashboards werden nicht unterstützt.

Weitere Informationen zu den Funktionen von BEx Web Applications finden Sie im SAP Help Portal unter *http://help.sap.com*: **SAP NetWeaver 7.3** > **SAP-NetWeaver-Bibliothek: Funktionsorientierte Sicht** > **Business Warehouse** > **SAP Business Explorer** > **BEx Web** > **Analyse und Reporting: BEx Web Applications**.

Weitere Informationen zum Abrufen und Speichern von BEx Web Applications in BI-Launchpad finden Sie im *Benutzerhandbuch für BI-Launchpad* unter *http://help.sap.com*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Starten eines Servers für BEx Web Applications [Seite 630]
Starten eines eigenständigen Servers für BEx Web Applications [Seite 630]
Konfigurieren der Servereinstellungen [Seite 630]
Überprüfen der Verbindung zum BW-System [Seite 631]
Konfigurieren einer Verbindung zwischen BEx Web Application Designer und der BI-Plattform [Seite 632]

18.1.3.10.1 Starten eines Servers für BEx Web Applications

Vor Ausführung dieser Aufgabe muss der Adaptive Processing Server gestoppt werden.

1. Melden Sie sich bei der Central Management Console (CMC) an.
2. Wählen Sie **Server** aus.
3. Klappen Sie den Knoten **Dienstkategorien** auf, und wählen Sie **Analysis-Dienste** aus.
4. Wählen Sie **Adaptive Processing Server** und dann **Dienste auswählen** im Kontextmenü aus.
5. Verschieben Sie **BEx-Web-Applications-Dienst** aus der Liste **Verfügbare Dienste** in die Liste "Dienste" auf der rechten Seite.
6. Starten Sie den BEx-Web-Applications-Dienst neu, indem Sie den Adaptive Processing Server neu starten.

18.1.3.10.2 Starten eines eigenständigen Servers für BEx Web Applications

1. Melden Sie sich bei der Central Management Console (CMC) an.
2. Wählen Sie **Server** aus.
3. Klappen Sie den Knoten **Dienstkategorien** auf, und wählen Sie **Analysis Services**.
4. Wählen Sie **Adaptive Processing Server** und dann **Server klonen** im Kontextmenü aus.
5. Geben Sie einen Namen für den Server ein (beispielsweise `AdaptiveProcessingServer`), und wählen Sie den gewünschten Knoten im Feld **Für Knoten klonen** aus.
6. Markieren Sie den geklonten Server, und wählen Sie **Dienste auswählen** im Kontextmenü aus.
7. Wählen Sie **BEx-Web-Applications-Dienst** in der Liste **Verfügbare Dienste**, und verschieben Sie ihn in die Dienste-Liste auf der rechten Seite.
8. Starten Sie den BEx-Web-Applications-Dienst, indem Sie den neuen Adaptive Processing Server starten.

18.1.3.10.3 Konfigurieren der Servereinstellungen

1. Melden Sie sich bei der Central Management Console (CMC) an.
2. Wählen Sie **Server** aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Klappen Sie den Knoten **Dienstkategorien** auf, und wählen Sie **Analysis Services**.
4. Wählen Sie den Server aus, der den BEx-Web-Applications-Dienst hostet, und wählen Sie im Kontextmenü die Option **Eigenschaften**.
5. Nehmen Sie unter **Konfiguration des BEx-Web-Applications-Diensts** im Bereich *BEx-Web-Applications-Dienst* die folgenden Einstellungen vor:
   a) Prüfen Sie die maximale Anzahl an Clientsitzungen, und ändern Sie diese bei Bedarf.
   b) Geben Sie unter **SAP BW-Mastersystem** den Namen der OLAP-Verbindung zum BW-System, das Sie in der BI-Plattform erstellt haben, ein. Der Standardname lautet **SAP_BW**.
   c) Geben Sie den Namen der **RFC-Destination des JCo-Servers** ein, die Sie im BW-System unter **Configuration of RFC Connections** (Konfiguration der RFC-Verbindungen) eingegeben haben (Transaktionscode `sm59`).
   d) Geben Sie den Namen des **Gateway-Hosts des JCo-Servers** ein, den Sie im BW-System unter **Configuration of RFC Connections** (Konfiguration der RFC-Verbindungen) definiert haben (Transaktionscode `sm59`).
   e) Geben Sie den Namen des **Gateway-Diensts des JCo-Servers** ein, den Sie im BW-System unter **Configuration of RFC Connections** (Konfiguration der RFC-Verbindungen) definiert haben (Transaktionscode `sm59`).
   f) Prüfen Sie die **Verbindungsanzahl des JCo-Servers**, und ändern Sie diese bei Bedarf.
6. Wählen Sie **Speichern & schließen**.
7. Wählen Sie den Server aus, der den BEx-Web-Applications-Dienst hostet, und wählen Sie im Kontextmenü **Server neu starten**.

   Zur Übernahme der ausgewählten Einstellungen müssen Sie den Server neu starten.

> **Hinweis**
>
> Vor dem Neustart des Servers muss jedoch die RFC-Destination im ABAP-System erstellt werden.

Weitere Informationen

Erstellen einer RFC-Destination im ABAP-System [Seite 633]

18.1.3.10.4 Überprüfen der Verbindung zum BW-System

1. Melden Sie sich bei der Central Management Console (CMC) an.
2. Wählen Sie **OLAP-Verbindungen**.
3. Prüfen Sie, ob eine Verbindung zum BW-System hergestellt wurde. Andernfalls klicken Sie auf die Schaltfläche **Neue Verbindung**, um eine neue Verbindung einzurichten. Der Standardname der Verbindung lautet `SAP_BW`. Sie können auch einen anderen Namen eingeben.
4. Stellen Sie sicher, dass die Option **Vordefiniert** unter **Authentifizierung** ausgewählt ist und Sie die erforderlichen Eingaben für Benutzer und Kennwort vorgenommen haben.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Dieses Benutzerkonto ist für die RFC-Destination des JCo-Servers erforderlich, die die Integration von BEx Web Application Designer, des BW-Systems und der BI-Plattform ermöglicht.

> **Tipp**
>
> Um die Verbindung sicher zu gestalten, stellen Sie sicher, dass nur Administratoren über entsprechende Zugriffsrechte verfügen.
>
> 1. Klicken Sie hierzu mit der rechten Maustaste auf die Verbindung zum BW-System (Standardname `SAP_BW`), und wählen Sie **Benutzersicherheit**.
> 2. Nehmen Sie die erforderlichen Sicherheitseinstellungen vor, und erteilen Sie Zugriffsrechte wenn möglich nur an Administratoren.

18.1.3.10.5 Konfigurieren einer Verbindung zwischen BEx Web Application Designer und der BI-Plattform

Um sicherzustellen, dass Autoren BEx Web Applications direkt im BI-Launchpad aus dem BEx Web Application Designer ausführen können, müssen Sie die entsprechenden Einstellungen in der Tabelle **Connected Portals** (Angeschlossene Portale) (`RSPOR_T_PORTAL`) im BW-System vornehmen.

1. Rufen Sie im BW-System die Transaktion `SM30` (**Table View Maintenance** (Tabellenansicht-Pflege) auf.
2. Geben Sie unter **Table/View** (Tabelle/Sicht) `RSPOR_T_PORTAL` ein.
3. Wählen Sie **Maintain** (Pflegen).
4. Wählen Sie zum Erstellen eines neuen Eintrags die Option **New Entries** (Neue Einträge).
5. Nehmen Sie die folgenden Einstellungen vor:
   a) Um die Integration zwischen dem BW-System und der BI-Plattform sicherzustellen, müssen Sie in Transaktion `SM59` eine RFC-Destination erstellen. Geben Sie diese RFC-Destination unter **Destination** (RFC-Destination) ein.
   b) Wählen Sie **Standard Portal** (Standard-Portal). Dadurch wird gewährleistet, dass Web Applications in Web Application Designer immer in der BI-Plattform aufgerufen werden.
   c) Geben Sie unter **URL Prefix** (URL-Präfix) die URL zum Web Application Container Server (WACS) der BI-Plattform ein, samt Protokoll, Hostname und Port. Beispiel: `http://<WACS><Domäne>:<Port>`.
   d) Wählen Sie unter **Platform** (Plattform) die Option **BOE**.
   e) Wählen Sie **Use SAP Export Lib (PDF)** (SAP Export Lib (PDF) verwenden), wenn die Exportbibliothek für SAP Business Explorer aktiviert werden soll. Somit können PDF-, PostScript- und PCL-Dateien aus BEx Web Applications exportiert werden.
6. Speichern Sie Ihre Eingaben.

Weitere Informationen

Erstellen einer RFC-Destination im ABAP-System [Seite 633]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18.1.3.10.5.1 Erstellen einer RFC-Destination im ABAP-System

Zur Integration des BW-Systems und der BI-Plattform benötigen Sie eine RFC-Destination. Mithilfe dieser RFC-Destination kann das BW-System mit der BI-Plattform kommunizieren.

1. Rufen Sie **Configuration of RFC Connections** (Konfiguration der RFC-Verbindungen) mit dem Transaktionscode `SM59` auf.
2. Wählen Sie **Create** (Anlegen).
3. Geben Sie Details zur RFC-Destination ein:
   a) Geben Sie einen Namen für die RFC-Destination ein.
   b) Wählen Sie als Verbindungstyp **T für TCP/IP** (T für TCP/IP-Verbindung) aus.
   c) Geben Sie eine Beschreibung ein.

      Sie können die Sprache der RFC-Destination entsprechend ändern.
   d) Wählen Sie unter **Technical Settings** (Technische Einstellungen) die Option **Registered Server Program** (Registriertes Serverprogramm) als Aktivierungstyp aus.
   e) Geben Sie unter **Technical Settings** (Technische Einstellungen) die Programm-ID ein.

      Die Programm-ID muss mit der Programm-ID (JCo-Server-RFC-Destination) übereinstimmen, die Sie beim Erstellen der Destination für dieses BW-System im BI-Server angegeben haben.
   f) Geben Sie unter **Technical Settings** (Technische Einstellungen) unter **Gateway Options** (Gateway-Optionen) den Gateway-Host und den Gateway-Service ein, anhand dessen der BI-Plattform-Server mit dem BW-System kommuniziert.
4. Aktivieren Sie auf der Registerkarte **Logon & Security** (Anmeldung & Sicherheit) die Option **Send SAP Logon Ticket** (SAP-Anmeldeticket senden).
5. Speichern Sie Ihre Eingaben.

Weitere Informationen

Konfigurieren der Servereinstellungen [Seite 630]

18.1.3.11 Konfigurieren von SAP-HANA-Einzelanmeldung

Im Bereich *Anwendungen* der CMC in der BI-Plattform können Sie die Einzelanmeldung für SAP-HANA-Datenbankverbindungen konfigurieren. SSO wird anhand von SAML (Security Assertion Markup Language) implementiert.

Nachdem Sie eine BI-Plattform-Sitzung eingerichtet haben, können Sie ein SAML-Ticket generieren, das für die Anmeldung an SAP HANA verwendet werden kann, ohne dass der Benutzer ein Kennwort eingeben muss.

Nachfolgend ist der grundlegende Ablauf zum Herstellen einer Verbindung zu SAP-HANA-Datenquellen beschrieben:

1. Ein Administrator konfiguriert in der CMC eine vertrauenswürdige Verbindung zwischen SAP HANA und der BI-Plattform.
2. Ein Benutzer meldet sich mit einem unterstützten Authentifizierungsprovider an der BI-Plattform an.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Sofern die Benutzer-IDs von SAP HANA und der BI-Plattform übereinstimmen, kann die BI-Plattform eine SAML-Assertion generieren, die von SAP HANA akzeptiert werden kann, um eine Verbindung für den aktuellen Benutzer herzustellen. Die an SAP HANA übergebene Benutzer-ID ist die BI-Plattform-Benutzer-ID für den angemeldeten Benutzer.
4. Eine BI-Plattform-Clientanwendung stellt eine SAP-HANA-Verbindung her.

> **Hinweis**
>
> Bevor Sie SAP-HANA-Einzelanmeldung mit SAML konfigurieren, müssen Sie SSL auf dem SAP-HANA-Rechner konfigurieren. Ausführliche Informationen finden Sie in Ihrer SAP-HANA-Dokumentation.

18.1.3.11.1 Erstellen einer SAP-HANA-Verbindung

1. Rufen Sie die betreffenden SAP-HANA-Datenbankparameter ab.
   a) Öffnen Sie die SAP-HANA-Studio-Anwendung.
   b) Öffnen Sie die Seite "Eigenschaften" für Ihr System, und suchen Sie die URL für die Datenbankverbindung.
   c) Notieren Sie den Namen des Hostrechners und die Portnummer.

      Sie benötigen diese Informationen in Schritt 2.
2. Konfigurieren Sie eine SAP-HANA-Verbindung in der BI-Plattform.
   a) Wechseln Sie in den Bereich *Anwendungen* der CMC, und doppelklicken Sie auf **HANA Authentifizierung**.
   b) Klicken Sie im Dialogfeld *HANA-Authentifizierung* auf die Schaltfläche **Verbindung erstellen**.
      Das Dialogfeld *HANA-Authentifizierungsverbindung erstellen* wird geöffnet.
   c) Geben Sie den Namen und die Portnummer des Hostrechners ein, die sie in Schritt 1 notiert haben.
   d) Geben Sie im Feld *Eindeutige ID des Identitätsproviders* einen Wert ein, der für Ihre BI-Plattform-Implementierung verwendet wird.
   e) Klicken Sie auf **Ausführen**.
      Im Feld *Base64-Zertifikat des Identitätsproviders* wird ein Zertifikat erstellt.
3. Konfigurieren Sie Ihre SAP-HANA-Implementierung.
   a) Klicken Sie im SAP HANA Studio mit der rechten Maustaste auf das SAP-HANA-System, und klicken Sie auf **Eigenschaften**.
   b) Wählen Sie **SAML-Konfiguration** aus.
   c) Klicken Sie auf **Hinzufügen**.
   d) Wählen Sie im Dialogfeld **SAML-Identitätsprovider erstellen** die Option **Aus Zertifikat lesen** aus.
   e) Klicken Sie auf **Datei öffnen**, damit die DN-Werte eingegeben werden.
   f) Klicken Sie auf **OK**.
   g) Starten Sie SAP HANA neu.
4. Testen Sie die SAP-HANA-Konfiguration.
   a) Wechseln Sie zum Bereich *Anwendungen* der CMC, und doppelklicken Sie auf **HANA-Authentifizierung**.
   b) Öffnen Sie im Dialogfeld *HANA-Authentifizierung* die Verbindung, die Sie in Schritt 2 erstellt haben.
      Das Dialogfeld *HANA-Authentifizierungsverbindung bearbeiten* wird geöffnet.
   c) Geben Sie unter *Verbindung für folgenden Benutzer testen* einen Benutzernamen ein, und klicken Sie auf die Schaltfläche **Verbindung testen**, um zu verifizieren, dass Ihre Verbindungseinstellungen gültig sind.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Geben Sie z.B. den Benutzernamen **Administrator** ein. Wenn die Einstellungen ungültig sind, wird eine Fehlermeldung angezeigt. Sie können zum Beheben des Fehlers folgende Schritte ausführen:

- Stellen Sie sicher, dass kein anderes Zertifikat in der Datei `trust.pem` einen Betreff oder Aussteller mit demselben CN-Eigenschaftswert enthält. Um die Komponenten des Zertifikats einzusehen, suchen Sie im Internet nach "x509 certificate decoder", um einen Zertifikat-Decoder zu suchen.
- Geben Sie die folgenden Befehle ein, um die HANA-seitige Konfiguration zu prüfen:

```
select * from "SAML_PROVIDERS"
select user_name, is_saml_enabled from users where user_name =
'<UserName>'
select * from "PUBLIC"."SAML_USER_MAPPINGS"
```

- Wenn beim Konfigurieren von SSO für SAP HANA ein SAML-Authentifizierungsfehler angezeigt wird, können Sie zum Beheben des Fehlers folgende Schritte ausführen:
  1. Setzen Sie in der Datei `indexserver.ini` den Parameter `sslCreateSelfSignedCertificate` auf **`false`**.
  2. Legen Sie in derselben Datei für die Parameter `sslKeyStore` und `sslTrustStore` die Verwendung von absoluten Pfaden fest.
  3. Generieren Sie die Dateien `key.pem` und `trust.pem` neu.

Wenn die Datei `key.pem` nicht im Verzeichnis `.ssl` enthalten ist, wurde SAP HANA nicht richtig für die Verwendung von SSL konfiguriert.

18.1.3.11.2 SAP-HANA-Verbindungseinstellungen

In der Tabelle unten sind die in der CMC verfügbaren Einstellungen zur Konfiguration von SAP-HANA-Verbindungen zusammengefasst.

Einstellung	Beschreibung
HANA-Hostname	Geben Sie den Namen Ihres SAP-HANA-Hosts an.
HANA-Port	Geben Sie die Portnummer für Ihren SAP-HANA-Host an.
Eindeutige ID des Identitätsproviders	Ein eindeutiger Name in einer bestimmten HANA-Installation. Ordnungsgemäß signierte Tickets von diesem Identitätsprovidernamen werden von der HANA-Installation für Anmeldungen akzeptiert.
Base64-Zertifikat des Identitätsproviders	Wenn Sie auf **Generieren** klicken, wird im Feld *Base64-Zertifikat des Identitätsproviders* ein Zertifikat erstellt. Kopieren Sie dieses Zertifikat in die Datei `trust.pem` in Ihrer SAP-HANA-Implementierung. Dieses Zertifikat stellt die Vertrauensstellung zwischen SAP HANA und der BI-Plattform her. Der externe Identitätsprovider selbst wird mit einem X509-Zertifikat identifiziert, mit dem alle Identitätssicherstellungen signiert werden. Das Zertifikat muss Base64-codiert sein.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18.2 Verwalten von Anwendungen über BOE.war-Eigenschaften

18.2.1 BOE-WAR-Datei

Sie können die Einstellungen für die BI-Plattform-Webanwendungen ändern, indem Sie die Standardeigenschaften für die Datei "BOE.war" überschreiben. Diese Datei ist auf dem Rechner implementiert, auf dem der Webanwendungsserver gehostet wird. Ausführliche Informationen darüber, wie die Datei implementiert wird, finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.

Die in der Datei BOE.war enthaltenen Eigenschaften kontrollieren Angaben für das standardmäßige Anmeldeverhalten, Standardauthentifizierungsmethoden und Einstellungen für die Einzelanmeldung. Sie können zwei Typen von Eigenschaften angeben:

- Globale Eigenschaften: Diese Eigenschaften haben Auswirkungen auf alle in der Datei BOE.war enthaltenen Webanwendungen.
- Anwendungsspezifische Eigenschaften: Diese Einstellungen der Eigenschaften haben nur Auswirkungen auf eine bestimmte Webanwendung.

Zum Ändern der Standardeigenschaften speichern Sie die neuen Einstellungen von globalen oder anwendungsspezifischen Eigenschaften in dem Konfigurationsverzeichnis "custom". Das Verzeichnis befindet sich standardmäßig in: `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Ändern Sie die Eigenschaften nicht im Verzeichnis `config\default`.

> **Hinweis**
>
> Auf manchen Webanwendungsservern wie der mit der BI-Plattform gebündelten Tomcat-Version können Sie direkt auf die Datei "BOE.war" zugreifen. In diesem Fall lassen sich benutzerdefinierte Einstellungen direkt festlegen, ohne dass die WAR-Datei deinstalliert werden muss. Wenn Sie nicht direkt auf die implementierten Webanwendungen zugreifen können, müssen Sie die Datei deinstallieren, anpassen und danach wieder implementieren. Weitere Informationen finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.

18.2.1.1 Globale Eigenschaften für BOE.war

Die folgende Tabelle enthält eine Liste der Einstellungen der `global.properties`-Standarddatei für BOE.war.

Um Einstellungen zu überschreiben, erstellen Sie in `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` eine neue Datei.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Einstellung	Standardwerte	Beschreibung
`persistentcookies.enabled`	`persistentcookies.enabled=true`	Aktivieren oder Deaktivieren persistenter Cookies auf der Webanwendungsanmeldeseite.
`siteminder.authentication`	`siteminder.authentication=secLDAP`	Angeben der mit SiteMinder zu verwendenden Authentifizierungsmethode. Nur die Optionen "secLDAP" und "secwinAD" sind verfügbar.
`siteminder.enabled`	`siteminder.enabled=false`	Aktivieren und Deaktivieren der Authentifizierung mit SiteMinder.
`sso.enabled`	`sso.enabled=false`	Aktiviert und deaktiviert die Einzelanmeldung (SSO) bei der BI-Plattform.
`sso.sap.primary`	`sso.sap.primary=false`	Setzen Sie diese Einstellung auf `true`, wenn Sie die SAP-Einzelanmeldung als primären Einzelanmeldungsmechanismus für die Anwendung verwenden möchten. Gilt nur, wenn sowohl die SAP- als auch die SiteMinder-Einzelanmeldung verwendet werden.
`max.tree.children.threshold`	`max.tree.children.threshold=200`	Gibt den Schwellenwert an, bei dem in der Baumstruktursteuerung nicht alle Knoten angezeigt werden, sondern die Meldung "Zu viele untergeordnete Elemente".
`trusted.auth.shared.secret`	Keine	Angeben des Sitzungsvariablennamens, mit dessen Hilfe der geheime Schlüssel für die vertrauenswürdige Authentifizierung abgerufen wird. Nur relevant, wenn der gemeinsame geheime Schlüssel über die Websitzung übergeben wird.
`trusted.auth.user.param`	Keine	Angeben der Variable, die zum Abrufen des Benutzernamens für die vertrauenswürdige Authentifizierung verwendet wird; folgende Werte sind zulässig: • `Header` • `URL-Parameter` • `Cookie` • `Session`
`trusted.auth.user.retrieval`	Keine	Angeben der Methode an, die zum Abrufen des Benutzernamens für die vertrauenswürdige Authentifizierung verwendet wird; die Methode kann auf einen der folgenden Werte festgelegt werden: • `"REMOTE_USER"` • `"HTTP_HEADER"` • `"COOKIE"` • `"QUERY_STRING"` • `"WEB_SESSION"` • `"USER_PRINCIPAL"` Um die vertrauenswürdige Authentifizierung zu deaktivieren, setzen Sie dies auf einen leeren Wert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Einstellung	Standardwerte	Beschreibung
trusted.auth.user.namespace.enabled	trusted.auth.user.namespace.enabled=false	Aktivieren und Deaktivieren der dynamischen Bindung von Aliasen zu vorhandenen Benutzerkonten. Wenn diese Eigenschaft auf true gesetzt ist, werden Benutzer von der vertrauenswürdigen Authentifizierung mithilfe der Aliasbindung bei der BI-Plattform authentifiziert. Dank Aliasbindung kann der Anwendungsserver als SAML-Dienstprovider fungieren. Daher wird die vertrauenswürdige Authentifizierung aktiviert, um die SAML-Einzelanmeldung beim System bereitzustellen. Wenn false eingestellt ist, authentifiziert die vertrauenswürdige Authentifizierung Benutzer mithilfe der Namensübereinstimmung.
vintela.enabled	vintela.enabled=false idm.realm=YOUR_REALM idm.princ=YOUR_PRINCIPAL idm.allowUnsecured=true idm.allowNTLM=false idm.logger.name=simple idm.logger.props=error-log.properties	Zum Aktivieren oder Deaktivieren von Vintela-Einstellungen für die Windows AD-Authentifizierung.
pinger.showWarningDialog.cmc	pinger.showWarningDialog.cmc=true	Angeben, ob das Warnungsdialogfeld mit der Meldung angezeigt werden soll, die darüber informiert, dass die aktuelle Sitzung in der CMS in Kürze abläuft.
pinger.showWarningDialog.bilaunchpad	pinger.showWarningDialog.bilaunchpad=true	Angeben, ob das Warnungsdialogfeld mit der Meldung angezeigt werden soll, die darüber informiert, dass die aktuelle Sitzung im BI-Launchpad in Kürze abläuft.
pinger.warningPeriod.pingIncrementsInSeconds	pinger.warningPeriod.pingIncrementsInSeconds=15	Angeben, wie häufig eine Webserveranforderung gesendet werden soll, während die Sitzungsablaufwarnmeldung angezeigt wird. Dies ist für die anwendungsübergreifende Synchronisierung des Warnungsdialogs wichtig.
pinger.warningPeriod.lengthInMinutes	pinger.warningPeriod.lengthInMinutes=5	Angeben, wann die Warnung vor dem Sitzungsablauf angezeigt werden soll.
logoff.on.websession.expiry	logoff.on.websession.expiry=true	Angeben, ob alle Anwendungssitzungen abgemeldet werden, wenn die Websitzung abläuft.
pinger.enabled	pinger.enabled=true	Aktivieren oder Deaktivieren des Warnmeldungsmechanismus für den Sitzungsablauf.
system.com.sap.bip.jcomanager.destinations.maxsize	system.com.sap.bip.jcomanager.destinations.maxsize=1000	Angeben der maximalen Anzahl zwischengespeicherter Java-Verbindungen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Einstellung	Standardwerte	Beschreibung
`httpproxy.username`	`httpproxy.username=myusername`	Angeben des Benutzernamens für die Anmeldung an dem HTTP-Proxyserver.
`httpproxy.password`	`httpproxy.password=mypassword`	Angeben des Kennworts für die Anmeldung an dem HTTP-Proxyserver.
`logon.embed.secret`	Keine	Ein gemeinsamer geheimer Schlüssel zwischen einem Portal, das BI-Plattform-Anwendungen und BI-Plattform-Server einbettet, mit dem festgestellt wird, ob BI-Plattform-Anwendungen sicher in andere Seiten eingebettet werden können.
`logon.embed.timeout`	`logon.embed.timeout=300`	Anzahl an Sekunden, nach denen BI-Plattform-Anwendungen wie das BI-Launchpad die Einbettung in ein Portal ablehnen. Stellen Sie sicher, dass die Systemuhren auf dem BI-Plattform-Webserver und den Portal-Serverrechnern innerhalb dieser Anzahl von Sekunden übereinstimmen.
`iview.autologoff`	`iview.autologoff=true`	Auf `true` festgelegt, um die sofortige automatische Abmeldung für SAP NetWeaver iViews zu aktivieren.
`pinger.showWarningDialog`	`pinger.showWarningDialog=true`	Gibt an, ob das Warnungsdialogfeld mit der Meldung angezeigt werden soll, die darüber informiert, dass die aktuelle Sitzung in Kürze abläuft. Gilt nicht für die CMC und das BI-Launchpad.
`ure.request.queue.timeout.seconds`	`ure.request.queue.timeout.seconds=20`	Anzahl von Sekunden, die eine Anforderung auf erwartete vorige Anforderungen wartet, bevor es zur Zeitüberschreitung kommt. Wenn Benutzer Navigations- oder Ordnererweiterungs-Aktionen im Baumstruktur-Steuerelement im BI-Launchpad durchführen, werden AJAX-Anforderungen für diese Aktionen in die Warteschlange aufgenommen. Die Benutzeroberfläche wartet, bis diese Anforderungen abgeschlossen sind, bevor der Benutzer die Kontrolle zurückerhält. Diese Einstellung legt die Anzahl der Sekunden fest, die die Benutzeroberfläche auf Anforderungen wartet, wenn in der Backend-Abfrage unerwartete Verzögerungen auftreten.

18.2.1.2 Eigenschaften von BI-Launchpad

Die folgende Tabelle enthält eine Aufstellung der Einstellungen aus der `bilaunchpad.properties`-Standarddatei für die BOE.war-Datei. Um Einstellungen zu überschreiben, erstellen Sie in `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` eine neue Datei.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Einstellung	Beschreibung
app.name	Angeben des Anzeigenamens der Anwendung. Der Name wird auf der Titelseite und dem Anmeldebildschirm der Webanwendung angezeigt. Standard: app.name=BI launch pad
app.name.short	Angeben des Anzeigenamens der Anwendung. Der Name wird auf der Titelseite und dem Anmeldebildschirm der Webanwendung angezeigt. Standard: app.name.short=BI launch pad
app.url.name	Angeben des URL-Namens der Anwendung mit vorangestelltem Zeichen "/"". Standard: app.url.name=/BI
authentication.default	Angeben der zur Authentifizierung von Benutzern in der Anwendung verwendeten Authentifizierungsmethode. Sie können Folgendes für diese Einstellung verwenden: **Authentifizierung** / **Werteinstellung** Enterprise: secEnterprise LDAP: secLDAP Windows AD: secWinAD SAP: secSAPR3 PeopleSoft: secpsenterprise JD Edwards: secPSE1 Siebel: secSiebel7 Oracle EBS: secOraApps Standard: authentication.default=secEnterprise
authentication.visible	Angeben, ob Benutzer, die sich bei BI-Launchpad anmelden, die Möglichkeit haben, die Authentifizierungsmethode anzuzeigen und zu ändern. Standard: authentication.visible=false
cms.default	Angeben des CMS-Standardnamens. Standard: cms.default=[Name des Hostrechners]
cms.visible	Angeben, ob bei BI-Launchpad angemeldete Benutzer die Möglichkeit haben, den CMS-Namen anzuzeigen und zu ändern. Standard: cms.visible=true
dialogue.prompt.enabled	Angeben, ob die Benutzer eine Eingabeaufforderung erhalten sollen, wenn Sie die Eingabeseite in einem Dialogfeld verlassen. Standard: dialogue.prompt.enabled=false
logontoken.enabled	Angeben, ob die Tokenerstellung nach der Anmeldung eines Benutzers bei BI-Launchpad für die Sitzung aktiviert werden soll. Das Token wird in einem Cookie gespeichert. Standard: logontoken.enabled=false

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Einstellung	Beschreibung
`SMTPFrom`	Aktivieren oder Deaktivieren des Felds *Von* bei der zeitgesteuerten Verarbeitung eines Objekts für ein Ziel. Standard: `SMTPFrom=true` Wenn Sie den Wert auf `false` einstellen, wird das Feld *Von* nicht angezeigt, und das System versucht, den E-Mail-Wert *Von* in der folgenden Reihenfolge abzurufen: 1. Erstens aus der Berichtsstandardeinstellung für ein Berichtsobjekt 2. Zweitens aus der E-Mail-Adresse im Benutzerprofil des angemeldeten Benutzers 3. Drittens aus der Job-Server-Standardeinstellung
`url.exit`	Angeben, zu welcher URL die Benutzer umgeleitet werden sollen, nachdem diese ihre BI-Launchpad-Sitzung beendet haben. Diese Einstellung gilt nur für die Benutzer, die sich über einen externen Prüfungsprozess bei der Anwendung angemeldet haben.
`disable.locale.preference`	Aktivieren oder Deaktivieren der Möglichkeit des Benutzers, die lokalen Einstellungen für BI-Launchpad anzuzeigen und zu ändern. Standard: `disable.locale.preference=false`
`extlogon.allow.logoff`	Aktivieren oder Deaktivieren der automatischen Abmeldung von Benutzersitzungen, nachdem diese ihre BI-Launchpad-Sitzung geschlossen haben. Auf "false" gesetzt, wenn die Benutzersitzungen bei der Abmeldung der Benutzer bei BI-Launchpad nicht automatisch beendet werden sollen. Standard: `extlogon.allow.logoff=true`
`logon.allowInsecureEmbedding`	Gibt an, ob andere Seiten ohne Übergabe eines gültigen Einbettungs-Tokens in diese Anwendung eingebettet werden können (als Frame). Standard: `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Gibt an, ob eine kommagetrennte Liste der SSO-Typen aktiviert wird sowie die Reihenfolge ihrer Ausführung. Eine leere Liste zeigt an, dass die bisherige Reihenfolge verwendet werden soll. Wenn die Liste angegeben wird, werden die bisherigen Optionen ignoriert. Gültige Optionen: `vintela`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `trustedX509`, `sapSSO` und `siteminder`. Falls keine erwünscht sind, geben Sie `none` an.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

18.2.1.3 OpenDocument-Eigenschaften

Die folgende Tabelle enthält eine Aufstellung der Einstellungen aus der `opendocument.properties`-Standarddatei für die BOE.war-Datei. Um Einstellungen zu überschreiben, erstellen Sie in `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` eine neue Datei.

Einstellung	Beschreibung
`app.name`	Angeben des Anzeigenamens der Anwendung. Der Name wird auf der Titelseite und dem Anmeldebildschirm der Webanwendung angezeigt. Standard:`app.name=SAP BusinessObjects OpenDocument`
`app.name.short`	Angeben des Anzeigenamens der Anwendung. Der Name wird auf der Titelseite und dem Anmeldebildschirm der Webanwendung angezeigt. Standard: `app.name.short=OpenDocument`
`authentication.default`	Angeben der zur Authentifizierung von Benutzern in der Anwendung verwendeten Authentifizierungsmethode. Sie können Folgendes für diese Einstellung verwenden: **Authentifizierung** / **Werteinstellung** Enterprise: `secEnterprise` LDAP: `secLDAP` Windows AD: `secWinAD` SAP: `secSAPR3` PeopleSoft: `secpsenterprise` JD Edwards: `secPSE1` Siebel: `secSiebel7` Oracle EBS: `secOraApps` Standard: `authentication.default=secEnterprise`
`authentication.visible`	Angeben, ob Benutzer, die sich bei OpenDocument anmelden, die Möglichkeit haben, die Authentifizierungsmethode anzuzeigen und zu ändern. Standard: `authentication.visible=false`
`cms.default`	Angeben des CMS-Standardnamens. Standard: `cms.default=[Name des Hostrechners]`
`cms.visible`	Angeben, ob Benutzer, die sich bei OpenDocument anmelden, die Möglichkeit haben, den CMS-Namen anzuzeigen und zu ändern. Standard: `cms.visible=true`
`logontoken.enabled`	Angeben, ob die Tokenerstellung nach der Anmeldung eines Benutzers bei OpenDocument für die Sitzung aktiviert werden soll. Das Token wird in einem Cookie gespeichert. Standard: `logontoken.enabled=false`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Einstellung	Beschreibung
`extlogon.allow.logoff`	Aktivieren oder Deaktivieren der automatischen Abmeldung von Benutzersitzungen, nachdem diese ihre OpenDocument-Sitzung geschlossen haben. Auf "false" gesetzt, wenn die Benutzersitzungen bei der Abmeldung der Benutzer bei OpenDocument nicht automatisch beendet werden sollen. Standard: `extlogon.allow.logoff=true`
`SAPLogonToken.enabled`	Gibt an, ob die Authentifizierung von SAP-Anmeldetoken des RESTful-Webdiensts an der BI-Plattform zulässig ist. Das SAP-Anmeldetoken wird durch den X-Wert des SAP-Anmeldetokens im Request-Header nach einer erfolgreichen Anmeldung mit der RESTful-Webdienst-URL angegeben. Standard: `SAPLogonToken.enabled=true`
`logon.allowInsecureEmbedding=false`	Gibt an, ob andere Seiten ohne Übergabe eines gültigen Einbettungs-Tokens in diese Anwendung eingebettet werden können (als Frame). Standard: `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Gibt an, ob eine kommagetrennte Liste der SSO-Typen aktiviert wird sowie die Reihenfolge ihrer Ausführung. Eine leere Liste zeigt an, dass die bisherige Reihenfolge verwendet werden soll. Wenn die Liste angegeben wird, werden die bisherigen Optionen ignoriert. Gültige Optionen: `serializedSession`, `sapLogonToken`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `vintela`, `infoview`, `trustedX509`, `sapSSO` und `siteminder`. Falls keine erwünscht sind, geben Sie `none` an.

18.2.1.4 CMC-Eigenschaften

In der folgenden Tabellen sind die Einstellungen aufgeführt, die in der standardmäßigen `cmc.properties`-Datei für BOE.war enthalten sind. Um Einstellungen zu überschreiben, erstellen Sie in `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` eine neue Datei.

Einstellung	Beschreibung
`app.url.name`	Gibt den URL-Namen der Anwendung mit einem vorangestellten Schrägstrich "/" an. Standardwert: `app.url.name=/CMC`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Einstellung	Beschreibung
`authentication.default`	Angeben der zur Authentifizierung von Benutzern in der Anwendung verwendeten Authentifizierungsmethode. Sie können Folgendes für diese Einstellung verwenden: **Authentifizierung** / **Werteinstellung** Enterprise: `secEnterprise` LDAP: `secLDAP` Windows AD: `secWinAD` SAP: `secSAPR3` PeopleSoft: `secpsenterprise` JD Edwards: `secPSE1` Siebel: `secSiebel7` Oracle EBS: `secOraApps` Standard: `authentication.default=secEnterprise`
`authentication.visible`	Gibt an, ob Benutzer, die sich bei der CMC anmelden, die Möglichkeit der Anzeige und Änderung der Authentifizierungsmethode haben. Standard: `authentication.visible=false`
`cms.default`	Angeben des CMS-Standardnamens. Standard: `cms.default=[Name des Hostrechners]`
`cms.visible`	Gibt an, ob Benutzer, die sich an der CMC anmelden, die Möglichkeit der Anzeige und Änderung des CMS-Namens haben. Standard: `cms.visible=true`
`dialogue.prompt.enabled`	Angeben, ob die Benutzer eine Eingabeaufforderung erhalten sollen, wenn Sie die Eingabeseite in einem Dialogfeld verlassen. Standard: `dialogue.prompt.enabled=false`
`logontoken.enabled`	Gibt an, ob die Tokenerstellung für die Sitzung aktiviert wird oder nicht, nachdem sich ein Benutzer bei der CMC angemeldet hat. Das Token wird in einem Cookie gespeichert. Standard: `logontoken.enabled=false`
`SMTPFrom`	Aktivieren oder Deaktivieren des Felds *Von* bei der zeitgesteuerten Verarbeitung eines Objekts für ein Ziel. Standard: `SMTPFrom=true` Wenn Sie den Wert auf `false` einstellen, wird das Feld *Von* nicht angezeigt, und das System versucht, den E-Mail-Wert *Von* in der folgenden Reihenfolge abzurufen: 1. Erstens aus der Berichtsstandardeinstellung für ein Berichtsobjekt

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Einstellung	Beschreibung
	2. Zweitens aus der E-Mail-Adresse im Benutzerprofil des angemeldeten Benutzers 3. Drittens aus der Job-Server-Standardeinstellung

18.3 Anpassen der Eingangspunkte für die BI-Launchpad- und die OpenDocument-Anmeldung

Sie können die Anmeldeseite für die BI-Launchpad- und OpenDocument-Webanwendungen anpassen. Sie können beispielsweise die Anmeldeseite mit einem Firmenlogo oder einer unternehmenseigenen Formatvorlage anpassen oder eine benutzerdefinierte Anmeldeseite erstellen, die die vertrauenswürdige Authentifizierung ermöglicht.

Um die Anmeldeseite anzupassen, ändern Sie die Datei `custom.jsp`, die in den BI-Launchpad- und OpenDocument-Anwendungsbereichen der `BOE.war`-Webanwendung gespeichert ist, und implementieren Sie die `BOE.war`-Webanwendung erneut in SAP BusinessObjects Business Intelligence. Die Benutzer greifen auf den benutzerdefinierten Anmeldeeinstiegspunkt zu, indem sie zu einer eindeutigen URL navigieren.

Um mit diesen Beispielen zu arbeiten, müssen Sie mit der Implementierung von BI-Plattform-Webanwendungen vertraut sein. Weitere Informationen finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.

18.3.1 Dateispeicherorte von BI-Launchpad und OpenDocument

Die Webanwendungen BI-Launchpad und OpenDocument sind Bestandteil der Webarchivdatei `BOE.war`. Der Speicherort des `BOE.war`-Archivs ist in der Datei `BOE.properties` definiert.

Auf Windows-Systemen lautet der Pfad zur Datei `BOE.properties` wie folgt:

- `<BOE_INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf\apps\BOE.properties`

Auf UNIX-Systemen lautet der Pfad zur Datei `BOE.properties` wie folgt:

- `<BOE_INSTALLVERZ>/sap_bobj/enterprise_xi40/wdeploy/conf/apps/BOE.properties`

In den folgenden Tabellen ist der Speicherort gemeinsamer Dateien innerhalb der Webarchivdatei `BOE.war` für die Anwendungen BI-Launchpad und OpenDocument aufgeführt.

Tabelle 20: Dateispeicherorte von BI-Launchpad

> **Hinweis**
>
> Die Webanwendung BI-Launchpad war früher unter dem Namen InfoView bekannt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Dateityp	Speicherort
Benutzerdefiniertes Anmeldeskript	`WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp`
Verzeichnis für zusätzliche Dateien	`WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources`
Benutzerdefinierte Anmelde-URL	`http://<Servername>:<Port>/BOE/BI/custom.jsp`

Tabelle 21: Dateispeicherorte von OpenDocument

Dateityp	Speicherort
Benutzerdefiniertes Anmeldeskript	`WEB-INF\eclipse\plugins\webpath.OpenDocument\web\opendoc\custom.jsp`
Verzeichnis für zusätzliche Dateien	`WEB-INF\eclipse\plugins\webpath.OpenDocument\web\noCacheCustomResources`
Benutzerdefinierte Anmelde-URL	`http://<Servername>:<Port>/BOE/OpenDocument/opendoc/custom.jsp`

18.3.2 Definieren einer benutzerdefinierten Anmeldeseite

Der Einsteigspunkt zur Anmeldeseite der BI-Plattform lässt sich anpassen. Sie können beispielsweise eine benutzerdefinierte Anmeldeseite erstellen, auf der ein Firmenlogo angezeigt und eine unternehmenseigene Formatvorlage verwendet werden.

Bearbeiten Sie die Datei `custom.jsp`, um die Anmeldeerfahrung der Benutzer anzupassen, und legen Sie unterstützende Dateien im Ordner `noCacheCustomResources` ab.

In diesem Beispiel wird die Erstellung einer benutzerdefinierten Anmeldeseite veranschaulicht, die den Benutzer zu der Standardanmeldeseite umleitet.

1. Erstellen Sie eine Datei, die Ihren benutzerdefinierten Anmeldecode enthält, und speichern Sie sie als `custom.js` im Ordner `noCacheCustomResources`.

   In diesem Beispiel wird eine Funktion definiert, die den Benutzer zu der Standardanmeldeseite, d.h. `logon.jsp` umleitet.

   ```
   function load() {window.location =  "logon.jsp";}
   ```

2. Bearbeiten Sie die Datei `custom.jsp`, um die Anmeldeseite anzupassen.

   Mithilfe dieses Beispiels werden eine Begrüßungsmeldung und ein Hyperlink angezeigt, der die `load`-Methode aufruft, die in der Datei `custom.js` gespeichert ist.

   ```
   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
    "http://www.w3.org/TR/html4/loose.dtd">

   <%@ page language=  "java" contentType=  "text/html;charset=utf-8"%>
   ```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
<html>
  <head> <title>Welcome</title>
  </head>
  <body>
    <script type=  "text/javascript" src=  "noCacheCustomResources/custom.js"></
script>
    <p>Welcome to ABC corporation.</p>
    <a href= "javascript:load()">Enter</a>
  </body>
</html>
```

3. Implementieren Sie die `BOE.war`-Webanwendung erneut, und starten Sie den Webserver neu.

18.3.3 Hinzufügen der vertrauenswürdigen Authentifizierung bei der Anmeldung

Legen Sie zur Aktivierung der vertrauenswürdigen Authentifizierung den vertrauenswürdigen Benutzer als Sitzungsattribut in der Datei `custom.jsp` fest, und ändern Sie die Authentifizierungseinstellungen in einer Kopie der Datei `global.properties`. Die Werte der benutzerdefinierten Kopie der Datei `global.properties` überschreiben die Standardwerte.

1. Bearbeiten Sie die Datei `custom.jsp` so, dass ein Sitzungsattribut zur Definition des vertrauenswürdigen Benutzers festgelegt wird.

   ```
   request.getSession().setAttribute("TrustedUserAttribute", "TrustedUser");
   ```

2. Erstellen Sie eine benutzerdefinierte Kopie der Datei `global.properties`, indem Sie `WEB-INF\config\default\global.properties` in `WEB-INF\config\custom\global.properties` kopieren.
3. Ändern Sie `WEB-INF\config\custom\global.properties` so, dass die Einzelanmeldung (SSO) aktiviert wird.

   ```
   sso.enabled=true
   ```

4. Ändern Sie `WEB-INF\config\custom\global.properties` so, dass die Parameter für die vertrauenswürdige Authentifizierung festgelegt werden, darunter die Sitzungsvariable des vertrauenswürdigen Benutzers und der gemeinsame geheime Schlüssel.

   Ersetzen Sie `"..."` durch den gemeinsamen geheimen Schlüssel für Ihr System.

   ```
   trusted.auth.user.param=TrustedUserAttribute
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.shared.secret="..."
   ```

   Weitere Informationen finden Sie im verwandten Thema zur Konfiguration der vertrauenswürdigen Authentifizierung für Webanwendungen.
5. Implementieren Sie die Webanwendung erneut, und führen Sie einen Neustart des Webservers durch.
6. Aktivieren Sie die vertrauenswürdige Authentifizierung in der CMC.

   Doppelklicken Sie auf der Registerkarte *Authentifizierung* auf **Enterprise**, und aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Authentifizierung ist aktiviert**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Aktivieren der vertrauenswürdigen Authentifizierung [Seite 227]
Konfigurieren der vertrauenswürdigen Authentifizierung für die Webanwendung [Seite 232]

18.4 Anpassen von Anwendungsbenutzeroberflächen

Bestimmte Anwendungsbenutzeroberflächen können über die CMC angepasst werden.

In der Central Management Console können Sie das Erscheinungsbild bestimmter Anwendungen anpassen. Sie können z. B. Benutzeroberflächenelemente umschalten.

18.4.1 Web Intelligence

18.4.1.1 Anpassen von Web-Intelligence-Oberflächenelementen

In der CMC können Sie die Anzeige von Web-Intelligence-Oberflächenelementen für Benutzergruppen anpassen, wie z.B. ganze Symbolleisten oder spezifische Objekte in der Symbolleiste, und den Zugriff auf spezifische Dokumentenmodi anpassen.

Standardmäßig werden alle Oberflächenelemente angezeigt. Wenn bestimmte Elemente nicht angezeigt werden sollen, deaktivieren Sie diese in der CMC: auf der Registerkarte **Benutzer und Gruppen**, wählen Sie einen Benutzer oder eine Gruppe aus, und klicken Sie anschließend auf **Aktionen** > **Anpassung**.

Der Bereich "Anpassung" enthält folgende Registerkarten:

- Benutzeroberflächenelemente

  Auf dieser Registerkarte wählen Sie einzelne auszublendende Oberflächenelemente, wie z.B. eine Symbolleiste oder eine Registerkarte oder deren Unterelemente, wie z.B. einen Schaltflächenbefehl, aus.
- Funktionen

  Auf dieser Registerkarte können Sie auswählen, dass zu einer Funktion gehörende Schaltflächen wie z.B. "Regenerieren" ausgeblendet werden.

> **Hinweis**
>
> Die Anpassung ist auf alle Web-Intelligence-Anwendungsclients anwendbar: Java Applet und Rich-Client.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Aktivieren von Erweiterungspunkten für die Web-Intelligence-Benutzeroberfläche für bestimmte Benutzergruppen [Seite 661]

18.4.1.1.1 Funktionen (Registerkarte)

Funktionselement	Beschreibung	Betrifft die folgenden Oberflächenelemente
Regenerieren	Die Benutzer können Dokumente regenerieren, um Daten von der Datenquelle zu aktualisieren.	Die Schaltfläche "Regenerieren in der Symbolleiste "Standardaktionsgruppe", die im Lese- und Entwurfsmodus verwendet wird.
Drill	Benutzer können Drill-Vorgänge für Daten in einem Dokument ausführen.	Die Schaltfläche "Drill" an folgenden Orten: • Symbolleiste "Analysegruppe" im Lesemodus. • Unterregisterkarte "Interagieren" unter der Registerkarte "Analyse" im Entwurfsmodus.
Lesemodus	Die Benutzer können ein Dokument im Lesemodus anzeigen.	Die Schaltfläche "Ansicht" an folgenden Orten: • Kontextmenü der Anwendung • Anwendungs-Steuerungssymbolleiste
Entwurfsmodus	Die Benutzer können ein Dokument im Entwurfsmodus anzeigen.	Die Schaltfläche "Entwurf" an folgenden Orten: • Kontextmenü der Anwendung • Anwendungs-Steuerungssymbolleiste
Datenmodus	Die Benutzer können ein Dokument im Datenmodus anzeigen.	Die Schaltfläche "Daten" an folgenden Stellen: • Kontextmenü der Anwendung • Anwendungs-Steuerungssymbolleiste

18.4.1.1.2 Benutzeroberflächenelemente (Registerkarte)

Einige der Oberflächenelemente, die Sie anpassen können, sind in den Diagrammen der nachfolgenden Unterabschnitte abgebildet. Verwenden Sie die folgende Tabelle, um die Elementeinträge in den Diagrammen zu identifizieren.

Benutzeroberflächenelement-Eintrag	Unterelement-Eintrag	Beschreibung	Nummer im Diagramm
Begrüßungsfenster		Dieses Bild wird beim Öffnen von Web Intelligence angezeigt.	

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Benutzeroberflächenelement-Eintrag	Unterelement-Eintrag	Beschreibung	Nummer im Diagramm
Kontextmenü der Anwendung		Dieses Menü wird bei Rechtsklick auf den Web Intelligence-Bildschirm angezeigt.	1
	Anwendungsmodus	Dies ist die Option zum Wechseln des Anwendungsmodus im Kontextmenü der Anwendung.	1a
	Filterleiste	Dies ist die Filterleistenoption im Kontextmenü der Anwendung.	1b
	Gliederung	Dies ist die Gliederungsoption im Kontextmenü der Anwendung.	1c
	Formelleiste	Dies ist die Formelleistenoption im Kontextmenü der Anwendung.	1d
	Seitenbereich	Dies ist die Seitenbereichsoption im Kontextmenü der Anwendung.	1e
	Berichtsregisterkarten	Dies ist die Berichtsregisterkartenoption im Kontextmenü der Anwendung.	1f
	Statusleiste	Dies ist die Statusleistenoption im Kontextmenü der Anwendung.	1g
Seitenbereich		Der Seitenbereich neben dem Berichtsbereich, in dem Zugriff auf verschiedene Informationsregisterkarten besteht.	2
	Dokumentübersicht	Registerkarte "Dokumentübersicht" im Seitenbereich.	2a
	Navigationsübersicht	Registerkarte "Navigationsübersicht" ("Berichtsstruktur" in der HTML-Schnittstelle) im Seitenbereich.	2b
	Eingabesteuerelemente	Registerkarte "Eingabesteuerelemente" im Seitenbereich.	2c
	Eingabe Benutzereingabeaufforderung	Registerkarte "Eingabe Benutzereingabeaufforderung" im Seitenbereich.	2d
	Verfügbare Objekte	Registerkarte "Verfügbare Objekte" im Seitenbereich.	2e
	Dokumentstruktur und Filter	Registerkarte "Dokumentstruktur und Filter" im Seitenbereich.	2f
	Webdienstveröffentlichung	Registerkarte "Webdienstveröffentlichung" im Seitenbereich.	2g
	Daten	Registerkarte "Daten" im Seitenbereich.	2h
Statusleiste		Die Statusleiste, in der Benutzer Informationen zum Status von Dokumentaktionen einsehen und Aufgaben wie Zoomen,	3

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Benutzeroberflächenelement-Eintrag	Unterelement-Eintrag	Beschreibung	Nummer im Diagramm
		Seitennavigation und Formelleistenaktivierung ausführen können.	
	Bericht-Dropdown-Liste	Die Dropdown-Liste "Bericht" in der Statusleiste.	3a
	Druckstatussymbol	Das Symbol "Druckstatus" in der Statusleiste.	3b
	Datenänderungen verfolgen	Der Nachverfolgungsstatus von Datenänderungen in der Statusleiste.	3c
	Seitennavigation	Die Seitennavigationsleiste in der Statusleiste.	3d
	Paginierungsmodus	Die Paginierungsmodusdrucktasten in der Statusleiste.	3e
	Zoomliste	Die Dropdown-Liste für die prozentuale Vergrößerung in der Statusleiste.	3f
	Zoomschieberegler	Die Zoomschiebereglerleiste in der Statusleiste.	3g
	Arbeitsbereichsstatus	Die Arbeitsbereichsstatusanzeige in der Statusleiste. **Hinweis** Die Arbeitsbereichsstatus-Anzeige ( ) wird zwischen dem Zoomschieberegler und dem letzten Aktualisierungsdatum angezeigt, wenn ein Problem im Arbeitsbereich angezeigt wird.	Wird nicht angezeigt
	Letztes Regenerierungsdatum	Das Datum der letzen Dokumentregenerierung in der Statusleiste.	3i
	Verbindungsstatus	Der Status des Web-Intelligence-Rich-Clients in der Statusleiste.	3j
Berichtszone		Die Berichtszone in Web Intelligence.	4
	Berichtsregisterkarten	Die Berichtsregisterkarten in der Berichtszone.	4a
	Bidirektionaler Bildlauf	Die Funktion für bidirektionalen Bildlauf in der unteren Ecke der Berichtszonenseite.	4b
	Formelleiste	Die Formelleiste im oberen Teil der Berichtszone.	4c
Lesemodus-Symbolleiste		Die im Lesemodus angezeigten Symbolleisten.	5
	Web-Intelligence-Dropdown-Liste	Die Dropdown-Liste Web Intelligence im Lesemodus.	5a

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Benutzeroberflächenelement-Eintrag	Unterelement-Eintrag	Beschreibung	Nummer im Diagramm
	Dateigruppe	Symbolleiste "Dateigruppe" im Lesemodus.	5b
	Standardaktionsgruppe	Symbolleiste "Standardaktionsgruppe" im Lesemodus.	5c
	Analysegruppe	Symbolleiste "Analysegruppe" im Lesemodus.	5d
Entwurfsmodus-Symbolleiste		Die Symbolleisten und Registerkarten, die im Entwurfsmodus angezeigt werden.	6
	Registerkarte "Datei"	Die Registerkarte "Datei" im Lesemodus.	6a
	Registerkarte "Eigenschaften"	Die Registerkarte "Eigenschaften" im Lesemodus.	6b
	Standardaktionsgruppe	Symbolleiste "Standardaktionsgruppe" im Lesemodus.	6c
	Registerkarte "Berichtselemente"	Die Registerkarte "Berichtselemente" im Lesemodus.	6d
	Registerkarte "Format"	Die Registerkarte "Format" im Lesemodus.	6e
	Registerkarte "Datenzugriff"	Die Registerkarte "Datenzugriff" im Lesemodus.	6f
	Registerkarte "Analyse"	Die Registerkarte "Analyse" im Lesemodus.	6g
	Registerkarte "Seite einrichten"	Die Registerkarte "Seite einrichten" im Lesemodus.	6h
Erste Symbolleiste		Die Symbolleisten, die beim ersten Öffnen von Web Intelligence angezeigt werden.	7
	Web-Intelligence-Dropdown-Liste	Die Dropdown-Liste Web Intelligence in der ersten Symbolleiste.	7a
	Dateigruppe	Symbolleiste "Dateigruppe" in der ersten Symbolleiste.	7b
Anwendungs-Steuerungssymbolleiste		Die Anwendungs-Steuerungssymbolleiste, die in der oberen Symbolleiste von Web Intelligence angezeigt wird.	8
	Anwendungsmodus-Schaltflächen	Die Anwendungsmodusdrucktasten (Lese-, Entwurf- und Datenmodus) in der oberen Symbolleiste von Web Intelligence.	8a
	Extras	Das Symbol "Extras" in der oberen Symbolleiste von Web Intelligence.	8b

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Benutzero-berflächenele-ment-Eintrag	Unterelement-Eintrag	Beschreibung	Nummer im Diagramm
	Hilfe	Das Symbol "Hilfe" in der oberen Symbolleiste von Web Intel-ligence.	8c
	Schließen	Das Symbol "Schließen" in der oberen Symbolleiste von Web Intelligence.	8d
Tastenkombi-nationen		Tastenkombinationen, z. B. *STRGN* oder *STRGS*.	Wird nicht angezeigt

Begrüßungsbildschirm

In der Anpassung von Benutzern und Gruppen der CMC können Sie festlegen, dass der angezeigte Web-IntelligenceBegrüßungsbildschirm ausgeblendet wird. Die folgende Abbildung zeigt den Begrüßungsbildschirm, der beim Öffnen von Web Intelligence standardmäßig eingeblendet wird.

Abbildung 13: Begrüßungsbildschirm (englisches Beispiel)

Kontextmenü der Anwendung

Die folgenden Diagramme zeigen die Elemente, die im Kontextmenü (rechte Maustaste) ausgeblendet werden können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

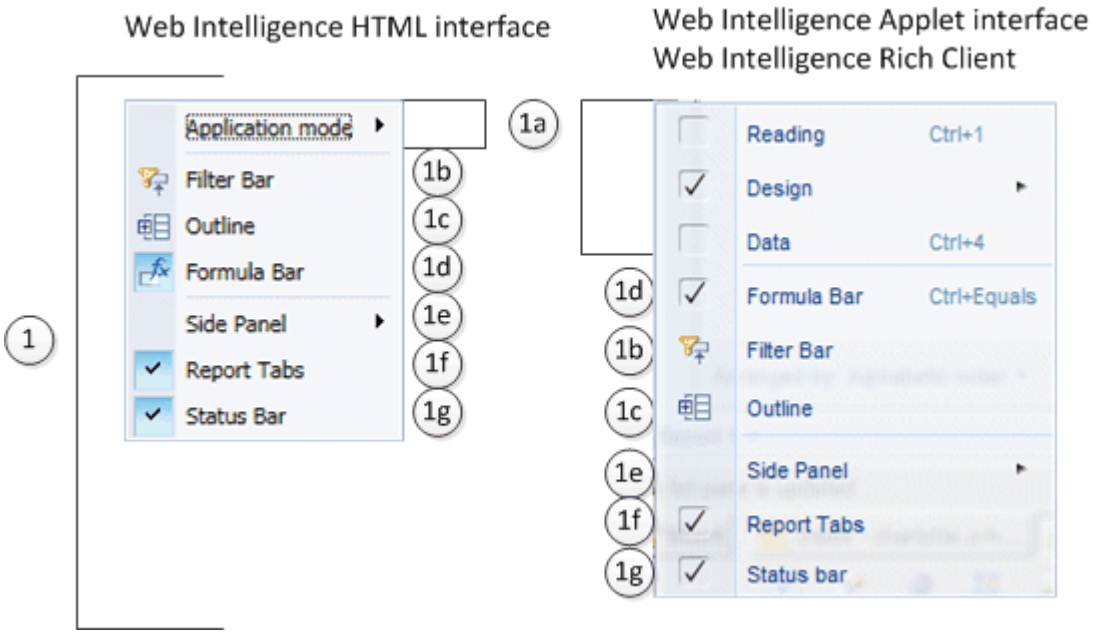


Abbildung 14: Kontextmenü der Anwendung (englisches Beispiel)

Erste Symbolleiste

Die folgenden Diagramme zeigen die Elemente, die in den Symbolleisten ausgeblendet werden können, die in Web Intelligence angezeigt werden, wenn kein Dokument geöffnet ist.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

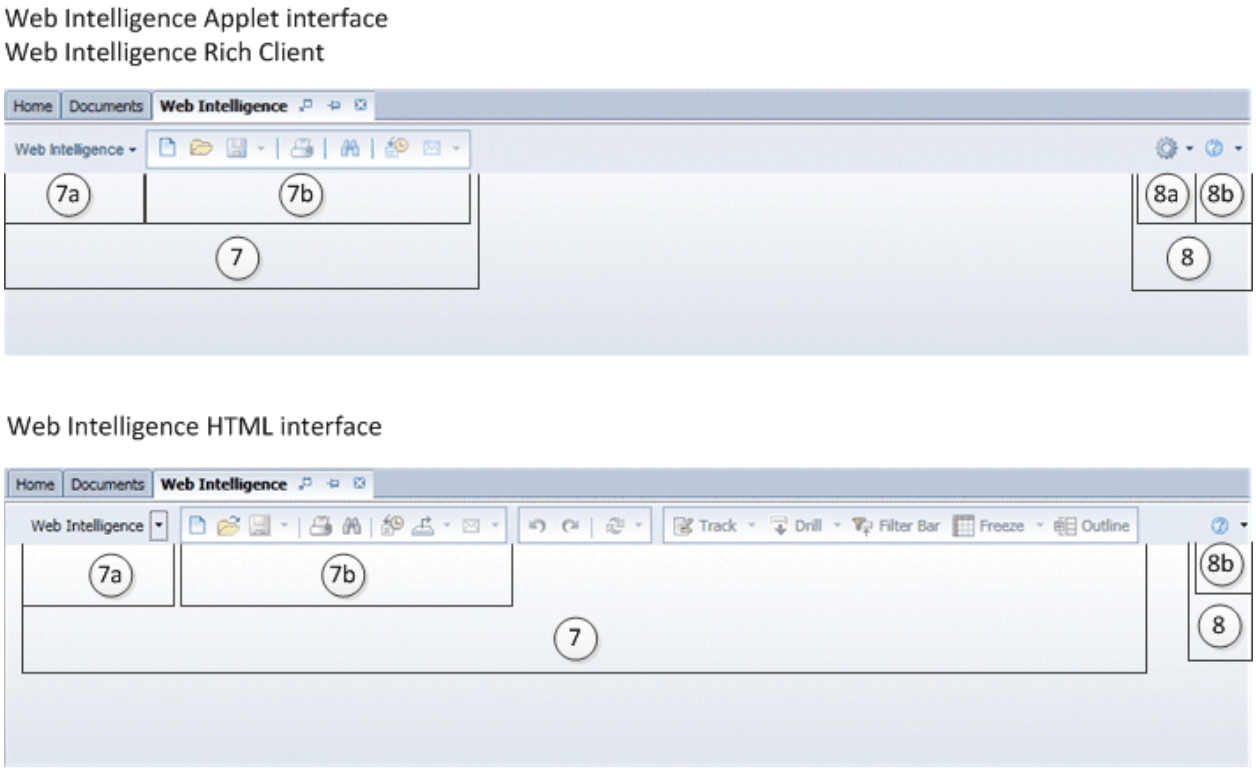


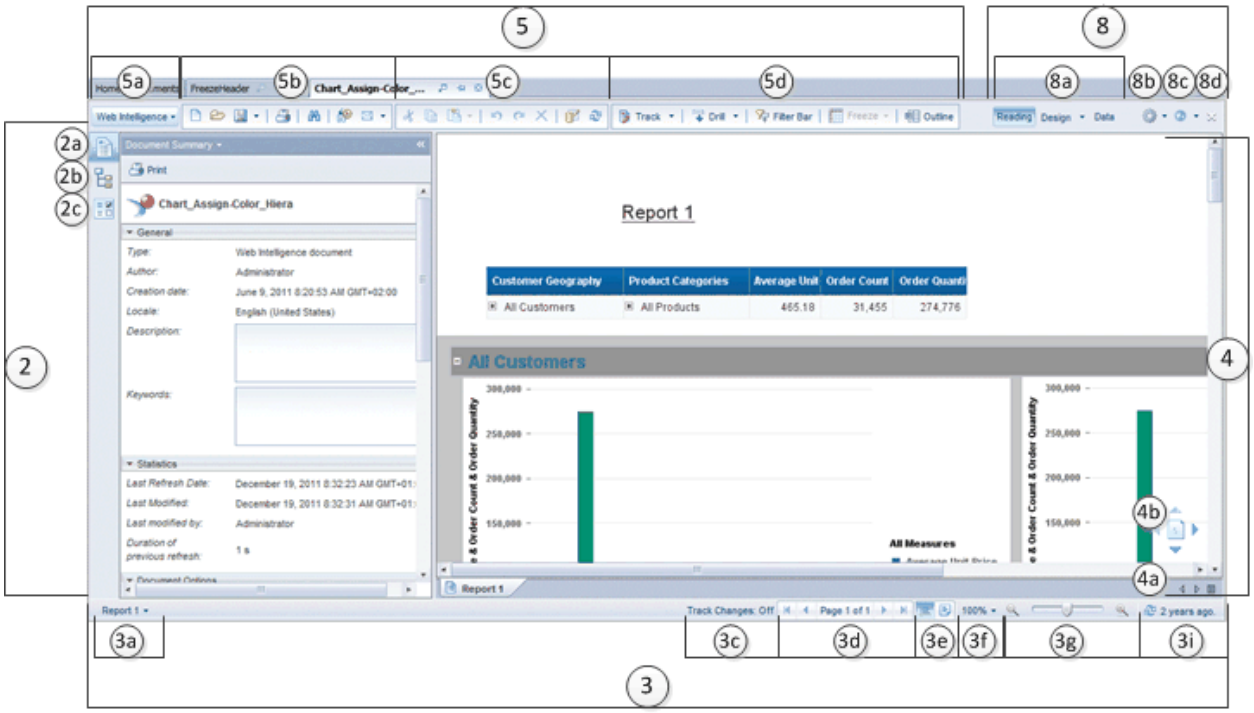
Abbildung 15: Erste Symbolleiste (englisches Beispiel)

Lesemodus

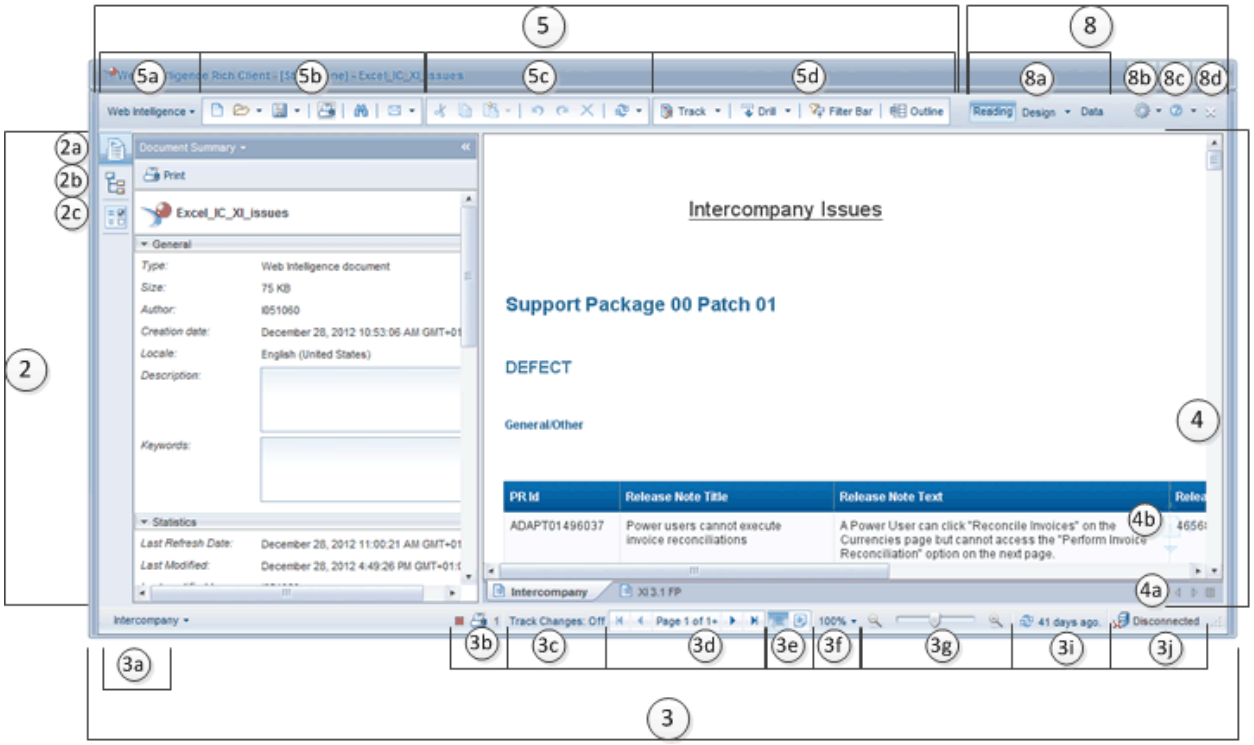
Die folgenden Diagramme zeigen die Elemente, die im Lesemodus von Web Intelligence ausgeblendet werden können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Web Intelligence Applet interface



Web Intelligence Rich Client



© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

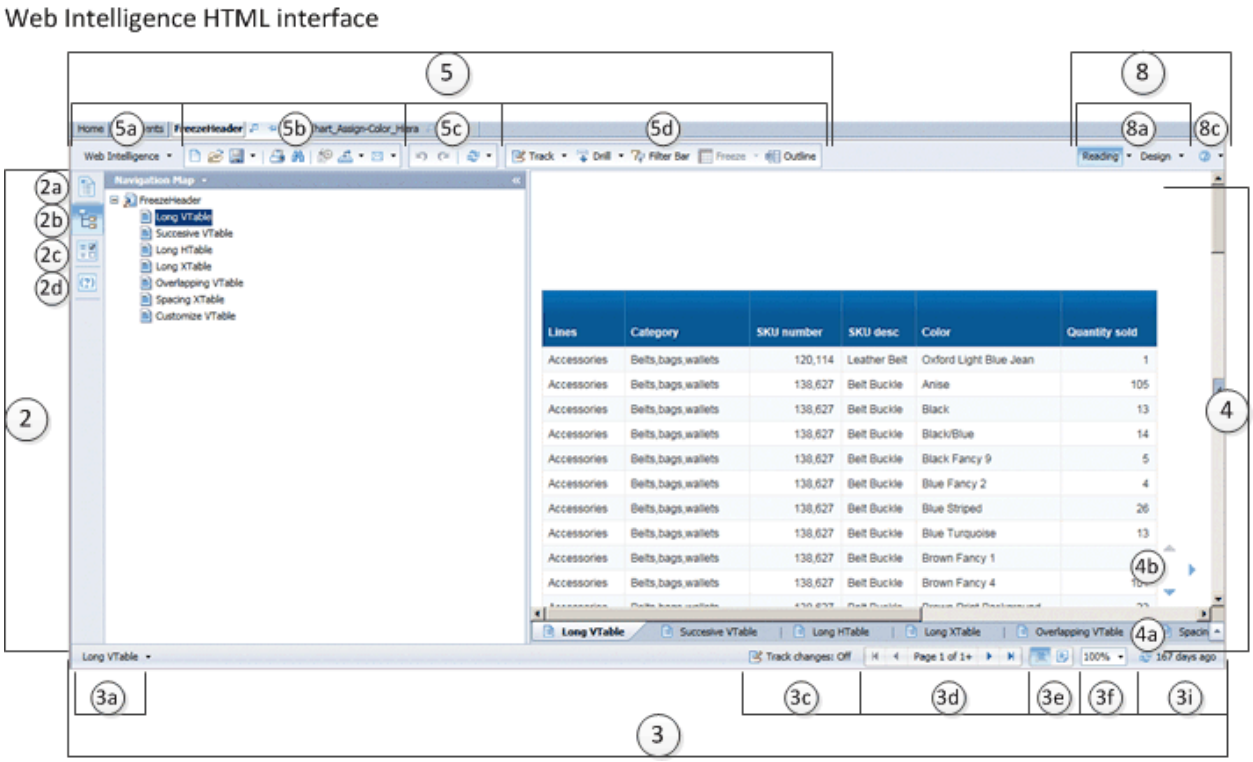


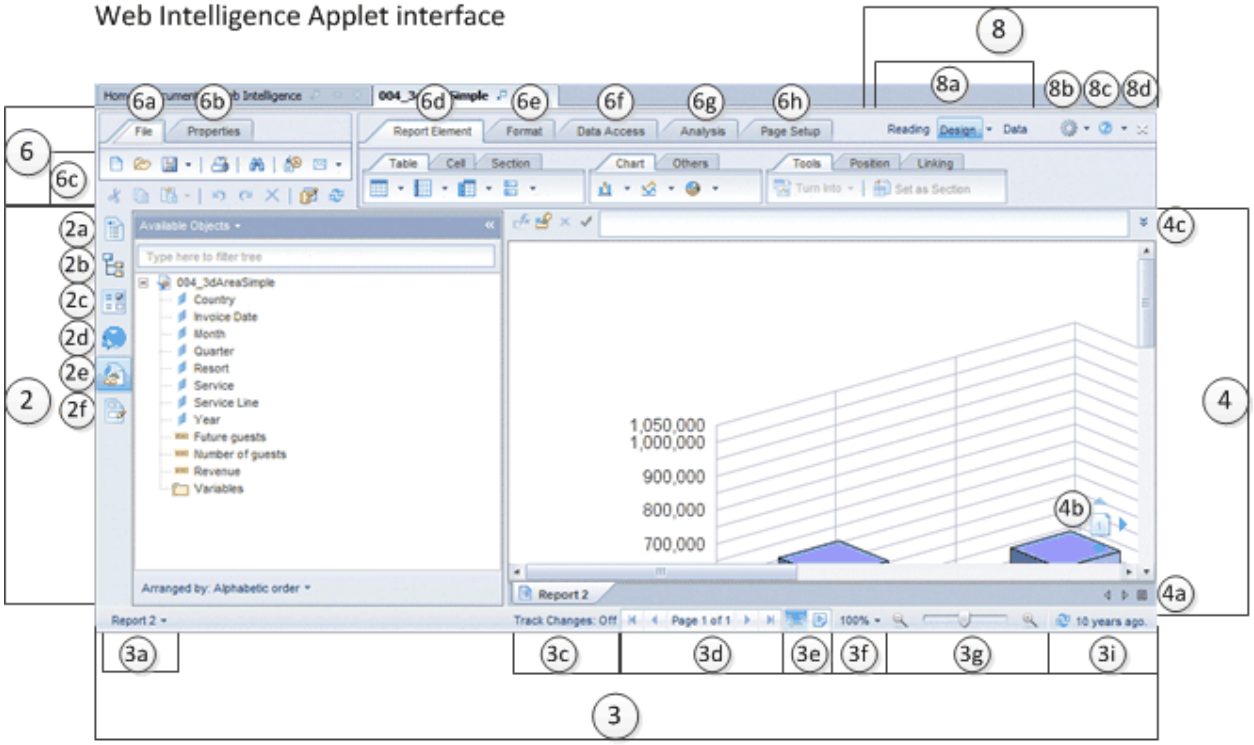
Abbildung 16: Lesemodus (englisches Beispiel)

Entwurfsmodus

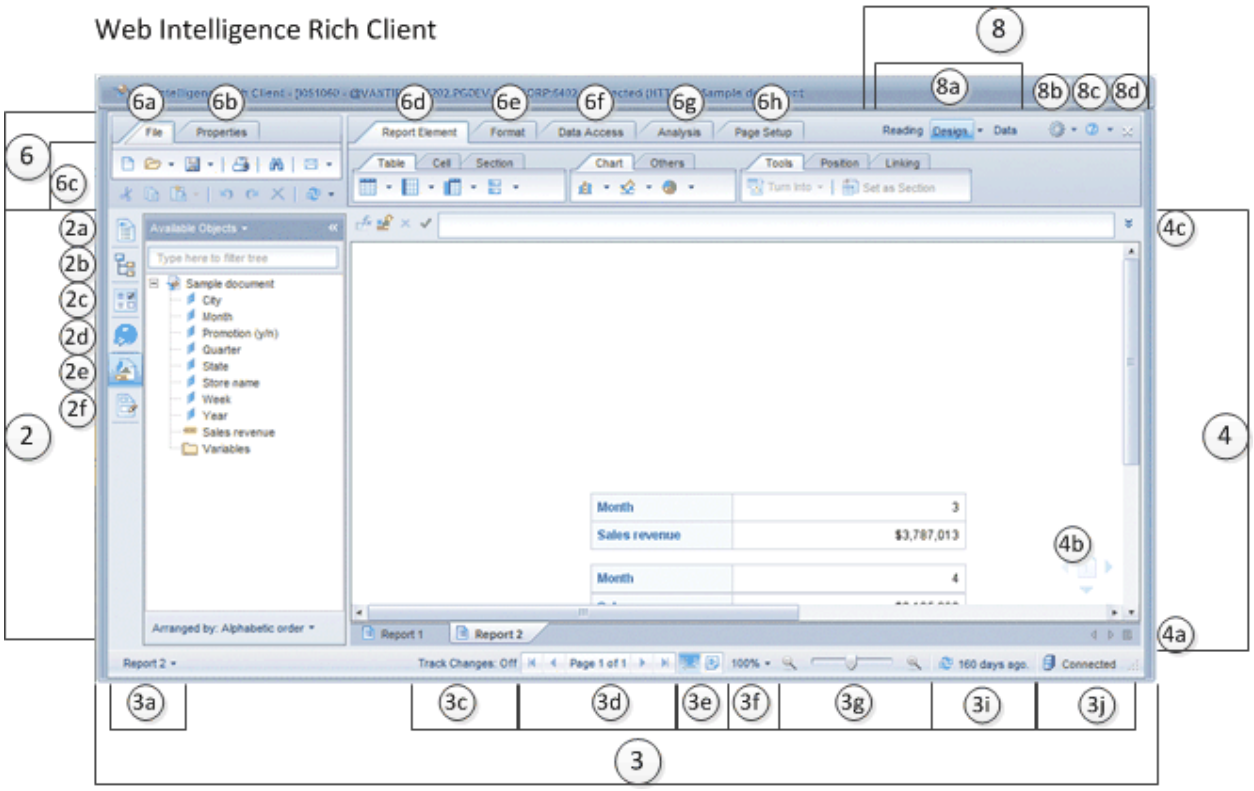
Die folgenden Diagramme zeigen die Elemente, die im Êntwurfsmodus von Web Intelligence ausgeblendet werden können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Web Intelligence Applet interface



Web Intelligence Rich Client



© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

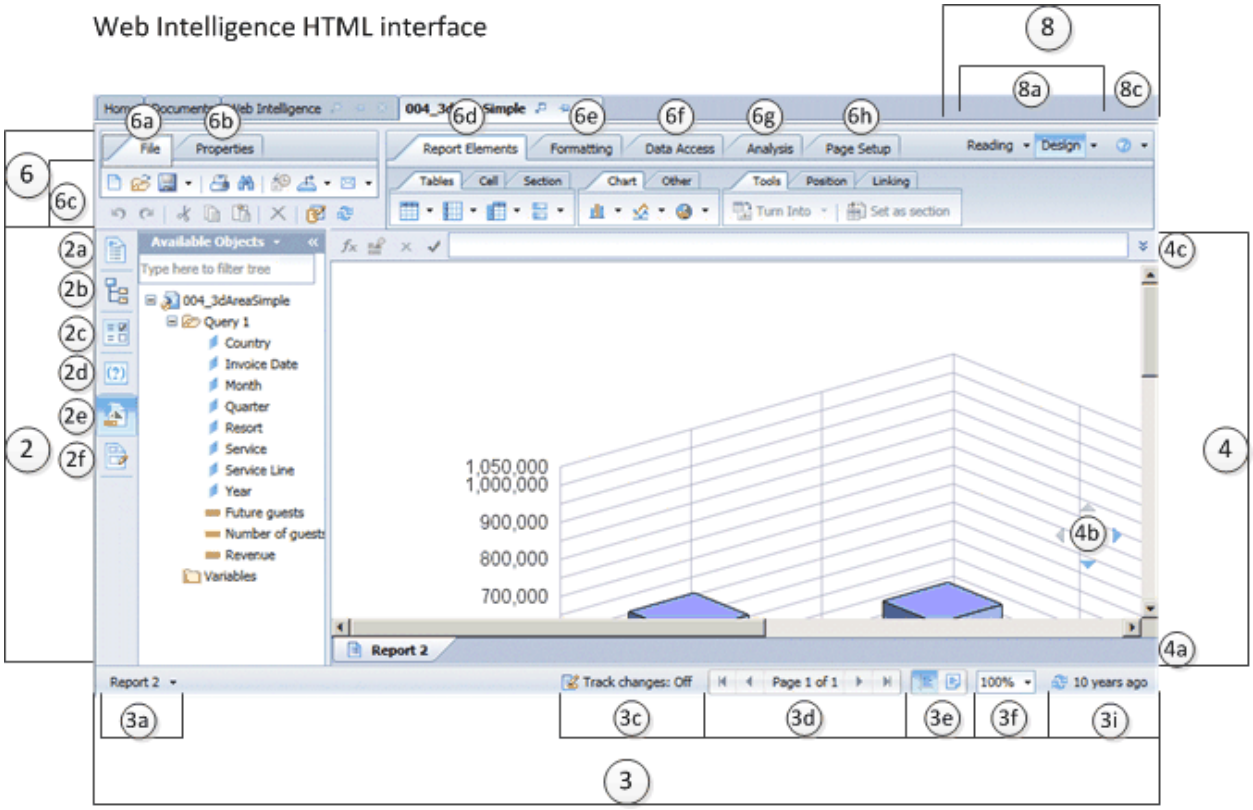


Abbildung 17: Entwurfsmodus (englisches Beispiel)

Datenmodus

Die folgenden Diagramme zeigen die Elemente, die im Datenmodus von Web Intelligence ausgeblendet werden können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

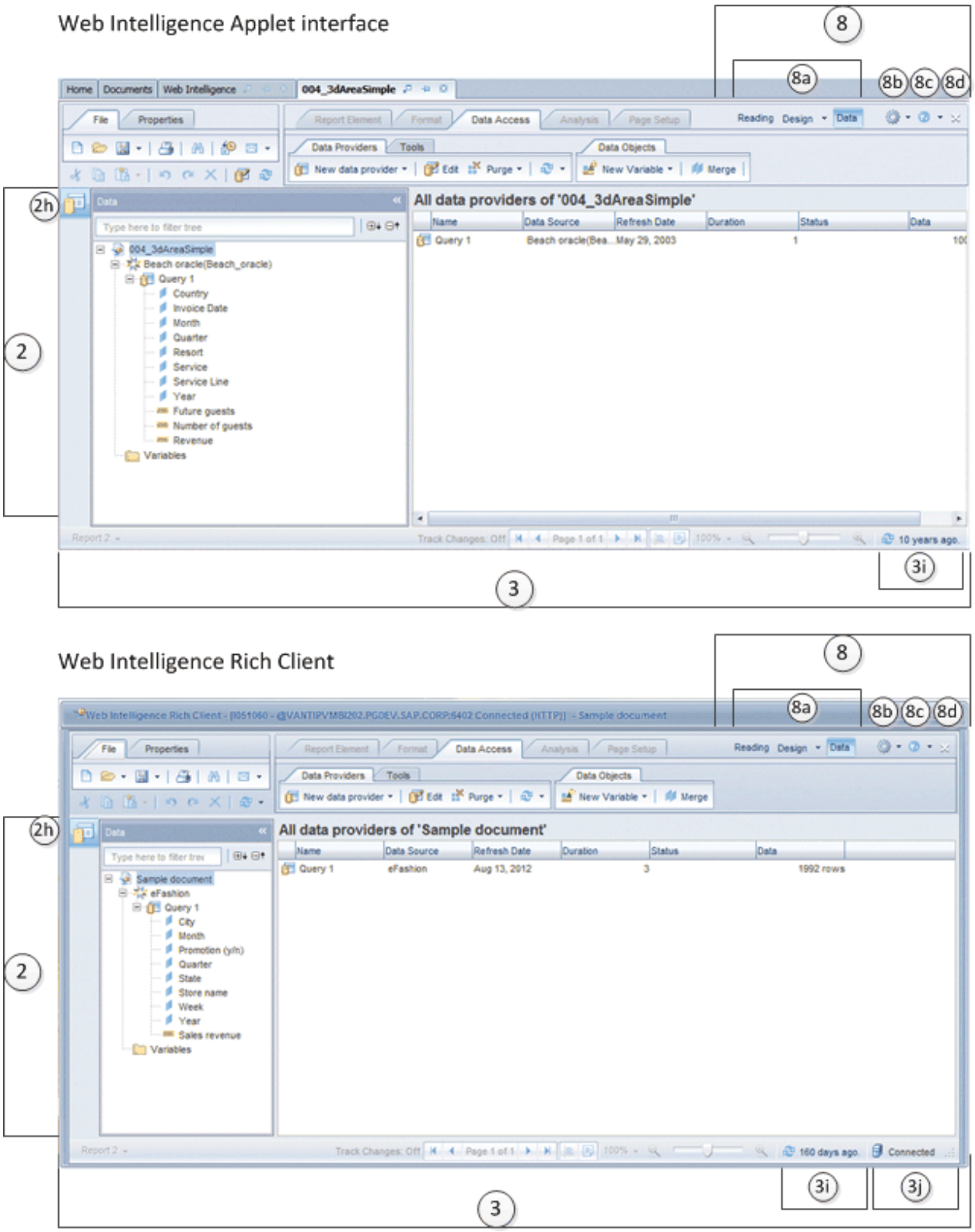


Abbildung 18: Datenmodus (englisches Beispiel)

18.4.1.1.3 Anpassen des Aussehens der Web-Intelligence-Oberfläche

Sie können das Aussehen der Web-Intelligence-Benutzeroberfläche anpassen, indem Sie Menüelemente,

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Unterelemente und Funktionen für alle Mitglieder einer ausgewählten Benutzergruppe ausblenden.

1. Melden Sie sich bei der CMC als Administrator an.
2. Wählen Sie in der Liste *Organisieren* die Option **Benutzer und Gruppen** aus.
3. Wählen Sie in der Liste *Gruppenhierarchie* eine Benutzergruppe aus.
4. Wählen Sie in der Liste *Verwalten* die Option **Eigenschaften**.
5. Wählen Sie im Seitenbereich **Anpassung**.
6. Führen Sie eine der folgenden Aktionen aus:
   - Um Elemente in Web Intelligence auszublenden, deaktivieren Sie die Elemente auf der Registerkarte "Benutzeroberflächenelemente" oder auf der Registerkarte "Funktionen".
   - Um ausgeblendete Elemente in Web Intelligence anzuzeigen, wählen Sie die Elemente auf der Registerkarte "Benutzeroberflächenelemente" oder auf der Registerkarte "Funktionen" aus.
7. Klicken Sie auf **Speichern und schließen**.

Wenn Sie die Anpassung speichern, werden diese Änderungen allen Benutzern der ausgewählten Gruppe angezeigt, wenn diese sich das nächste Mal beim BI-Launchpad anmelden und Web Intelligence öffnen.

> **Hinweis**
>
> Es wird empfohlen, sich beim BI-Launchpad als Benutzer aus der Gruppe anzumelden, die soeben angepasst wurde, Web Intelligence zu starten und zu überprüfen, ob die Oberfläche mit Ihren Anpassungseinstellungen übereinstimmt.

18.4.1.2 Aktivieren von Erweiterungspunkten für die Web-Intelligence-Benutzeroberfläche für bestimmte Benutzergruppen

Sie können Web Intelligence-Rechte konfigurieren, um ausgewählten Benutzergruppen Zugriff auf benutzerdefinierte Schnittstellenerweiterungen zu gewähren. Weitere Informationen zu Erweiterungsbündeln und API-Aufrufen des RESTful-Webdienstes finden Sie im *Benutzerhandbuch zu Erweiterungspunkten für die SAP-BusinessObjects-Web-Intelligence-Benutzeroberfläche*.

18.4.1.2.1 Aktivieren von Erweiterungspunkten für die Web-Intelligence-Benutzeroberfläche

Um die Erweiterungsfunktion verwenden zu können, müssen Sie in Ihrer Installation die entsprechenden Erweiterungsbündel erstellt und implementiert haben. Für jede Erweiterungsfunktion (z. B. "Benutzerdefinierte Schaltfläche" oder "Im HTML-Format speichern") implementieren Sie ein Erweiterungsbündel.

1. Melden Sie sich bei der CMC als Administrator an.
2. Wählen Sie in der Liste *Organisieren* die Option **Benutzer und Gruppen** aus.
3. Klicken Sie in der Liste *Gruppenhierarchie* mit der rechten Maustaste auf eine Benutzergruppe, und wählen Sie **Anpassung** aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Klicken Sie auf die Registerkarte **Erweiterungen**, und wählen Sie die benutzerdefinierten Erweiterungen aus, die die Benutzer verwenden sollen.

Die Erweiterungen sind standardmäßig nicht ausgewählt (nicht verfügbar). Sie müssen die Erweiterungen auswählen, die Sie für die ausgewählte Benutzergruppe verfügbar machen möchten.

18.4.1.3 Ausrichten von Web-Intelligence-Inhalten

Wählen Sie die Richtung für die Ausrichtung der Dokumentinhalte (von Links-nach-rechts oder von Rechts-nach-links) beim Erstellen von Web-Intelligence-Dokumenten durch Benutzer aus.

Für die Web-Intelligence-Applet-Schnittstelle können Sie die die Ausrichtung von Inhalten in der CMC festlegen. Treffen Sie eine Auswahl aus folgenden Optionen:

- **Von Rechts-nach-links, wenn sowohl das bevorzugte Anzeigegebietsschema als auch das Produktgebietsschema auf eine linksläufige Sprache** (Standardoption) festgelegt ist
- **Von Rechts-nach-links oder von Links-nach-rechts je nach dem bevorzugten Anzeigegebietsschema des Benutzers**
- **Immer von Rechts-nach-links**
- **Immer von Links-nach-rechts**

> **Hinweis**
>
> Die Einstellung für die Ausrichtung von Inhalten gilt für alle Benutzer.

Für die Web-Intelligence-Rich-Client-Schnittstelle wird die Ausrichtung von Inhalten anhand der Gebietsschemas ermittelt, die in den BI-Launchpad-Einstellungen festgelegt sind:

- Das System verwendet die Rechts-nach-links-Ausrichtung nur, wenn sowohl das bevorzugte Anzeigegebietsschema als auch das Produktgebietsschema auf eine linksläufige Sprache festgelegt ist.
- In allen anderen Fällen erfolgt eine Ausrichtung der Inhalte von Links-nach-rechts.

> **Hinweis**
>
> Informationen zum Festlegen von Gebietsschemas finden Sie im *Benutzerhandbuch für Business-Intelligence-Launchpad*.

> **Hinweis**
>
> Die Ausrichtung von Inhalten wird nur zum Zeitpunkt der Dokumenterstellung angewendet und wirkt sich nicht auf vorhandene Dokumente aus.

18.4.1.3.1 Einrichten der Inhaltsanpassung für die Web-Intelligence-Applet-Oberfläche

Einrichten der Inhaltsanpassung für die Web-Intelligence-Applet-Oberfläche.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Melden Sie sich bei der CMC als Administrator an.
2. Wählen Sie in der Liste *Verwalten* die Option **Anwendungen**.
3. Wählen Sie *Web Intelligence*.
4. Klicken Sie auf **Verwalten** > **Eigenschaften**.
5. Blättern Sie nach unten zum Bereich **Inhaltsanpassung für neue Dokumente**, und wählen Sie die gewünschte Option aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

19 Verwalten von Verbindungen und Universen

19.1 Verwalten von Verbindungen

Eine Verbindung ist eine benannte Gruppe von Parametern, durch die definiert wird, wie eine oder mehrere SAP BusinessObjects-Anwendungen auf relationale oder OLAP-Datenbanken zugreifen können. Verbindungsdetails wie Servername, Datenbank, Benutzername und Kennwort können sicher im BI-Plattform-Repository im Ordner "Verbindungen" gespeichert werden.

Designer definieren Universen auf der Grundlage von Verbindungen. Benutzer von Abfrage-, Analyse- und Reportinganwendungen greifen über das Universum auf die Datenbank zu, ohne dass sie die zugrunde liegenden Datenstrukturen in der Datenbank kennen müssen.

Sie können mit den folgenden Anwendungen Verbindungen erstellen:

- Universe-Design-Tool. Verbindungen werden im Repository gespeichert.
- Information-Design-Tool. Verbindungen können lokal erstellt und dann im Repository veröffentlicht oder direkt im Repository erstellt und bearbeitet werden.

> **Hinweis**
>
> Weitere Informationen zur Verwaltung von OLAP-Datenquellenverbindungen finden Sie im *Administratorhandbuch für SAP BusinessObjects Analysis, Edition für OLAP*.

Sie erteilen Rechte, damit Benutzer Verbindungen erstellen, bearbeiten und löschen können.

Sie erteilen Benutzern Zugriff auf Universumsverbindungen und ermöglichen ihnen das Erstellen und Anzeigen von Dokumenten, die Universen und Verbindungen verwenden.

Weitere Informationen

Verwalten von Sicherheitseinstellungen für Objekte in der CMC [Seite 133]
Verbindungsrechte [Seite 933]

19.1.1 So löschen Sie eine Universumsverbindung

> **Tipp**
>
> Außerdem können im Universe-Design-Tool und im Information-Design-Tool Verbindungen gelöscht werden.

1. Wählen Sie im Bereich *Verbindungen* eine Universumsverbindung aus der Liste aus.
2. Klicken Sie auf **Verwalten** > **Löschen**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

19.2 Verwalten von Universen

Ein Universum ist eine strukturierte Sammlung von Metadatenobjekten, mit denen Geschäftsbenutzer Unternehmensdaten in einer nichttechnischen Sprache analysieren und als Berichte aufbereiten können. Zu diesen Objekten zählen Dimensionen, Kennzahlen, Hierarchien, Attribute, vordefinierte Berechnungen, Funktionen und Abfragen. Die Metadatenobjektschicht ist auf einem relationalen Datenbankschema oder einem OLAP-Cube aufgebaut, so dass die Objekte direkt den Datenbankstrukturen zugeordnet sind. Da ein Universum Verbindungen zu den Datenquellen beinhaltet, können die Benutzer von Abfrage- und Analysetools eine Verbindung zu einem Universum herstellen und mit den Objekten in einem Universum Abfragen ausführen und Berichte erstellen, ohne dass sie die zugrunde liegenden Datenstrukturen der Datenbank kennen müssen.

Mit den folgenden Tools können Sie Universen erstellen:

- Universe-Design-Tool. Mit diesem Tool erstellte Universen sind an der Erweiterung .unv zu erkennen und werden .unv-Universen genannt. .unv-Universen werden auf einer geschützten Verbindung definiert und im Order "Universes" des Repositorys gespeichert.
- Information-Design-Tool. Mit diesem Tool erstellte Universen basieren auf der neuen semantischen Ebene. Sie unterscheiden sich durch die Erweiterung .unx und werden daher .unx-Universen genannt. .unx-Universen werden lokal erstellt und im Ordner "Universes" des Repositorys veröffentlicht. Designer können mithilfe des Sicherheitseditors des Information-Design-Tools Sicherheit auf Objektebene definieren.

Sie erteilen Benutzern Anwendungs- und Universumsrechte, damit sie Universen erstellen, bearbeiten und löschen und Sicherheit auf Universen entwerfen können.

Sie erteilen Benutzer Universumsrechte, damit sie Dokumente erstellen und anzeigen können, die Universen nutzen.

Weitere Informationen

Verwalten von Sicherheitseinstellungen für Objekte in der CMC [Seite 133]
Universe-Design-Tool-Rechte [Seite 942]
Universumsrechte (.unv) [Seite 929]
Information-Design-Tool-Rechte [Seite 943]
Universumsrechte (.unx) [Seite 931]

19.2.1 So löschen Sie Universen

➔ Tipp

Außerdem können im Information-Design-Tool Universen gelöscht werden.

1. Wählen Sie im Bereich *Universen* der CMC ein Universum aus der Liste aus.
2. Klicken Sie auf **Verwalten** > **Löschen**.
3. Wenn Sie zum Bestätigen aufgefordert werden, klicken Sie auf **OK**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

20 Überwachung

20.1 Informationen zur Überwachung

Das Überwachungstool ermöglicht die Ermittlung der Laufzeit- und Verlaufsmetriken der BI-Plattform-Server für die Berichterstellung und Benachrichtigung. Mithilfe des Überwachungstools können Systemadministratoren ermitteln, ob eine Anwendung ordnungsgemäß funktioniert und ob die Antwortzeiten den Erwartungen entsprechen. Durch die Bereitstellung wichtiger Geschäftsmetriken liefert das Überwachungstool bessere Einblicke in die BI-Plattform.

Die Überwachung ermöglicht Ihnen die Ausführung dieser Aufgaben:

- Überprüfung der Leistung jedes einzelnen Servers: Dies ist mithilfe von Kontrollmodulen möglich, die den Status jedes einzelnen Servers in Form von Ampeln anzeigen. Der Systemadministrator kann Schwellenwerte für diese Kontrollmodule festlegen und Warnmeldungen erhalten, wenn diese Schwellenwerte überschritten werden. So kann im Falle eines drohenden Fehlers oder Ausfalls proaktiv gehandelt werden.
- Anzeigen wichtiger System-Schlüsselleistungsindikatoren (Key Performance Indicators, KPIs): Auf diese Weise wird die Überwachung von Aktivitäten und Ressourcen unterstützt. Diese KPIs werden auf der Dashboard-Seite des Überwachungstools angezeigt.
- Anzeigen der gesamten BI-Plattform-Implementierung basierend auf Servergruppen, Dienstkategorien und Enterprise-Knoten im grafischen und im tabellarischen Format.
- Anzeigen kürzlicher Fehler auf dem Dashboard-Bildschirm.
- Überprüfung der Systemverfügbarkeit und Antwortzeit: Diagnosen simulieren Workflows, um zu prüfen, ob die Server und Dienste in der BI-Plattform-Implementierung erwartungsgemäß funktionieren. Durch die Analyse der Roundtrip-Zeit dieser Diagnosen in regelmäßigen Abständen kann der Systemadministrator das Systemauslastungsmuster einschätzen.
- Analyse von Spitzenauslastung und Spitzenzeitraum für den CMS: So kann der Systemadministrator bestimmen, ob weitere Lizenzen oder Systemressourcen erforderlich sind.
- Integration in andere Unternehmensanwendungen: Das Überwachungstool der BI-Plattform kann in anderen Unternehmensanwendungen wie SAP Solution Manager und IBM Tivoli Monitoring integriert werden.

Weitere Informationen zur Verwendung des Überwachungstools, einschließlich Diagnosen und Kontrollmodule, finden Sie in der *Onlinehilfe für die CMC von SAP BusinessObjects Business Intelligence*.

Weitere Informationen

Info zu Servermetriken (Anhang) [Seite 989]

20.2 Monitoring-Begriffe

Die folgende Liste enthält Begriffe in Zusammenhang mit dem Überwachungstool:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Trend

Aufzeichnen oder Anzeigen von Verlaufsdaten zur Ermittlung von Trends.

Dashboard

Die Seite "Dashboard" stellt eine zentralisierte Ansicht für den Systemadministrator zur Überwachung der Leistung aller Server bereit. Sie stellt Echtzeitinformationen über die System-KPIs, aktuelle Warnmeldungen und Kontrollmodule und die entsprechenden, auf den Kontrollmodulstatus basierenden Diagramme zur Verfügung.

Kontrollmodul

Kontrollmodule stellen den Echtzeit-Status sowie Verlaufstrends von Servern und Workflows innerhalb der BI-Plattform bereit. Benutzer können Schwellenwerte und Warnmeldungen mit Kontrollmodulen verknüpfen. Mithilfe von Daten aus Diagnosen, Servern, SAPOSCOL oder abgeleiteten Metriken können Sie ein Kontrollmodul erstellen.

Abgeleitete Metrik

Abgeleitete Metriken sind Metriken, die Sie erstellen, indem Sie zwei oder mehr vorhandene Metriken in einer mathematischen Gleichung kombinieren. Sie können eine Metrik basierend auf den Anforderungen des Benutzers erstellen und anschließend ein Kontrollmodul anhand dieser Metrik erstellen.

Topologische Metrik

Topologische Metriken stellen Ihnen den Nettostatus für alle Dienstkategorien in der BI-Plattform bereit. Der Crystal-Reports-Dienst beispielsweise stellt den kombinierten Status von allen mit Crystal-Reports-Servern in Verbindung stehenden Kontrollmodulen bereit.

Status

Die Statuswerte sind:

- "0" – "Die Metrik hat einen ungültigen Status"
- "1" – "Der Status der Metrik verschlechtert sich, Sofortmaßnahmen sind erfoderlich"
- "2" – "Die Metrik hat einen gültigen Status"

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

KPI

KPIs (Key Performance Indicators) sind Standardmetriken in der BI-Plattform. Sie bieten Informationen zu Zeitplänen und Anmeldesitzungen. Zum Beispiel deutet eine hohe Anzahl von **laufenden Aufträgen** auf eine gute Leistung der Server hin. Dagegen lässt eine hohe Anzahl von **ausstehenden Aufträgen** auf eine schlechte Leistung und hohe Systemlast schließen.

Diagnose

Diagnosen überwachen verschiedene Dienste und simulieren die verschiedenen Funktionalitäten der BI-Plattform-Komponenten. Durch die zeitgesteuerte Verarbeitung von Diagnosen zu vorgegebenen Intervallen kann der Systemadministrator die Verfügbarkeit und Leistung von durch die BI-Plattform bereitgestellten Schlüsseldiensten nachverfolgen. Diese Daten können auch zur Kapazitätsplanung verwendet werden.

Ampel

Bei einer Ampel handelt es sich um ein Symbol, das die Farben Grün, Gelb oder Rot anzeigt, um den Status eines Kontrollmoduls zu einem bestimmten Zeitpunkt anzugeben. Benutzer können zwei oder drei Statuswerte für ein Kontrollmodul festlegen.

Trenddiagramm

Ein Trenddiagramm ist eine grafische Darstellung metrischer Verlaufsdaten, die von Diagnosen und Servern generiert wurden. Es unterstützt den Systemadministrator bei der Überwachung des Systems in verschiedenen Zeitintervallen und bei der Einschätzung des Systemauslastungsmusters.

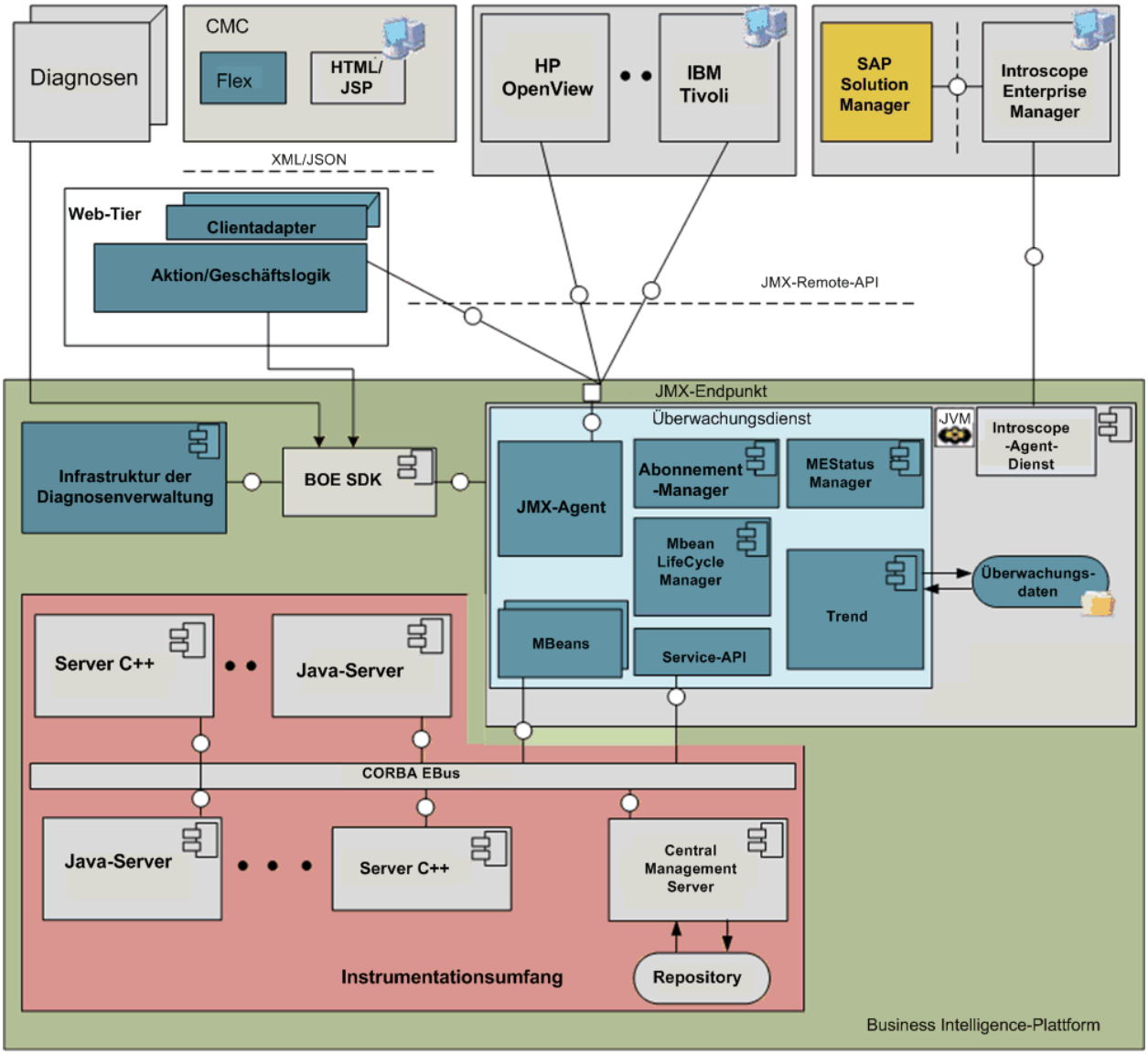
Warnmeldung

Eine Warnmeldung ist eine Benachrichtigung, die vom Überwachungstool generiert wird, wenn ein festgelegter Schwellenwert für eine auf ein Kontrollmodul angewendete Metrik überschritten wird. Sie können auswählen, ob Sie die Warnmeldungen per E-Mail oder über die Seite *Dashboard* erhalten.

20.2.1 Architektur

Dieser Abschnitt enthält einen groben Überblick über die Überwachungsarchitektur und eine kurze Erklärung zu den Rollen der unterschiedlichen Komponenten. Die Überwachungsarchitektur wird im Folgenden grafisch dargestellt:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.



Die Architekturkomponenten der höheren Ebene sind im Folgenden aufgeführt:

- Adaptive Processing Server (APS)
- JMX-Agent/-Server (Java Management Extensions)
- MBeans
- JMX-Clients
- Verwaltungskonsolen
- Trenddatenbank

Der Überwachungsdienst wird auf dem Adaptive Processing Server gehostet. Die Anwendung basiert auf JMX-Technologie.

Der Überwachungsdienst stellt die wichtigsten in der Überwachung verfügbaren Dienste bereit. Der Überwachungsdienst stellt folgende Dienste bereit:

- Bereitstellung des JMX-Agent-Diensts.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Dynamische Erstellung der MBeans für SAP BusinessObjects-Server.
- Bereitstellung von LifeCycle-Management für die MBeans.
- Bereitstellung eines Mechanismus zum Registrieren neuer Diagnosen.
- Ermöglicht Benutzern die Erstellung komplexer Schwellenwertbedingungen unter Verwendung der Server-Metriken.
- Bereitstellung des Schwellenwert-Benachrichtigungsmechanismus und Senden von Warnmeldungen.
- Speichert historische Daten.

Der Dienst für die zeitgesteuerte Verarbeitung von Diagnosen, der auf dem Adaptive Job Server gehostet wird, wickelt die Ausführung und Zeitsteuerung von Diagnosen ab. Aus diesem Grunde sollte der Adaptive Job Server laufen, damit die Diagnosen durchgeführt werden können.

Das Monitoring stellt auch einen URL-Endpunkt für JMX oder Remote Method Invocation (RMI) zur Verfügung. Andere Unternehmensanwendungen wie etwa IBM Tivoli Monitoring können eine Verbindung mit der Überwachungsanwendung herstellen und unter Verwendung einer JMX-Remote-API auf die BI-Plattform-Metriken zugreifen. Das Monitoring verwendet eine spezielle Derby-Datenbank für die Speicherung von Verlaufsdaten zum Ermitteln von Trends. Weitere Informationen zum Schema der Trenddatenbank erhalten Sie unter *Trenddatenbankschema* [Seite 1031].

20.3 Konfigurieren von Datenbank-Support für die Überwachung

In diesem Abschnitt wird die Konfiguration der Überwachung und die Berichterstellung anhand von Überwachungsdaten beschrieben.

> **Hinweis**
>
> Nur Kontrollmodule, für die die Einstellung **In Trenddatenbank schreiben** aktiviert ist, schreiben Überwachungsinformationen in die Trenddatenbank.

Es gibt zwei Datenbankoptionen zum Aufzeichnen von Überwachungsinformationen:

- Aufzeichnen der Informationen in der eingebetteten Derby-Datenbase (Standardoption).

  Das Überwachungstool enthält eine eingebettete Derby-Datenbank, häufig als “Trenddatenbank” bezeichnet, in der die Überwachungsinformationen standardmäßig gespeichert werden. Die Benutzer können Berichte aus der Derby-Datenbank erstellen, sie bietet jedoch kein Failover oder Sicherungs- und Wiederherstellungstools herkömmlicher relationaler Datenbanken. Außerdem muss die Derby-Datenbank manuell regeneriert werden, um die aktuellen Informationen zurückzugeben.
- Aufzeichnen der Informationen in der Audit-Datenbank (der relationalen Datenbank, in der der CMS Audit-Daten speichert).

  Anstelle der Standard-Derby-Datenbank können Sie auch den Audit-Datenspeicher – häufig als Audit-Datenbank bezeichnet – verwenden. Sie können entweder die in der BI-Plattform enthaltene Audit-Datenbank oder eine andere unterstützte Datenbank, die Sie als Ihre Audit-Datenbank konfiguriert haben, verwenden. Benutzer, die die Audit-Datenbank verwenden, können Berichte anhand der Audit-Daten zusammen mit den Überwachungsinformationen erstellen. Bei der Erfassung der Daten in einer relationalen Datenbank stehen Sicherungs- und Wiederherstellungsfunktionen sowie Echtzeitverfügbarkeit der Daten zur Verfügung.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Konfiguration zur Verwendung der Derby-Datenbank [Seite 671]
Konfiguration für die Verwendung der Audit-Datenbank [Seite 671]

20.3.1 Konfiguration zur Verwendung der Derby-Datenbank

Das Überwachungstool speichert Überwachungsdaten standardmäßig in der eingebetteten Derby-Datenbank. Wenn Sie die Derby-Datenbank verwenden möchten, stellen Sie sicher, dass die folgenden Datenbankeinstellungen in der CMC vorgenommen wurden:

1. Klicken Sie im Bereich *Verwalten* auf der CMC-Startseite auf **Anwendungen**.
2. Doppelklicken Sie auf **Überwachungstool**, um die Seite "Eigenschaften" zu öffnen.
3. Prüfen Sie im Bereich *Trenddatenbank-Einstellungen*, ob **Eingebettete Datenbank verwenden** ausgewählt wurde.

Um Abfragen in der Derby-Datenbank für Berichterstellung und Datenanalyse auszuführen, ist ein Universum für die Derby-Datenbank erforderlich. Es wird ein Universum mit Ihrer BI-Plattform-Implementierung in diesem Speicherort in der CMC bereitgestellt: **Universen** > **Monitoring TrendData Universes**.

20.3.2 Konfiguration für die Verwendung der Audit-Datenbank

Wenn Sie die Audit-Datenbank für Überwachungsdaten verwenden möchten, müssen Sie zusätzlich folgende Konfigurationsschritte ausführen:

- Falls Ihre Derby-Trenddatenbank bereits Daten enthält, müssen Sie die Derby-Datenbank in die Audit-Datenbank migrieren und anschließend die BI-Plattform konfigurieren, um Überwachungsinformationen in der Audit-Datenbank aufzuzeichnen. Nachfolgend sind die wichtigsten auszuführenden Schritte aufgeführt. Einzelheiten finden Sie in den verwandten Themen.
  1. Migrieren Sie die Derby-Datenbank.
  2. Konfigurieren Sie die SBO-Dateien, und fügen Sie Aliasnamen hinzu.
  3. Wechseln Sie zur Audit-Datenbank.
  4. Starten Sie den Adaptive Processing Server neu, von dem der Überwachungsdienst gehostet wird.
  5. Stellen Sie auf dem Monitoring-Dashboard sicher, dass alles erwartungsgemäß funktioniert. Verifizieren Sie, dass die folgenden Überwachungstabellen in der Datenbank erstellt wurden:

     MOT_MES_DETAILS
     MOT_MES_METRICS
     MOT_TREND_DATA
     MOT_TREND_DETAILS
- Falls Ihre Trenddatenbank keine Daten enthält, Sie also über eine Neuinstallation verfügen, muss die Datenbank nicht migriert werden; es muss lediglich die BI-Plattform so konfiguriert werden, dass sie Überwachungsinformationen in der Audit-Datenbank aufzeichnet. Nachfolgend sind die wichtigsten auszuführenden Schritte aufgeführt. Einzelheiten finden Sie in den verwandten Themen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Verifizieren Sie, dass die Datenbank funktioniert und das Auditing ordnungsgemäß ausgeführt wird.
2. Erstellen Sie die Überwachungstabellen im ADS.
3. Konfigurieren Sie die SBO-Dateien, und fügen Sie Aliasnamen hinzu.
4. Wechseln Sie zur Audit-Datenbank.
5. Starten Sie den Adaptive Processing Server neu, von dem der Überwachungsdienst gehostet wird.
6. Stellen Sie auf dem Monitoring-Dashboard sicher, dass alles erwartungsgemäß funktioniert. Verifizieren Sie, dass die folgenden Überwachungstabellen in der Datenbank erstellt wurden:

   MOT_MES_DETAILS
   MOT_MES_METRICS
   MOT_TREND_DATA
   MOT_TREND_DETAILS

Hinweis

Wenn Sie Überwachungsdaten in der Audit-Datenbank aufzeichnen und anhand dieser Daten Berichte erstellen wollen, müssen Sie ein benutzerdefiniertes Universum erstellen. Das in der BI-Plattform enthaltene Universum ist ausschließlich zur Verwendung mit der eingebetteten Derby-Datenbank ausgelegt.

Weitere Informationen

Migration der Derby-Datenbank in die Audit-Datenbank [Seite 672]
Konfigurieren von SBO-Dateien [Seite 675]
Einfügen von Aliasnamen in die SBO-Datei [Seite 677]
Wechseln zur Audit-Datenbank [Seite 678]
Erstellen der Überwachungstabellen im ADS [Seite 673]

20.3.2.1 Migration der Derby-Datenbank in die Audit-Datenbank

Wenn Sie die Audit-Datenbank für Ihre Überwachungsdaten verwenden möchten, und Ihre Derby-Trenddatenbank bereits Daten enthält, müssen Sie die Derby-Datenbank in die Audit-Datenbank migrieren.

Bevor Sie mit der Datenmigration beginnen überprüfen Sie, ob folgende Voraussetzungen erfüllt sind:

- Die Datenbank funktioniert, und das Auditing wird ordnungsgemäß ausgeführt.
- Sie verfügen über die nötigen Rechte und Datenbank-Clientanwendungen auf der Zieldatenbank, um neue Tabellen zu erstellen, CSV-Dumps zu importieren usw.
- Die Audit-Datenbank unterstützt den Import von CSV-Dateien mit kommagetrennten Werten.

Führen Sie die folgenden Schritte aus, um die Datenbankmigration durchzuführen:

1. *Sichern der Derby-Datenbank* [Seite 673]
2. *Exportieren von Daten in CSV-Dateien* [Seite 673]
3. *Erstellen der Überwachungstabellen im ADS* [Seite 673]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. *Wiederherstellen von Inhalten in der Zieldatenbank* [Seite 674]

> **Hinweis**
>
> In einem geclusterten Szenario wird erwartet, dass die Benutzer dieselbe Instanz der Derby-Datenbank für alle Überwachungsinstanzen verwenden. Falls die Benutzer über mehrere Derby-Datenbankinstanzen in einem geclusterten Szenario verfügen, sollten sie nur die Daten von einer Derby-Instanz importieren. Da der Import von Daten von mehreren Derby-Instanzen zu Dateninkonsistenz führt, wird er nicht empfohlen.

20.3.2.1.1 Sichern der Derby-Datenbank

1. Klicken Sie im Bereich *Verwalten* auf der CMC-Startseite auf **Anwendungen**.
2. Doppelklicken Sie auf **Überwachungstool**, um die Seite "Eigenschaften" zu öffnen.
3. Geben Sie im Bereich *Trenddatenbank-Einstellungen* einen Dateispeicherort ein, an dem die Derby-Trenddatenbank gesichert werden soll, und klicken Sie auf **Sichern**.
4. Klicken Sie neben *Datenbanksicherungs-Auftrag ausführen* auf **Jetzt**.

   Wenn die Datenbanksicherung erfolgreich ist, wird eine Bestätigungsmeldung angezeigt. Überprüfen Sie auch den Speicherort des Ordners, den Sie als Sicherungsverzeichnis eingegeben haben, und stellen Sie sicher, dass die Sicherungsdateien dort abgelegt wurden.

20.3.2.1.2 Exportieren von Daten in CSV-Dateien

In diesem Abschnitt wird das Erstellen der für die Migration erforderlichen CSV-Dump-Dateien erläutert. Die CSV-Dateien enthalten kommagetrennte Werte des Dateninhalts der eingebetteten Derby-Datenbank.

1. Klicken Sie im Bereich *Verwalten* auf der CMC-Startseite auf **Anwendungen**.
2. Doppelklicken Sie auf **Überwachungstool**, um die Seite "Eigenschaften" zu öffnen.
3. Klicken Sie im Bereich *Trenddatenbank-Einstellungen* neben *Daten aus der eingebetteten Datenbank als CSV-Dateien exportieren* auf **Exportieren**.

Die folgenden vier CSV-Dateien werden am Standardspeicherort der Trenddatenbank, d.h. `<BOE_Install_Verz>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0/Data/TrendingDB`, generiert:

- Mot_Mes_Details.csv
- Mot_Trend_Data.csv
- Mot_Trend_Details.csv
- Mot_Mes_Metrics.csv

20.3.2.1.3 Erstellen der Überwachungstabellen im ADS

Führen Sie die folgenden Schritte aus, um die Ziel-Audit-Datenbank vorzubereiten:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Nach der Installation der BI-Plattform stehen die zu den unterstützten CMS-Audit-Datenbanken gehörenden DDLs im Verzeichnis `<Installverz>\ SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB` zur Verfügung. Dort befinden sich sieben verschiedene Dateien (mit der Erweiterung .sql) mit dem entsprechenden Datenbanknamen. Beispiel: `Oracle.sql` für Oracle, `Sybase ASE.sql` für die Sybase-ASE-Datenbank usw.
2. Wechseln Sie nun zur Zieldatenbank (in diesem Fall ist die Zieldatenbank die Datenbank, in der das CMS-Auditing konfiguriert wurde), und führen Sie die .sql-Datei aus. Die vier folgenden Überwachungstabellen werden erstellt: `MOT_TREND_DETAILS`, `MOT_TREND_DATA`, `MOT_MES_DETAILS` und `MOT_MES_METRICS`. Die erforderlichen Indizes werden ebenfalls mit den Tabellen erstellt.

Wenn die Daten mit den korrekten Datentypen aus der .sql-Datei erstellt werden, wird das für das Überwachungstool erforderliche Datenbankschema erstellt.

20.3.2.1.4 Wiederherstellen von Inhalten in der Zieldatenbank

Die folgenden Schritte sind durchzuführen, um den Inhalt in der Zieldatenbank wiederherzustellen:

1. Aktivieren der Identity-Einfügung.

   Die Überwachungstabellen enthalten eine Reihe von IDENTITY-Spalten. Diese Spalten generieren ihre Werte automatisch. Einige Datenbanken (wie z.B. MS SQL Server und SYBASE ASE) erlauben keine explizite Einfügung von Werten in diese Spalten. Während der Datenmigration müssen jedoch auch die Werte der Identity-Spalte migriert werden. Daher müssen die Benutzer das Einfügen dieser Werte über den folgenden SQL-Befehl explizit aktivieren: `SET IDENTITY_INSERT <TABELLENNAME> ON`.
2. Importieren der CSV-Dump-Datei in die Zieltabelle.

   Mit der in den Datenbankclients installierten Software können Benutzer die Daten entweder über eine Menüoption oder einen Befehl von einer CSV-Datei in die Tabelle importieren. Die Benutzer müssen diese Option zum Importieren der Daten aus der CSV-Datei in die entsprechende Tabelle verwenden. Importieren Sie die Datendateien in folgender Reihenfolge in die neuen Tabellen:

   1. `MOT_TREND_DETAILS`
   2. `MOT_TREND_DATA`
   3. `MOT_MES_DETAILS`
   4. `MOT_MES_METRICS`
3. Deaktivieren der Identity-Einfügung.

   Nach Abschluss des Datenimports müssen die Benutzer die Identity-Einfügung für diese Tabelle über den folgenden SQL-Befehl deaktivieren:`SET IDENTITY_INSERT <TABELLENNAME> OFF`.

   Die Deaktivierung der Identity-Einfügung für eine Tabelle nach dem Datenimport ist Voraussetzung für die Aktivierung der Identity-Einfügung für die nächste Tabelle. Aus diesem Grund kann der Identity-Einfügungsvorgang stets nur für eine Tabelle aktiviert werden.

Die Aktivierung oder Deaktivierung der Identity-Einfügung ist nur auf MS SQL Server und Sybase ASE anwendbar. Für andere Datenbanken, z.B. Oracle, MaxDb, DB2, MySQL und SQL Anywhere, ist dieser Vorgang nicht erforderlich. Sie können die Daten direkt in die Tabellen importieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

20.3.2.2 Konfigurieren von SBO-Dateien

Die Überwachungsanwendung verwendet intern Connection-Server-Bibliotheken, und die SBO-Konfiguration ist erforderlich, damit der Connection Server eine Verbindung zum Datenbanktreiber herstellen kann. Sie müssen den Datenbanktreiber und seinen Speicherort in der SBO-Datei angeben, um diese Verbindung herzustellen.

Hinweis

Das Überwachungstool bezieht sich auf den Überwachungsverbindungsnamen und verwendet JDBC bei Angabe von `<Hostname>.<Portnr>.<dbName>`, ansonsten ODBC. Die Connection-Server-SBO-Dateien müssen entsprechend für das Überwachungstool konfiguriert werden, damit eine Verbindung zur Audit-Datenbank hergestellt werden kann.

Hinweis

Für Oracle-Datenbanken werden nur JDBC-Verbindungen unterstützt.

Beispiel

- Wenn das Feld "Verbindungsname", das auf der Seite "Auditing" der CMC konfiguriert wird, die Struktur `<Hostname><Portnr><dbName>` aufweist, muss der JAR-Treiber in der folgenden Datei konfiguriert werden: `dataAccess\connectionServer\jdbc\<dbTyp>.sbo`
- Wenn das Feld "Verbindungsname", das auf der Seite "Auditing" der CMC konfiguriert wird, ein ODBC-DSN ist, muss der Treiber in der folgenden Datei konfiguriert werden: `<Installverz>\dataAccess\connectionServer\odbc\<dbTyp>.sbo`
- Wenn die für die Überwachung verwendete Datenbank eine SAP-HANA-Datenbank ist, muss der Treiber in der folgenden Datei konfiguriert werden: `<Installverz>\dataAccess\connectionServer\odbc\newdb.sbo`
- Wenn die für die Überwachung verwendete Datenbank eine MS-SQL-Server-Datenbank ist, muss der Treiber in der folgenden Datei konfiguriert werden: `<Installverz>\dataAccess\connectionServer\odbc\sqlsrv.sbo`
- Wenn die für die Überwachung verwendete Datenbank eine DB2-for-i-Datenbank (nur Windows) ist, muss der Treiber in der folgenden Datei konfiguriert werden: `<Installverz>\dataAccess\connectionServer\odbc\db2iseries.sbo`.

Konfigurieren von SBO-Dateien

Die ODBC-Bibliotheken sind in der Regel in den SBO-Dateien bereits konfiguriert, und Sie müssen nur die Aliasnamen hinzufügen. Andernfalls führen Sie die Konfiguration in der SBO-Datei nach dem Muster der folgenden Beispiele durch:

Beispiel

- Wenn die für die Überwachung verwendete Datenbank eine SAP-HANA-Datenbank ist, muss die SBO-Konfiguration wie folgt aussehen:

```
<DataBase Active="Yes" Name="SAP HANA database 1.0" Platform="MSWindows">
    <Aliases>
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
        <Alias>SAP High-Performance Analytic Appliance (SAP HANA) 1.0</Alias>
        <Alias>Hana</Alias>
    </Aliases>
    <Libraries>
        <Library Platform="MSWindows">dbd_wnewdb</Library>
        <Library Platform="MSWindows">dbd_newdb</Library>
    </Libraries>
    <Parameter Name="Driver Name">HDBODBC</Parameter>
</DataBase>
```

- Wenn die für die Überwachung verwendete Datenbank eine MS-SQL-Server-2008-Datenbank ist, muss die SBO-Konfiguration wie folgt aussehen:

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
    <Libraries>
        <Library>dbd_wmssql</Library>
        <Library>dbd_mssql</Library>
    </Libraries>
    <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
    <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
    <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
    <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
</DataBase>
```

- Wenn die für die Überwachung verwendete Datenbank eine DB2-for-i-Datenbank (nur für Windows) ist, muss die SBO-Konfiguration wie folgt aussehen:

```
<DataBase Active="Yes" Name="DB2 UDB for iSeries v5">
 <!-- You can add an alias here if you are using some connections that are
defined with an older database engine -->
 <Alias>DB2/400 V5</Alias>
 <Alias>DB2/400 V4</Alias>
 <Alias>DB2 for iSeries v4</Alias>
 <Alias>DB2</Alias>
 </Aliases>
```

- Wenn die für die Überwachung verwendete Datenbank eine MySQL-5-Datenbank ist, muss die SBO-Konfiguration wie folgt aussehen:

```
<DataBase Active="Yes" Name="MySQL 5">
    <JDBCDriver>
        <ClassPath>
            <Path>C:\mysqljdbcdriver.jar</Path>
              </ClassPath>
        <Parameter Name="JDBC Class">com.mysql.jdbc.Driver</Parameter>
        <Parameter Name="URL Format">jdbc:mysql://$DATASOURCE$/$DATABASE$</
Parameter>
    </JDBCDriver>
    <Parameter Name="Driver Capabilities">Query,Procedures</Parameter>
    <Parameter Name="Force Execute">Always</Parameter>
    <Parameter Name="Extensions">mysql5,mysql,jdbc</Parameter>
</DataBase>
```

- Wenn die für die Überwachung verwendete Datenbank eine Oracle-Datenbank ist, muss die SBO-Konfiguration wie folgt aussehen:

```
<DataBase Active="Yes" Name="Oracle 11">
        <Aliases>
           <Alias>Oracle</Alias>
        </Aliases>
      <JDBCDriver>
            <ClassPath>
               <Path>C:\app\Administrator\product\11.2.0\client_64\jdbc\lib
\ojdbc6.jar</Path>
             </ClassPath>
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
                <Parameter Name="JDBC Class">oracle.jdbc.OracleDriver</
Parameter>
                <Parameter Name="URL Format">jdbc:oracle:thin:@//$DATASOURCE$/
$DATABASE$</Parameter>
       </JDBCDriver>
       <Parameter Name="Extensions">oracle11,oracle,jdbc</Parameter>
        <Parameter Name="Escape Character">/</Parameter>
         <Parameter Name="Force Execute">Always</Parameter>
         <Parameter Name="Catalog Separator">.</Parameter>
</DataBase>
```

Weitere Informationen über die Konfiguration des Treibers in den SBO-Dateien finden Sie im *Datenzugriffshandbuch*.

20.3.2.3 Einfügen von Aliasnamen in die SBO-Datei

Zusätzlich zur Konfiguration der Treiber müssen Benutzer auch einen Alias in die SBO-Datei unter der für das Auditing verwendeten Datenbankversion einfügen. Die folgende Tabelle enthält die Aliasnamen, die für die angegebenen Datenbanken verwendet werden sollten.

DB-Name	In der SBO zu verwendender Aliasname
SAP HANA	Hana
Microsoft SQL Server	MS SQL Server
My SQL	MySQL
SAP Max DB	MaxDB
IBM DB2	DB2
Sybase SQL Anywhere	Sybase SQL Anywhere
Sybase Adaptive Server Enterprise	Sybase Adaptive Server Enterprise
Oracle	Oracle

Die angegebenen Namen müssen verwendet werden, da das Überwachungstool die SBO nach diesen Namen durchsucht.

Beispiel

Wenn die für das Auditing verwendete Datenbank MS SQL Server 2008 ist, muss der Alias wie folgt zu der SBO hinzugefügt werden:

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
        <Aliases>
        <Alias>MS SQL Server</Alias>
        </Aliases>
            <Libraries>
                <Library>dbd_wmssql</Library>
                <Library>dbd_mssql</Library>
            </Libraries>
            <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
            <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
            <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
            <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
   </DataBase>
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

20.3.2.4 Wechseln zur Audit-Datenbank

Wechseln Sie die Datenbank, damit Überwachungstrendinformationen in der Audit-Datenbank gespeichert werden.

1. Klicken Sie im Bereich *Verwalten* auf der CMC-Startseite auf **Anwendungen**.
2. Doppelklicken Sie auf **Überwachungstool**, um die Seite "Eigenschaften" zu öffnen.
3. Wählen Sie im Bereich *Trenddatenbank-Einstellungen* die Option **Audit-Datenbank verwenden**.

> **Hinweis**
>
> Wenn Sie für die Auditierung eine Oracle-Datenbank verwenden, muss die **ADS Datenbank Verbindungsname** auf der Auditing-Seite der CMC als JDBC-Verbindung angegeben werden. Geben Sie den Verbindungsnamen folgendermaßen an: `<Servername>,<Port>,<Dienstname>`.

> **Hinweis**
>
> Um sicherzustellen, dass die Überwachungstabellen ordnungsgemäß erstellt werden, gewähren Sie folgende Berechtigungen für das Datenbank-Benutzerkonto:
>
> AUSFÜHREN
> SEQUENZ ERSTELLEN
> AUSLÖSER ERSTELLEN

20.4 Konfigurationseigenschaften

In diesem Abschnitt werden die Monitoring-Eigenschaften und ihre Bearbeitung beschrieben.

So zeigen Sie die Konfigurationseigenschaften des Monitorings an:

1. Wechseln Sie zur Registerkarte **Anwendungen** der CMC.
2. Klicken Sie mit der rechten Maustaste auf **Überwachungstool**, und wählen Sie **Eigenschaften** aus. Das Fenster *Überwachungstool-Eigenschaften* wird angezeigt. Die konfigurierbaren Eigenschaften werden in der folgenden Tabelle beschrieben:

Sektion	Feld	Beschreibung
	Überwachungstool aktivieren	Wählen Sie diese Option, um die Überwachungsfunktionen zu aktivieren. Wenn Sie die Auswahl dieser Option aufheben, werden sämtliche Überwachungsfunktionen, mit Ausnahme der Diagnosen, deaktiviert. Die Diagnose-Trend wird ebenfalls deaktiviert.
	Endpunkt-URL des Standard-JMX-Agenten (IIOP)	Enthält die Endpunkt-URL des Standard-JMX-Agenten, die das IIOP-Protokoll verwendet. Diese URL wird automatisch generiert, wenn Sie die Überwachung aktivieren

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Sektion	Feld	Beschreibung
		und dann den Server neu starten. Dies ist das Standardprotokoll für den Überwachungsdienst. Dieses Feld ist schreibgeschützt.
RMI	**RMI-Protokoll für JMX aktivieren**	Diese Option ist standardmäßig deaktiviert. Wenn Sie diese Option aktivieren, müssen Sie die RMI-Portnummer angeben. Dieser Port wird sowohl für den RMI-Registrierungseintrag als auch für den RMI-Konnektorport verwendet. Dieser Port sollte für den Dienst zur Verfügung stehen, anderenfalls kann der Dienst nicht gestartet werden. Starten Sie den Server neu, nachdem Sie die RMI-Portnummer angegeben haben. Nachdem der Server neu gestartet wurde, wird die Endpunkt-URL für den RMI JMX-Agent generiert. Diese Eigenschaft ist schreibgeschützt, enthält die Endpunkt-URL des JMX-Agents und verwendet das RMI-Protokoll. Verwenden Sie diese URL, um eine Verbindung mit dem Monitoring anderer Clients herzustellen.
Hostmetriken	**Hostmetriken aktivieren**	Diese Option ist standardmäßig deaktiviert. Wenn Sie diese Option aktivieren, müssen Sie den Pfad zur Installation der SAPOSCOL-Binärdatei angeben. Um Hostmetriken zu aktivieren, müssen Sie SAPOSCOL installieren. Weitere Informationen zur Installation von SAPOSCOL finden Sie unter “Installieren von SAPOSCOL”.
Trenddatenbankeinstellungen	**Audit-Datenbank verwenden**	Wählen Sie diese Option, um den Trendverlauf der Metriken in der CMS-Audit-Datenbank zu speichern. **Hinweis** Das CMS-Auditing muss aktiviert sein, damit dies funktioniert.
	Eingebettete Datenbank verwenden	Wählen Sie diese Option, um den Metrik-/Kontrollmodul-Trendverlauf in der im Überwachungstool enthaltenen eingebetteten Datenbank zu speichern.
	Ältere Daten löschen, wenn Datenbankgröße auf über (MB) anwächst	Die Daten der Trenddatenbank werden bereinigt, wenn die Datenbankgröße die angegebene Größe übersteigt. Für die Datenbank

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Sektion	Feld	Beschreibung
		wird ein Puffer von 30 % eingerichtet. Wenn Sie diese Eigenschaft beispielsweise auf 100 MB gesetzt haben, und die Größe der Datenbank bei der Systemprüfung mehr als 100 MB beträgt, werden die Daten bis auf eine Datenbankgröße von 70 MB bereinigt.
	Datenbankbereinigung täglich ausführen um	Die Datenbankbereinigung wird zum angegebenen Zeitpunkt gestartet. Die Datenbank wird bereinigt, wenn die Datenbankgröße die festgelegte maximale Größe übersteigt.
	Sicherung der Trenddatenbank alle	Gibt die Anzahl der Stunden zwischen jeder Sicherung der Trenddatenbank an. Ist dieser Wert festgelegt, wird bei jedem Start des Systems oder bei jedem Neustart des APS sowie in jedem angegebenen Intervall eine Sicherung durchgeführt.
	Sicherungsverzeichnis der Trenddatenbank	Das Verzeichnis ist nicht standardmäßig angegeben. Sie können jedoch einen Pfad angeben. Geben Sie einen absoluten und keinen relativen Pfad an. Bei einem freigegebenen Verzeichnispfad muss eine Berechtigung für den Zugriff auf den freigegebenen Verzeichnispfad erteilt werden.
	Datenbanksicherungs-Auftrag ausführen	Wenn Sie diese Option aktivieren, wird der Datenbanksicherungs-Auftrag gestartet. Sie müssen den Verzeichnispfad für die Datenbanksicherung angeben, bevor Sie diese Option wählen.
	Daten aus der eingebetteten Datenbank als CSV-Dateien exportieren	Klicken Sie auf die Schaltfläche **Exportieren**, um die Datenbank als CSV-Dateien (kommagetrennte Werte) zu exportieren.
	Pfad der Trenddatenbank	Standardmäßig lautet der Pfad der Trenddatenbank `<INSTALLVERZ>\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0/Data/TrendingDB`. Sie können auch einen anderen Pfad angeben. Geben Sie jedoch einen absoluten und keinen relativen Pfad an. Für eine geclusterte Umgebung kann der Pfad freigegeben werden, und es muss eine Berechtigung für den Zugriff auf den freigegebenen Verzeichnispfad erteilt werden.
Weitere Einstellungen	**Metrik-Regenerierungsintervall (Sekunden)**	Der Mindestwert für das Intervall ist 15 Sekunden. Das Intervall bestimmt Folgendes:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Sektion	Feld	Beschreibung
		○ Berechnung der Schwellwertbedingung für die Kontrollmodule: Die Regeln für Achtung und Gefahr werden fortlaufend in dem angegebenen Zeitintervall berechnet. ○ Berechnung des Kontrollmodulstatus: Der Kontrollmodulstatus wird kontinuierlich innerhalb des festgelegten Zeitintervalls berechnet, sofern die Ereigniseinstellung des Kontrollmoduls mit folgender Option aktiviert wird: **Kontrollmodulstatus jedes Mal ändern, wenn die Auswertung der Achtung- oder Gefahr-Regel "wahr" ergibt**. ○ Trendermittlungszeitraum: Der Verlaufsmodus für die Diagramme wird fortlaufend in dem angegebenen Zeitintervall aufgezeichnet.
	Intervall für die automatische Regenerierung der Überwachungsoberfläche (Sekunden)	Dieses Intervall wird für die automatische Regenerierung auf der Überwachungsoberfläche verwendet (einschließlich Dashboard, Kontrollmodulliste und Diagnosen). Die Mindestdauer des Intervalls beträgt 15 Sekunden. Die Einstellungen für die automatische Regenerierung wirken sich nicht auf die Zeitdauer im Live-Modus aus, die standardmäßig auf 15 Sekunden festgelegt ist.
	Frequenz der Warnmeldungserinnerung (Tage)	Gibt die Anzahl an Tagen an, bevor eine Warnmeldungserinnerung generiert wird.

3. Klicken Sie auf **Speichern**.

> **Hinweis**
>
> Wenn Sie, mit Ausnahme der Aktivierung und Deaktivierung des Überwachungstools, eine dieser Eigenschaften ändern, müssen die Adaptive Processing Server, die die Überwachungsdienste hosten, neu gestartet werden.

Installieren von SAPOSCOL

Führen Sie die folgenden Schritte aus, um SAPOSCOL zu installieren:

1. Laden Sie `SAPHOSTAGENT710_XX.SAR` vom SAP Service Marketplace (*http://service.sap.com*) herunter.
2. Extrahieren Sie `SAPHOSTAGENT710_XX.SAR`, indem Sie den Befehl *SAPCAR.EXE -xvf SAPHOSTAGENT710_XX.SAR* ausführen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3. Installieren Sie `SAPHOSTEXEC`, indem Sie den Befehl *saphostexec.exe -install* ausführen. Wenn SAPHOSTEXEC als Dienst installiert ist, wird SAPOSCOL gestartet.
4. Prüfen Sie den Status von SAPOSCOL, indem Sie den Befehl *saposcol -s* ausführen.

20.4.1 JMX-Endpunkt-URL

Das Monitoring stellt eine JMX-Endpunkt-URL zur Verfügung, über die andere Clients unter Verwendung der JMX-Remote-API eine Verbindung herstellen können. Die JMX-Konnektivität wird standardmäßig über die Transportdatei von IOOP (Internet Inter-Orb Protocol) oder CORBA (Common Object Request Broker Architecture) bereitgestellt. Diese Verbindungs-URL wird auf der Eigenschaftenseite des Monitorings angezeigt. Durch die Möglichkeit, eine Verbindung über IIOP herzustellen, entfällt die Notwendigkeit, sich um Firewalls zu kümmern und Ports bereitzustellen. Die CORBA-Ports sind standardmäßig verfügbar. Die in der folgenden Tabelle aufgeführten JAR-Dateien werden vom JMX-Client benötigt, um eine Verbindung herzustellen:

JAR-Dateien
`activation-1.1.jar`
`axiom-api-1.2.5.jar`
`axiom-impl-1.2.5.jar`
`axis2-adb-1.3.jar`
`axis2-kernel-1.3.jar`
`cecore.jar`
`celib.jar`
`cesession.jar`
`commons-logging-1.1.jar`
`corbaidl.jar`
`ebus405.jar`
`log4j.jar`
`logging.jar`
`monitoring-plugins.jar`
`monitoring-sdk.jar`
`stax-api-1.0.1.jar`
`wsdl4j-1.6.2.jar`
`wstx-asl-3.2.1.jar`
`XmlSchema-1.3.2.jar`
`TraceLog.jar`
`ceaspect.jar`
`aspectjrt.jar`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eine weitere Option ist die Verbindung über den standardmäßigen RMI-Port. Weitere Informationen zur Herstellung einer Verbindung über den RMI-Port erhalten Sie unter *Konfigurationseigenschaften* [Seite 678].

20.4.2 HTTPS-Authentifizierung für Überwachungsdiagnosen

Die HTTPS-Serverauthentifizierung für Überwachungsdiagnosen wird unterstützt und erfordert vor dem Einsatz folgende Konfiguration:

1. Importieren Sie das Serverzertifikat in den Client-Truststore. Auf diese Weise kann die Clientseite (die Diagnose) die Serveridentität überprüfen. Führen Sie diesen Befehl aus: `<INSTALL_ROOT>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\lib> keytool -import -alias ca -keystore "<INSTALL_ROOT>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security\cacerts" -file ca.cer`

   `ca.cer` ist das selbstsignierte Zertifikat des Servers oder das Zertifikat der Zertifizierungsstelle (üblicherweise eine interne Zertifizierungsstelle), die das Serverzertifikat generiert hat. Wenn das Serverzertifikat von einer renommierten Zertifizierungsstelle generiert wurde, muss es nicht importiert werden, und dieser Schritt kann übersprungen werden. Dies liegt daran, dass das Serverzertifikat durch die Zertifizierungsstelle überprüft wird, deren öffentlicher Schlüssel sich standardmäßig bereits im Truststore befindet.
2. Ändern Sie die *URL-Basis* in den Einstellungen der BI-Launchpad-Diagnose in `https://<URL>/BOE/BI`, wobei <URL> sich auf den Host mit dem Namen bezieht, der im Zertifikat verwendet wird.

Die HTTPS-Clientauthentifizierung für Überwachungsdiagnosen wird nicht unterstützt.

20.4.3 Kennwortverschlüsselung für Diagnosen

Um bei der Verwendung von Diagnosen sicherzustellen, dass Kennwörter verschlüsselt sind, müssen Sie den Parameter *true* zu allen Kennwortparametern der Überwachungsdiagnose hinzufügen, wenn Sie die Diagnose über die Befehlszeile erstellen. Weitere Informationen und ein Syntaxbeispiel finden Sie im Thema *Managing Probes Through the Command Line* (Verwalten von Diagnosen über die Befehlszeile) in der CMC-Hilfe.

20.5 Integrieren in andere Anwendungen

Enterprise-Lösungen wie z.B. IBM Tivoli Monitoring können als JMX-Clients, die über die JMX-Endpunkt-URL eine Verbindung herstellen, in das Überwachungstool integriert werden. Nach der Integration können die SAP-BusinessObjects-Metriken auf der Benutzeroberfläche des Clients angezeigt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

20.5.1 Integrieren des Monitorings in IBM Tivoli

Um das Überwachungstool in IBM Tivoli zu integrieren, müssen Sie einen IBM Tivoli Monitoring Agent erstellen, installieren und konfigurieren. Führen Sie folgende Schritte für die Erstellung eines IBM Tivoli Monitoring Agents aus:

1. Installieren Sie IBM Tivoli Monitoring Agent Builder, Version 6.2.1.
2. Erstellen Sie einen neuen Agent. Weitere Informationen zum Erstellen eines neuen Agents finden Sie im Benutzerhandbuch für IBM Tivoli Monitoring Agent.
3. Wählen Sie im Schritt "“Defining data monitoring types”" (Datenüberwachungstypen definieren) die Option **Data from a server** (Daten von einem Server) im Bereich *Monitoring Data Categories* (Überwachungsdatenkategorien), und wählen Sie im Bereich **Data Sources** (Datenquellen) "*JMX*" aus.
4. Klicken Sie auf **Weiter**.
5. Klicken Sie im Fenster *JMX Information* (JMX-Informationen) auf **Browse** (Durchsuchen), um alle JMX MBeans auf dem MBean-Server anzuzeigen.

   > **Hinweis**
   >
   > Wenn Sie den Browser zum ersten Mal ausführen, müssen Sie eine neue Verbindung hinzufügen.

6. Klicken Sie im Fenster *Java Management Extensions (JMX) Browser* auf das "+" bei **Connection Name** (Verbindungsname), um eine neue Verbindung hinzuzufügen.
7. Wählen Sie im Fenster *MBean Server Connection Wizard* (Verbindungsassistent des MBean-Servers) die Option **Standard JMX Connections (JSR-160)** (Standard-JMX-Verbindungen (JSR-160)) aus.
8. Geben Sie im Fenster *Connection Properties* (Verbindungseigenschaften) folgende Informationen an:

Feld	Beschreibung
Verbindungsname	JSR-160-kompatibler Server
Benutzer-ID	Benutzername für die Anmeldung an der BI-Plattform
Kennwort	Kennwort für die Anmeldung an der BI-Plattform
Dienst-URL	Bereitstellung der JMX-Endpunkt-URL

9. Klicken Sie auf **Finish** (Fertig stellen).
10. Wählen Sie im Bereich *MBean Key Properties* (MBean-Schlüsseleigenschaften) die Optionen **Domain** (Domäne) und **Type** (Typ) aus.

    Alle MBeans werden im folgenden Textfeld angezeigt.
11. Wählen Sie alle MBeans mit Domäne als Server aus, jeweils eine MBean nach der anderen, sodass die Attribute aufgelistet werden. Wählen Sie ein Schlüsselattribut, wenn mehrere MBeans desselben Typs vorhanden sind. Wenn beispielsweise zwei Instanzen eines Servers ausgeführt werden, kann die PID jeder Instanz ein Schlüsselattribut sein.
12. Wählen Sie einen Server und die Optionen für die JMX-Attributgruppe im Fenster *JMX Agent-Wide Options* (JMX-Agent-Optionen) aus.
13. Wählen Sie im Fenster *Data Source Definition* (Datenquellendefinition) den hinzugefügten Agent aus, und klicken Sie auf **Add to Selected** (Zur Auswahl hinzufügen). Dadurch gelangen Sie zum Anfang des Agent-Erstellungszyklus, und Sie müssen obige Schritte wiederholen, um einen weiteren zu überwachenden Server hinzuzufügen.
14. Nach der Erstellung des Agents muss dieser installiert werden. Weitere Informationen zum Installieren eines Agents finden Sie im Benutzerhandbuch für IBM Tivoli Monitoring Agent ab Abbildungsnummer 154. Dieser

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Abschnitt enthält Informationen zur lokalen Installation des Agents sowie zur Erstellung einer installierbaren Lösung des Agents.

> **Hinweis**
>
> Wenn Sie unter Verwendung des Agent Builders einen Agent für die BI-Plattform erstellen, muss die BI-Plattform auf demselben System installiert sein. Wenn Sie jedoch einen bereits erstellten Agent unter Verwendung seiner Installationsdatei installieren, muss die BI-Plattform-Überwachung nicht installiert sein, da Sie bei der Konfiguration die Details eines beliebigen Systems mit einem JMX-Endpunkt angeben können.

Führen Sie zur Konfiguration eines installierten Agents die folgenden Schritte aus:

1. Öffnen Sie *Manage Tivoli Enterprise Monitoring Services* (Tivoli Enterprise-Überwachungsdienste verwalten) im TEMS-Modus. Der installierte Agent wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf die Agent-Vorlage, und wählen Sie **Configure using defaults** (Konfigurieren mit Standardwerten) aus.
3. Wählen Sie einen Instanznamen aus.

   Der Agent kann mit Hilfe von zwei verschiedenen Protokollen konfiguriert werden: RMI und BOEIIOP.

   So verwenden Sie das RMI-Protokoll:

   Klicken Sie auf **Weiter**. Nehmen Sie keine Änderungen an den Java-Parametern vor.
   Geben Sie Werte für JMX-Anmeldedaten an, z.B. Benutzer-ID, Kennwort und Dienst-URL. Weitere Informationen finden Sie unter *Konfigurationseigenschaften* in den Verwandten Themen.
   Klicken Sie auf **OK**.

   So verwenden Sie das BOEIIOP-Protokoll:

   Kopieren Sie die Dateien `bcm.jar` und `cryptojFIPS.jar` aus dem Ordner `%InstallDir%\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib` in einen Ordner in Ihrem System.
   Kopieren Sie die in der folgenden Tabelle aufgeführten JAR-Dateien in einen anderen Ordner.
   Legen Sie in den Java-Parametern die JVM-Argumente auf `-Djmx.remote.protocol.provider.pkgs = com.businessobjects.sdk.monitoring` und den Speicherort des Ordners `-Djmx.boeiiop.bcm.dir=<` fest, in den Sie die Dateien`bcm.jar` und `cryptojFIPS.jar` kopiert haben.
   Wählen Sie **Weiter**.
   Geben Sie Werte für JMX-Anmeldedaten an, z.B. Benutzer-ID, Kennwort und Dienst-URL. Weitere Informationen finden Sie unter *Konfigurationseigenschaften* in den Verwandten Themen.
   Legen Sie den Wert **`<Jar-Verzeichnisse>`** als Speicherort für den Ordner fest, in den Sie die Liste der JAR-Dateien aus der Tabelle kopiert haben.
   Klicken Sie auf **OK**.

JAR-Dateien
`activation-1.1.jar`
`axiom-api-1.2.5.jar`
`axiom-impl-1.2.5.jar`
`axis2-adb-1.3.jar`
`axis2-kernel-1.3.jar`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

JAR-Dateien
cecore.jar
celib.jar
cesession.jar
commons-logging-1.1.jar
corbaidl.jar
ebus405.jar
log4j.jar
logging.jar
monitoring-plugins.jar
monitoring-sdk.jar
stax-api-1.0.1.jar
wsdl4j-1.6.2.jar
wstx-asl-3.2.1.jar
XmlSchema-1.3.2.jar
TraceLog.jar
ceaspect.jar
aspectjrt.jar

4. Klicken Sie mit der rechten Maustaste auf den Agent, und wählen Sie **Start** im Fenster *Manage Tivoli Enterprise Monitoring Services* (Tivoli Enterprise-Überwachungsdienste verwalten) aus.
5. Öffnen Sie den IBM Tivoli Enterprise Portal Desktop/Browser Client. Im Fenster *Navigator* wird eine Schaltfläche angezeigt.
6. Klicken Sie auf die Schaltfläche **Navigator**.

   Der Agent wird zum Navigator hinzugefügt.

Weitere Informationen

Konfigurationseigenschaften [Seite 678]

20.5.2 Integrieren des Monitorings in SAP Solution Manager

Um das Monitoring in SAP Solution Manager zu integrieren, muss *Wily Introscope* auf Ihrem Rechner installiert sein und in Ihrem System ausgeführt werden. Der SAP Solution Manager muss für die Introscope-Arbeitsstation konfiguriert werden. Führen Sie während der Installation der BI-Plattform folgende Schritte aus:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Geben Sie im Schritt "“Konnektivität mit Introscope Enterprise Manager konfigurieren”" den Hostnamen und die Portdetails an. Es wird ein Introscope Agent unter `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\Wiley` installiert, wenn Sie die BI-Plattform installieren.
2. Starten Sie die Introscope-Arbeitsstation, und klicken Sie auf **New Investigator** (Neuer Investigator). Sie können die Servermetriken und virtuellen Metriken von SAP BusinessObjects im JMX-Bereich des konfigurierten Agenten anzeigen.

> **Hinweis**
>
> Sie können den Introscope (IS) Agent durch Auswahl von **CMC** > **Server** > **Serverknoten** > **Platzhalter** konfigurieren. Hier werden auch Host und Port des IS Enterprise Managers konfiguriert, so dass der IS Agent mit dem Überwachungstool kommunizieren kann. Weitere Informationen finden Sie unter *Verwalten von Servern* in der CMC-Hilfe.
>
> Damit die JMX-Metriken in IS zur Verfügung stehen, stellen Sie sicher, dass sowohl die IS Agent-Dienste als auch der Überwachungsdienst auf der AdaptiveProcessingServer-Instanz vorhanden sind.
>
> Wenn Sie die IS-Instrumentation aktivieren, wird die Code-Instrumentation automatisch aktiviert.

20.6 Cluster-Unterstützung für den Überwachungsserver

Das Überwachungstool unterstützt Clustering, das die Failover-Funktion bereitstellt.

Mit Cluster-Unterstützung ist zu jedem beliebigen Zeitpunkt nur ein Dienst aktiv und alle anderen Dienste sind passiv. Wenn in einer geclusterten Umgebung zwei Überwachungsdienste s1 und s2 vorhanden sind, steht nur einer von beiden zur Verfügung. Sowohl s1 als auch s2 versucht, aktiv zu werden, und wenn einer der beiden Dienste erfolgreich ist, wird der andere Dienst inaktiv oder passiv.

Der passive Dienst prüft regelmäßig die Verfügbarkeit des aktiven Diensts (jede Minute). Falls der aktive Dienst nicht verfügbar ist, wird sofort der passive Dienst aktiviert.

> **Hinweis**
>
> Es wird empfohlen, den Überwachungsdienst auf einer separaten APS-Instanz (Adaptive Processing Server) zu hosten, um Fehler oder Leistungseinbußen des APS zu vermeiden.

20.7 Fehlerbehebung

In diesem Abschnitt werden die einzelnen Lösungsschritte für eine Reihe von Problemen erläutert, die bei der Arbeit mit dem Überwachungstool auftreten können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

20.7.1 Dashboard

Der Überwachungshyperlink wird nicht auf der CMC-Seite angezeigt.

- Überprüfen Sie, ob der Benutzer über entsprechende Zugriffsrechte verfügt.
- Stellen Sie sicher, dass der Benutzer den Gruppen "Überwachungstool-Benutzer" oder "Administrator" oder einer anderen Gruppe, die zu diesen Gruppen gehört, hinzugefügt wurde.

Schlüsselleistungsindikatoren (Key Performance Indicators, KPIs) werden im Überwachungsdashboard nicht angezeigt.

- Überprüfen Sie, ob die erforderlichen Metriken angezeigt werden, nachdem Sie **Servereigenschaften** > **Metriken** ausgewählt haben.
- Stellen Sie sicher, dass der Central Management Server wie erwartet reagiert.

Das Überwachungstool kann nicht gestartet werden.

Laden Sie den neuesten Flash Player herunter, und installieren Sie ihn.

20.7.2 Warnmeldungen

Auf der Seite "Warnmeldungen" können keine Warnmeldungen empfangen werden.

- Prüfen Sie, ob die Option **Meine Warnmeldungen** in den Eigenschaften der Warnungsanwendung ausgewählt ist.
- Stellen Sie sicher, dass Sie über die nötigen Zugriffsrechte für den Empfang von Warnmeldungen verfügen.
- Überprüfen Sie, ob die aktuellen Warnmeldungen im Überwachungsdashboard angezeigt werden.

> **Hinweis**
>
> Sie können ein Crystal-Reports-Dokument an die festgelegte E-Mail-ID senden, um zu testen, ob der SMTP wie erwartet funktioniert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

E-Mail-Benachrichtigungen können nicht empfangen werden

- Prüfen Sie, ob die Option **E-Mail aktivieren** in den Eigenschaften der Warnungsanwendung ausgewählt ist.
- Prüfen Sie, ob die Einstellungen der E-Mail-Adresse zum Empfangen von E-Mail-Warnmeldungen geeignet sind.
- Überprüfen Sie, ob der SMTP-Server funktioniert.
- Stellen Sie sicher, dass die Adaptive-Job-Server-Instanz aktiviert wurde.
- Prüfen Sie die SMTP-Einstellungen im Ziel der Adaptive-Job-Server-Instanz.

20.7.3 Kontrollmodulliste

Für das Kontrollmodul können keine Verlaufsdaten empfangen werden.

- Überprüfen Sie das Abfrageintervall auf der Seite **Eigenschaften** des Überwachungstools.
- Überprüfen Sie die Ablaufverfolgungsdatei im Protokollierungsordner.
- Überprüfen Sie, ob für **Pfad der Trenddatenbank** auf der CMC-Seite **Anwendungen** ein Wert angegeben ist. Stellen Sie bei einer Clusterumgebung sicher, dass der Benutzer über Berechtigungen zum Zugriff auf den freigegebenen Pfad hat. Weitere Informationen finden Sie unter *Konfigurationseigenschaften* in den Verwandten Themen.
- Überprüfen Sie, ob die Systemzeit des Servers und Clients in einer bestimmten Zeitzone identisch ist.

Fehler beim Abrufen der synchronisierten Live-Daten

Überprüfen Sie, ob die Adaptive-Processing-Server-Instanz ausgeführt wird.

Die Registerkarte "Kontrollmodulliste" ist deaktiviert.

- Überprüfen Sie, ob der Überwachungsdienst ausgeführt wird.
- Überprüfen Sie die Protokolle des Überwachungsdiensts auf Fehlermeldungen.
- Überprüfen Sie, ob die Server und ihre Metriken in jConsole angezeigt werden.

Weitere Informationen

Konfigurationseigenschaften [Seite 678]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

20.7.4 Diagnosen

Diagnosen können nicht zeitgesteuert verarbeitet werden

- Überprüfen Sie, ob die Adaptive-Job-Server-Instanz, die den Dienst für die zeitgesteuerte Verarbeitung von Diagnosen hostet, ausgeführt wird.
- Stellen Sie sicher, dass eine für Crystal-Reports-Berichte und Web-Intelligence-Dokumente geeignete Berichts-CUID verwendet wird.
- Stellen Sie sicher, dass der Benutzer Administratorrechte besitzt oder Mitglied der Administratorengruppe ist.
- Überprüfen Sie, ob der Benutzer die erforderlichen Rechte zum Öffnen, Regenerieren und Exportieren von Crystal-Reports-Berichten oder Web-Intelligence-Dokumenten besitzt, die in den entsprechenden Diagnosen verwendet werden.

Der Status der zeitgesteuerten Verarbeitung von Diagnosen ist ""Ausstehend"

- Überprüfen Sie, ob die ProbeSchedulingService-Instanz installiert ist.
- Überprüfen Sie, ob die Adaptive-Job-Server-Instanz, die den Dienst für die zeitgesteuerte Verarbeitung von Diagnosen hostet, ausgeführt wird.

Beim Abrufen der Trenddaten aus der Datenbank ist ein Fehler aufgetreten

Überprüfen Sie, ob die AdaptiveProcessingServer-Instanz ausgeführt wird.

probeRun.bat kann nicht erfolgreich ausgeführt werden

- Überprüfen Sie, ob `java_home` festgelegt ist.
- Überprüfen Sie, ob die richtigen Parameter in die Befehlseingabeaufforderung eingegeben wurden.

> **Hinweis**
>
> Geben Sie **`probeRun.bat -help`** in die Befehlseingabeaufforderung ein, um zu prüfen, ob alle Parameter geeignet sind.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

20.7.5 Metriken

Hostmetriken werden nicht aufgeführt.

- Stellen Sie sicher, dass SAPOSCOL ausgeführt wird.
- Stellen Sie sicher, dass die Option **Hostmetriken aktivieren** auf der Seite **Eigenschaften** des Überwachungstools ausgewählt ist.
- Starten Sie die AdaptiveProcessingServer-Instanz neu, damit die Änderungen in Kraft treten.
- Stellen Sie sicher, dass der **Pfad zu Ihrer Installation der SAPOSCOL-Binärdatei** korrekt angegeben ist.

Beim Abrufen des JMX-Clients ist ein Fehler aufgetreten.

Überprüfen Sie, ob die AdaptiveProcessingServer-Instanz ausgeführt wird.

Der SAPOSCOL-Metrikwert ist auf der Metrikseite 0.

- Stellen Sie sicher, dass SAPOSCOL ausgeführt wird.
- Führen Sie Folgendes auf dem Host aus, auf dem SAPOSCOL installiert ist:
  1. `saposcol -s` zum Überprüfen des Status
  2. `saposcol -m`, um einen Snapshot der von SAPOSCOL erfassten Daten zu erhalten

20.7.6 Diagramm

In Diagrammen werden verschiedene Uhrzeiten für den Live- und den Verlaufsmodus angezeigt.

Stellen Sie sicher, dass die Systemzeit von Server und Client in einer bestimmten Zeitzone identisch ist.

Für ein Clusterszenario werden im Verlaufsmodus keine Diagrammdaten angezeigt.

Stellen Sie sicher, dass alle AdaptiveProcessingServer-Instanzen auf den gleichen Speicherort der Derby-Datenbank zeigen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

21 Auditing

21.1 Übersicht

Das Auditing ermöglicht es Ihnen, einen Datensatz zu wichtigen Ereignissen auf Servern und in Anwendungen beizubehalten und somit einen Überblick darüber zu erhalten, auf welche Informationen zugegriffen wird, wie der Zugriff erfolgt, welche Änderungen vorgenommen werden und wer diese Vorgänge durchführt. Diese Informationen werden in einer Datenbank aufgezeichnet, die als Audit-Datenspeicher (Auditing Data Store, ADS) bezeichnet wird. Sobald sich die Daten im Audit-Datenspeicher befinden, können Sie benutzerdefinierte Berichte nach Ihren Anforderungen entwerfen. Sie können Beispieluniversen und -berichte im SAP Community Network *http://scn.sap.com/* suchen.

Für die Zwecke dieses Kapitels ist ein Auditor ein für die Aufzeichnung oder Speicherung von Informationen zu einem Ereignis verantwortliches System, und ein auditiertes Objekt ist ein für die Durchführung eines auditierbares Ereignisses zuständiges System. Unter bestimmten Umständen kann ein System beide Funktionen durchführen.

Einführung in den Audit

Der Central Management Server (CMS) fungiert als Systemauditor, während die einzelnen Server oder Anwendungen, die ein Audit-Ereignis auslösen, als auditiertes Objekt fungieren. Wenn ein auditiertes Ereignis ausgelöst wird, generiert das auditierte Objekt einen Datensatz und speichert ihn in einer lokalen temporären Datei. Der CMS kommuniziert in regelmäßigen Abständen mit den auditierten Objekten, um diese Datensätze anzufordern, und schreibt die Daten in den ADS.

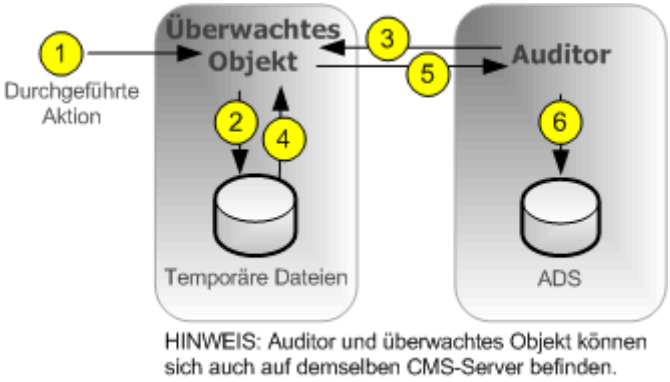
Außerdem steuert der CMS die Synchronisierung von Audit-Ereignissen, die auf unterschiedlichen Rechnern auftreten. Alle auditierten Objekte enthalten einen Zeitstempel für die aufgezeichneten Audit-Ereignisse. Um sicherzustellen, dass die Zeitstempel von Ereignissen auf verschiedenen Servern konsistent sind, sendet der CMS seine Systemzeit regelmäßig an die auditierten Objekte. Das auditierte Objekt vergleicht diese Zeit dann mit den internen Zeitgebern. Bei Unterschieden korrigiert es die für folgende Audit-Ereignisse aufgezeichnete Zeit.

Je nach Typ des auditierten Objekts verwendet das System einen der folgenden Workflows, um die Ereignisse aufzuzeichnen.

Server-Audit

Der CMS kann bei vom Server generierten Ereignissen als auditiertes Objekt und als Auditor fungieren.

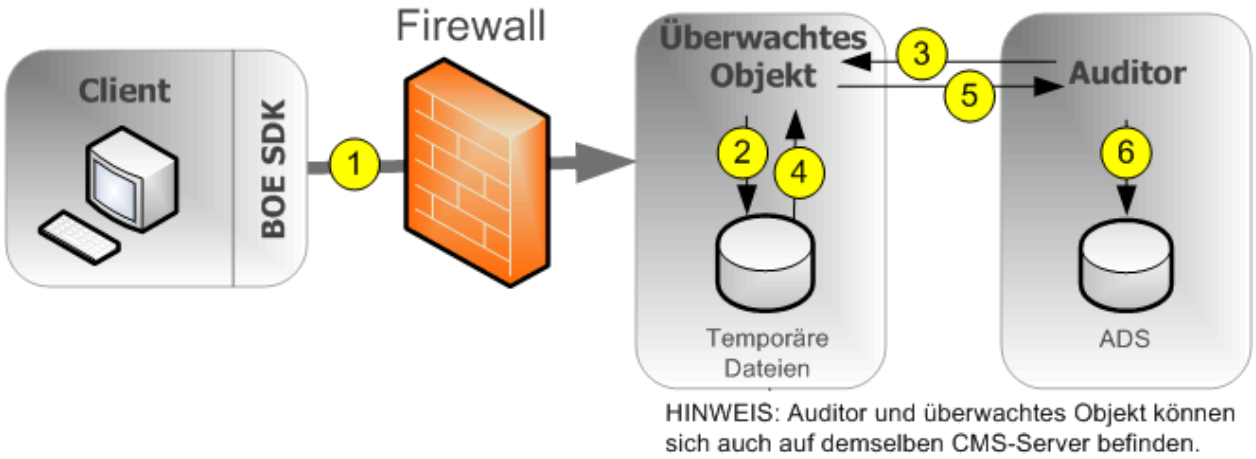
© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.



1. Ein auditierbares Ereignis wird vom Server ausgeführt.
2. Das auditierte Objekt schreibt Ereignisse in eine temporäre Datei. Die Schritte 1 und 2 können vor Schritt 3 mehrfach auftreten.
3. Der Auditor ruft das auditierte Objekt regelmäßig ab und fordert einen Stapel von Audit-Ereignissen an.
4. Das auditierte Objekt ruft die Ereignisse aus den temporären Dateien ab.
5. Das auditierte Objekt überträgt die Ereignisse an den Auditor.
6. Der Auditor schreibt die Ereignisse in den ADS und fordert das auditierte Objekt auf, die Ereignisse aus den temporären Dateien zu löschen.

Auditierung der Clientanmeldung für Clients, die die Verbindung über CORBA herstellen

Dazu gehören Anwendungen wie SAP BusinessObjects Web Intelligence.



1. Der Client stellt eine Verbindung zum CMS her, der als auditiertes Objekt fungiert. Der Client stellt seine IP-Adresse und den Computernamen bereit, die vom auditierten Objekt überprüft werden.

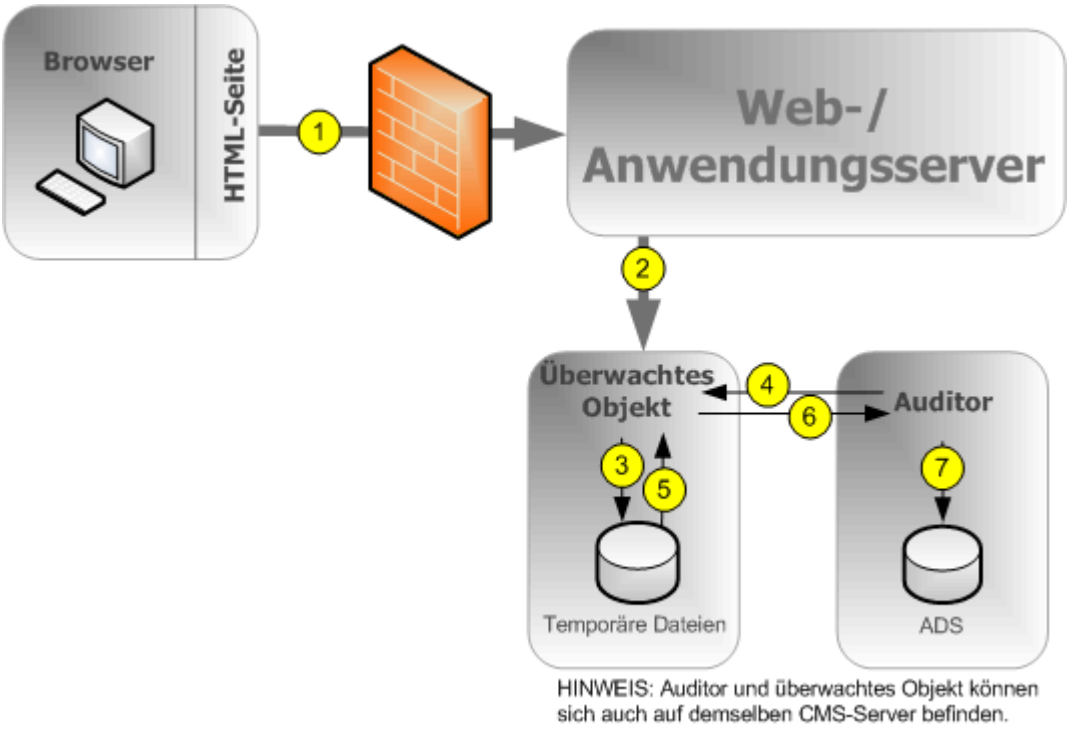
> **Hinweis**
>
> Ein Port sollte in der Firewall zwischen dem Client und dem CMS geöffnet sein. Weitere Informationen über Firewalls finden Sie in dem Kapitel zur Sicherheit im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Das auditierte Objekt schreibt Ereignisse in eine temporäre Datei. Die Schritte 1 und 2 können vor Schritt 3 mehrfach auftreten.
3. Der Auditor ruft das auditierte Objekt regelmäßig ab und fordert einen Stapel von Audit-Ereignissen an.
4. Das auditierte Objekt ruft die Ereignisse aus den temporären Dateien ab.
5. Das auditierte Objekt überträgt die Ereignisse an den Auditor.
6. Der Auditor schreibt die Ereignisse in den ADS und fordert das auditierte Objekt auf, die Ereignisse aus den temporären Dateien zu löschen.

Auditierung der Clientanmeldung für Clients, die die Verbindung über HTTP herstellen

Dazu gehören Online-Anwendungen wie das BI-Launchpad, die Central Management Console, SAP BusinessObjects Web Intelligence usw.

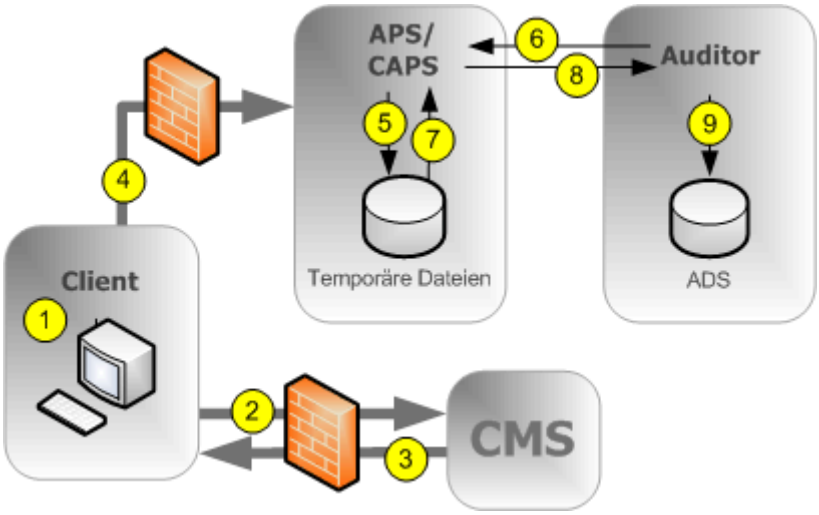


1. Der Browser stellt eine Verbindung zum Webanwendungsserver her, und Anmeldedaten werden an den Webanwendungsserver gesendet.
2. Die Anmeldeanforderung wird vom BI-Plattform-SDK zusammen mit der IP-Adresse und dem Namen des Browserrechners an das auditierte Objekt (CMS) gesendet.
3. Das auditierte Objekt schreibt Ereignisse in eine temporäre Datei. Die Schritte 1 bis 3 können vor Schritt 4 mehrfach auftreten.
4. Der Auditor ruft das auditierte Objekt regelmäßig ab und fordert einen Stapel von Audit-Ereignissen an.
5. Das auditierte Objekt ruft die Ereignisse aus den temporären Dateien ab.
6. Das auditierte Objekt überträgt die Ereignisse an den Auditor.
7. Der Auditor schreibt die Ereignisse in den ADS und fordert das auditierte Objekt auf, die Ereignisse aus den temporären Dateien zu löschen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Auditierung der Nichtanmeldung für Clients, die die Verbindung über CORBA herstellen

Dieser Workflow gilt für das Auditing von Ereignissen von SAP BusinessObjects Web Intelligence beim Herstellen einer Verbindung über CORBA.



1. Der Benutzer führt einen Vorgang aus, der auditiert werden kann.
2. Der Client stellt eine Verbindung zum CMS her, um zu überprüfen, ob der Vorgang für die Auditierung konfiguriert ist.
3. Wenn die Aktion so eingestellt ist, dass sie auditiert werden muss, leitet der CMS diese Informationen an den Client weiter.
4. Der Client sendet die Ereignisinformationen an den Proxydienst für den Client-Audit (Client Auditing Proxy Service, CAPS), der auf einem Adaptive Processing Server gehostet wird.

   Hinweis

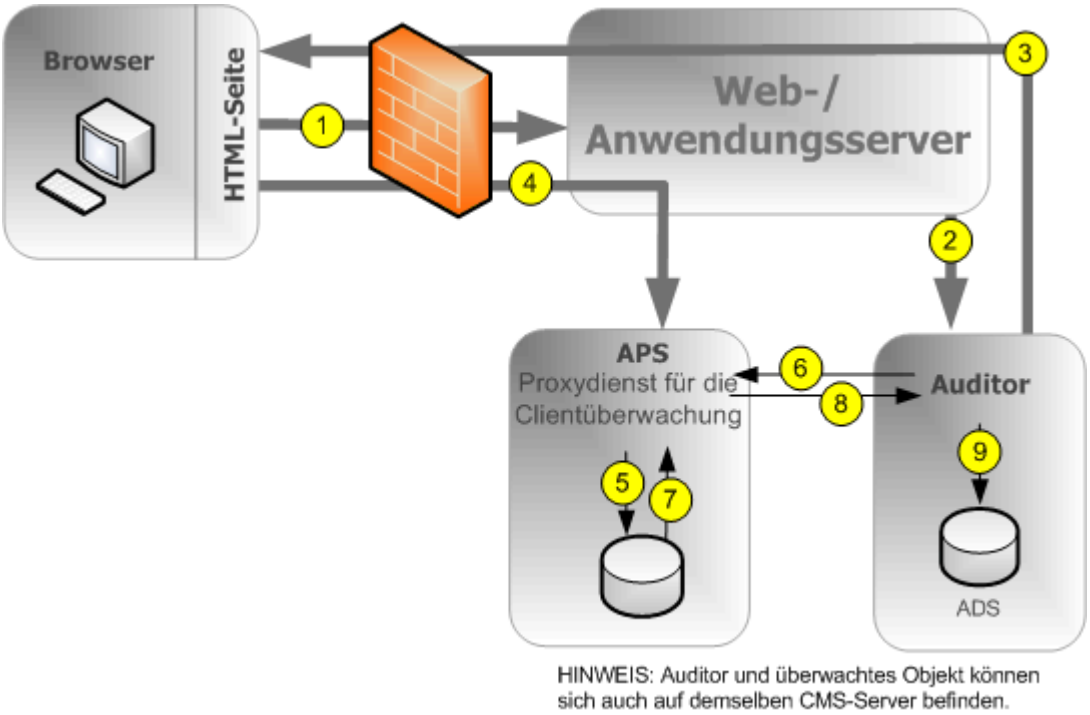
   Ein Port in der Firewall sollte zwischen jedem Client und jedem Adaptive Processing Server, der einen CAPS hostet, und den einzelnen Clients und dem CMS geöffnet sein. Weitere Informationen über Firewalls finden Sie in dem Kapitel zur Sicherheit im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.

5. Der CAPS schreibt Ereignisse in eine temporäre Datei. Die Schritte 1 bis 5 können vor Schritt 6 mehrfach auftreten.
6. Der Auditor ruft den CAPS regelmäßig ab und fordert einen Stapel von Audit-Ereignissen an.
7. Das CAPS ruft die Ereignisse aus den temporären Dateien ab.
8. Der CAPS sendet die Ereignisinformationen an den Auditor.
9. Der Auditor schreibt die Ereignisse in den ADS und fordert den CAPS auf, die Ereignisse aus den temporären Dateien zu löschen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Auditierung der Nichtanmeldung für Clients, die die Verbindung über HTTP herstellen

Dieser Workflow gilt für das Auditing von Ereignissen von SAP BusinessObjects Web Intelligence (außer für Anmeldeereignisse) bei Herstellung der Verbindung über HTTP.



1. Der Benutzer initiiert ein Ereignis, das u.U. auditiert werden kann. Die Clientanwendung stellt eine Verbindung zum Webanwendungsserver her.
2. Die Webanwendung prüft, ob das Ereignis für den Audit konfiguriert wurde.

   > **Hinweis**
   >
   > Obwohl im Diagramm eine Verbindung zum Auditor-CMS hergestellt wird, kann jeder beliebige CMS im Cluster kontaktiert werden, um diese Informationen abzurufen.

3. Der CMS gibt die Konfigurationsinformationen für den Audit an den Webanwendungsserver zurück, der diese Informationen wiederum an die Clientanwendung weitergibt.
4. Wenn das Ereignis für den Audit konfiguriert ist, sendet der Client die Ereignisinformationen and den Webanwendungsserver, der sie an den Proxydienst für den Client-Audit (CAPS) übergibt, der auf einem Adaptive Processing Server (APS) gehostet wird.
5. Der CAPS schreibt Ereignisse in eine temporäre Datei. Die Schritte 1 bis 5 können vor Schritt 6 mehrfach auftreten.
6. Der Auditor ruft den CAPS regelmäßig ab und fordert einen Stapel von Audit-Ereignissen an.
7. Das CAPS ruft die Ereignisse aus den temporären Dateien ab.
8. Der CAPS sendet die Ereignisinformationen an den Auditor.
9. Der Auditor schreibt die Ereignisse in den ADS und fordert den CAPS auf, die Ereignisse aus den temporären Dateien zu löschen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Clients, die das Auditing unterstützen

Die folgenden Clientanwendungen unterstützen das Auditing:

- Central Management Console (CMC)
- BI-Launchpad
- Open Document
- Analysis
- Live Office Web Services-Provider
- Web-Intelligence-Rich-Client
- Dashboards und Presentation Design
- Analysis-Anwendungen
- SAP BusinessObjects Design Studio, Version 1.3 und höher

> **Hinweis**
>
> Mindestens eine CAPS-Instanz muss ausgeführt werden, damit Audit-Ereignisse der oben aufgeführten Clients erfasst werden können.

Nicht aufgeführte Clients generieren Ereignisse nicht direkt, aber einige von den Servern als Ergebnis von Clientanwendungsvorgängen generierte Aktionen können auditiert werden.

Audit-Konsistenz

In den meisten Fällen, in denen das Audit ordnungsgemäß installiert und konfiguriert ist und gesicherte und einwandfreie Versionen aller Clientanwendungen verwendet werden, werden alle angegebenen Systemereignisse vom Audit ordnungsgemäß und konsistent aufgezeichnet. Sie sollten allerdings bedenken, dass sich bestimmte System- und Umgebungsbedingungen negativ auf das Audit auswirken können.

Zwischen dem Auftreten eines Ereignisses und der endgültigen Übertragung in den ADS entsteht immer eine Verzögerung. Bedingungen wie die Nichtverfügbarkeit des CMS oder der Audit-Datenbank oder der Verlust der Netzwerkkonnektivität können diese Verzögerungen vergrößern.

Als Systemadministrator sollten Sie die folgenden Bedingungen vermeiden, die zu unvollständigen Audit-Datensätzen führen können:

- Ein Laufwerk, auf dem Audit-Daten gespeichert sind, erreicht die Höchstkapazität. Sie sollten über viel Festplattenspeicherplatz für die temporären Dateien der Audit-Datenbank und des auditierten Objekts verfügen.
- Ein Server für auditierte Objekte wird unsachgemäß aus dem Netzwerk entfernt, bevor alle Audit-Ereignisse übertragen werden können. Stellen Sie sicher, dass nach dem Entfernen eines Servers aus dem Netzwerk genügend Zeit für die Übertragung der Audit-Ereignisse an die Audit-Datenbank eingeplant wird
- Löschung oder Änderung der temporären Dateien des auditierten Objekts.
- Hardware- oder Festplattenfehler.
- Ein Hostrechner für auditierte Objekte bzw. ein Auditor-Hostrechner wird physisch zerstört.

Darüber hinaus können einige Bedingungen verhindern, dass Audit-Ereignisse vom CMS-Auditor empfangen werden. Dazu gehören folgende Umstände:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Benutzer mit älteren Clientversionen.
- Die Übertragung von Audit-Informationen wird u.U. durch falsch konfigurierte Firewalls blockiert.

> **Hinweis**
>
> Von der Clientanwendung erzeugte Ereignisse enthalten Informationen, die von der Clientseite gesendet wurden, d.h. also außerhalb des vertrauenswürdigen Bereichs des Systems. Daher kann sind die Informationen unter bestimmten Umständen eventuell nicht so zuverlässig wie die von den Systemservern aufgezeichneten Informationen.

> **Hinweis**
>
> Wenn Sie einen Server aus Ihrer Implementierung entfernen möchten, sollten Sie ihn zunächst deaktivieren, aber weiterhin ausführen und mit dem Netzwerk verbunden lassen, bis alle Ereignisse in den temporären Dateien in die Audit-Datenbank übertragen werden konnten. In der Servermetrik *Aktuelle Anzahl der Audit-Ereignisse in der Warteschlange* wird angezeigt, wie viele Audit-Ereignisse auf die Übertragung warten. Wenn diese Metrik null erreicht, können Sie den Server stoppen. Der Speicherort der temporären Dateien wird durch den Platzhalter `%DefaultAuditingDir%` für diesen Knoten definiert. Weitere Informationen über Platzhalter finden Sie im Kapitel "Serververwaltung".

> **Hinweis**
>
> Wenn Sie den Client-Audit verwenden, sollten Sie einen dedizierten Adaptive Processing Server für den Proxydienst für den Client-Audit erstellen. Dies gewährleistet die beste Systemleistung. Zum Erhöhen der Fehlertoleranz des Systems kann es sinnvoll sein, den CAPS auf mehrere APS auszuführen.

Verwandte Links

Server- und Knotenplatzhalter [Seite 1012]

21.2 Seite CMC-Auditing

Die Seite *Auditing* in der CMC verfügt über folgende Bereiche:

- *Statusübersicht*
- *Ereignisse festlegen*
- *Ereignisdetails festlegen*
- *Konfiguration*

21.2.1 Auditing-Status

In der *Statusübersicht* wird ein Satz von Metriken angezeigt, mit deren Hilfe Sie die Audit-Konfiguration optimieren können und die Sie vor allen Problemen warnen, die die Integrität der Audit-Daten beeinträchtigen

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

könnten. Die Statusübersicht befindet sich im oberen Bereich der Seite *Auditing* in der Central Management Console.

Unter folgenden Umständen werden in der Übersicht auch Warnungen angezeigt:

- Die Verbindung zur Datenbank des Audit-Datenspeichers ist nicht verfügbar.
- Da kein laufender oder aktivierter Client Auditing Proxy Service vorhanden ist, können Client-Ereignisse nicht gesammelt werden.
- In einem auditierten Bereich sind Ereignisse vorhanden, die nicht abgerufen werden konnten (der/die betroffene/n Server wird ermittelt). Dies zeigt in der Regel an, dass ein Server nicht ordnungsgemäß gestoppt oder heruntergefahren wurde und in dessen temporären Dateien noch Ereignisse vorhanden sind.

> **Hinweis**
>
> Die Statusübersichtsmetriken sind grün, gelb oder rot markiert, um den Status der Audit-Funktion anzugeben.

Metriken des Auditing-Status

Metrik	Details
ADS zuletzt aktualisiert am	Datum und Uhrzeit, wann der Auditor-CMS das Abrufen der Audit-Ereignisse der auditierten Objekte zuletzt abgeschlossen hat.
Auslastung des Audit-Threads	Der Prozentsatz des Abrufzyklus, den der Auditor-CMS mit dem Abrufen der Daten von auditierten Objekten verbringt. Die restliche Zeit ist die Ruhezeit zwischen den Abrufzyklen. Erreicht dieser Wert 100 %, wird diese Zahl gelb angezeigt, .d.h. der Auditor ruft immer noch Daten von den auditierten Objekten ab, wenn der nächste Abrufzyklus gestartet werden soll. Dies kann zu Verzögerungen des Empfangs von Ereignissen durch den ADS führen. Wenn dies oft oder ständig geschieht, sollten Sie entweder Ihre Implementierung aktualisieren, damit der ADS Daten mit einer höheren Datenrate empfangen kann (z. B. durch schnellere Netzwerkverbindungen oder leistungsstärkere Datenbankhardware) oder die Anzahl der von Ihrem System verfolgten Audit-Ereignisse verringern.
Dauer des letzten Abrufzyklus (Sekunden)	Die Dauer des letzten Abrufzyklus in Sekunden. Dieser Wert zeigt die maximale Verzögerung für Ereignisdaten bis zum Eingang beim Audit-Datenspeicher während des vorherigen Abrufzyklus an. • Liegt dieser Wert unter 20 Minuten (1200 Sekunden), wird die Zahl auf einem grünen Hintergrund angezeigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Details
	• Liegt dieser Wert zwischen 20 Minuten und 2 Stunden (7200 Sekunden), wird die Zahl auf einem gelben Hintergrund angezeigt. • Übersteigt der Wert 2 Stunden, wird er auf einem roten Hintergrund angezeigt. Wenn dieser Zustand anhält und Sie die Verzögerung für zu lang halten, sollten Sie entweder Ihre Implementierung aktualisieren, damit der Audit-Datenspeicher Daten mit einer höheren Datenrate empfangen kann (z. B. durch schnellere Netzwerkverbindungen oder leistungsstärkere Datenbankhardware) oder die Anzahl der von Ihrem System verfolgten Audit-Ereignisse verringern.
CMS-Auditor	Der Name des CMS, der aktuell als Auditor fungiert.
ADS-Datenbank-Verbindungsname	Der Name der Datenbankverbindung, die aktuell vom Auditor-CMS verwendet wird, um eine Verbindung zum Audit-Datenspeicher (ADS) herzustellen. Bei SQL-Anywhere-, SQL-Server- und SAP-HANA-Servern ist dies der Name der ODBC-Verbindung. Bei anderen Datenbanktypen ist es der Datenbankname und Verbindungsport, gefolgt vom Servernamen.
ADS-Datenbank-Benutzername	Der Benutzername, den der Auditor-CMS verwendet, um sich am Audit-Datenspeicher anzumelden.

21.2.2 Konfigurieren von Audit-Ereignissen

Auf der Seite "Auditing" der CMC können Sie das Auditing aktivieren und die Ereignisse auswählen, die systemweit auditiert werden sollen.

Wenn bestimmte Ereignisse oder Ereignisdetails für Sie nicht von Interesse sind, wählen Sie sie nicht aus. Auf diese Weise können Sie auch die Systemleistung verbessern.

> **Hinweis**
>
> Wenn Sie beim Installieren der BI-Plattform keine ADS-Verbindung konfiguriert haben, müssen Sie eine Verbindung zur Datenbank einrichten, bevor Sie die Audit-Ereignisse konfigurieren. Ohne eine Verbindung werden weiterhin Ereignisse gesammelt, die jedoch nach dem Herstellen der Verbindung in den ADS geschrieben werden. Um das Auditing zu deaktivieren, sollte die Ebene ausgeschaltet werden. Siehe *Konfigurationseinstellungen des Audit-Datenspeichers (ADS).*

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

21.2.2.1 Konfigurieren von Audit-Ereignissen

1. Wählen Sie in der Central Management Console die Registerkarte **Auditing**.
   Die Seite **Auditing** wird angezeigt.
2. Verschieben Sie den Schieber **Ereignisse einstellen** zu der gewünschten Ebene.

   Die folgende Tabelle enthält die unterschiedlichen Einstellungen des Schiebereglers und die auf den einzelnen Ebenen erfassten Ereignisse.

Audit-Ebene	Erfasste Ereignisse
Deaktiviert	Keine
Minimal	○ Anmelden ○ Abmelden ○ Änderung von Rechten ○ Benutzerdefinierte Zugriffsberechtigung geändert ○ Audit-Änderung
Standard	**Minimal**-Ereignisse plus: ○ Anzeigen ○ Regenerieren ○ Eingabeaufforderung ○ Erstellen ○ Löschen ○ Ändern ○ Speichern ○ Suchen ○ Bearbeiten ○ Ausführen ○ Bereitstellen
Vollständig	**Minimal**- und **Standard**-Ereignisse plus: ○ Auslösen ○ Drill außerhalb des Bereichs ○ Seite abgerufen ○ Konfiguration der Hochstufverwaltung ○ Rollback ○ Zu VMS hinzufügen ○ Aus VMS abrufen ○ In VMS einchecken ○ Aus VMS einchecken ○ Aus VMS exportieren ○ In VMS sperren ○ Sperrung in VMS aufheben ○ VMS löschen ○ Cube-Verbindung ○ MDAS-Sitzung

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Audit-Ebene	Erfasste Ereignisse
	Hinweis Es gibt möglicherweise mehr Ereignisse, wenn Addons installiert sind.
Benutzerdefiniert	Sie wählen einen benutzerdefinierten Satz von Ereignissen aus.

3. Wenn Sie **Benutzerdefiniert** ausgewählt haben, klicken Sie in der Liste unter dem Schieber **Ereignisse einstellen** auf die Ereignisse, die Sie erfassen möchten.
4. Klicken Sie unter *Ereignisdetails festlegen* auf die optionalen Details, die Sie mit den Ereignissen aufzeichnen möchten. Wenn Sie weniger Details aufzeichnen, erhöht sich die Systemleistung.

Information	Beschreibung
Abfrage	Wenn eingestellt, wird das Ereignisdetail *Abfrage* (Detail-ID 25) für jedes Ereignis aufgezeichnet, das eine Datenbank abfragt.
Ordnerpfaddetails	Wenn eingestellt, werden die folgenden Details erfasst: ○ *Objektordnerpfad (Detail-ID 71)* ○ *Name des obersten Ordners (Detail-ID 72)* ○ *Pfad zum Container-Ordner (Detail-ID 64)*
Details zu Rechten	Wenn eingestellt, werden die folgenden Details erfasst: ○ *Recht hinzugefügt (Detail-ID 55)* ○ *Recht entfernt (Detail-ID 56)* ○ *Recht geändert (Detail-ID 57)*
Benutzergruppendetails	Wenn eingestellt, werden die folgenden Details erfasst: ○ *Benutzergruppenname (Detail-ID 16)* ○ *Benutzergruppen-ID (Detail-ID 15)*
Eigenschaftenwertdetails	Wenn eingestellt, wird das *Eigenschaftenwert*-Ereignisdetail (Detail-ID 29) erfasst, wenn die Eigenschaften eines Objekts aktualisiert werden. Dies wird nur für CMC-, BI-Launchpad- oder SharePoint-Ereignisse erzeugt.

5. Klicken Sie auf **Speichern**.

Hinweis

Beim Client-Auditing kann es bis zu zwei Minuten nach der Änderung dauern, bis das System beginnt, Daten für neue Ereignisse aufzuzeichnen. Berücksichtigen Sie diese Verzögerung, wenn Sie Änderungen im System implementieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

21.2.3 Konfigurationseinstellungen des Audit-Datenspeichers (ADS)

Wenn Sie beim Installieren der BI-Plattform keine Audit-Datenbank eingerichtet haben, oder Sie den Datenbankspeicherort oder Datenbankeinstellungen ändern möchten, können Sie die Verbindung zum ADS mit den folgenden Schritten konfigurieren.

Hier können Sie auch angeben, wie lange die Audit-Ereignisse in der Datenbank aufbewahrt werden.

Wenn Sie einen Upgrade von einer früheren Version von SAP BusinessObjects Enterprise XI 3.x durchgeführt und Version 3.x von Business Objects Metadata Manager (BOMM) installiert haben, sollten Sie den ADS so konfigurieren, dass er die gleiche Datenbank oder den gleichen Tabellenbereich wie der BOMM verwendet.

> **Hinweis**
>
> Wenn Sie eine vorhandene DB2 9.7 Workgroup als Audit-Datenbank verwenden, stellen Sie sicher, dass das Datenbankkonto für Seitengrößen von mehr als 8 kB konfiguriert ist.

21.2.3.1 Konfigurieren der Datenbankeinstellungen des Audit-Datenspeichers (ADS)

1. Wählen Sie in der Central Management Console die Registerkarte **Auditing**.
2. Wählen Sie im Bereich *Konfiguration* unter der Überschrift *ADS-Datenbank* den Datenbanktyp aus, den Sie für Ihre Audit-Daten eingerichtet haben.
3. Geben Sie im Feld *Verbindungsname* den Namen der Verbindung ein, die Sie für die Audit-Datenbank konfiguriert haben.

Datenbanktyp	Verbindungsname
IBM DB2	Dienstname
Microsoft SQL Server	ODBC DSN
MySQL	`<Serverhostname>,<Port>,<Datenbankname>`
Oracle	TNS-Dienstname
SAP HANA	ODBC DSN
SAP MaxDB	`<Serverhostname>,<Port>,<Datenbankname>`
Sybase Adaptive Server Enterprise	Dienstname
Sybase SQL Anywhere	ODBC DSN

   a) Wenn Sie eine Microsoft-SQL-Datenbank mit Windows-Authentifizierung verwenden, aktivieren Sie die Option **Windows-Authentifizierung**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Geben Sie in die Felder **Benutzername** und **Kennwort** den Benutzernamen und das Kennwort ein, das der Auditor-CMS zum Anmelden bei der Datenbank verwenden soll.

   Wenn IBM DB2 von der BI-Plattform als Standarddatenbank installiert wurde, lassen Sie die Felder **Benutzername** und **Kennwort** leer.
5. Geben Sie im Feld **Ereignisse älter als x Tage löschen** die Anzahl der Tage ein, für die die Informationen in der Datenbank bleiben sollen. (Mindestwert 1, Höchstwert 109.500.)

   > **Achtung**
   >
   > Daten, die älter sind als die hier festgelegte Anzahl von Tagen, werden dauerhaft aus dem Audit-Datenspeicher gelöscht und können nicht wiederhergestellt werden. Wenn Sie Datensätze langfristig aufbewahren möchten, sollten Sie die Möglichkeit in Betracht ziehen, Datensätze periodisch in eine Archivdatenbank zu verschieben.
6. Wenn Sie das Auditor-CMS im Fall eines Abbruchs der Datenbankverbindung manuell wieder mit der Datenbank verbinden möchten, deaktivieren Sie die Option **Verbindung mit Audit-Datenspeicher automatisch erneut herstellen**.

   > **Hinweis**
   >
   > Ist diese Option nicht ausgewählt, müssen Sie die Verbindung zum Audit-Datenspeicher manuell wiederherstellen, wenn die Verbindung abbricht. Dies können Sie durch einen Neustart des CMS oder Aktivieren von **Verbindung mit Audit-Datenspeicher automatisch erneut herstellen** tun. Ereignisse werden aufgezeichnet und in temporären Dateien gespeichert, bis der Audit-Datenspeicher wieder verbunden ist.
7. Klicken Sie auf **Speichern**.
8. Starten Sie alle CMS im Cluster neu.

   > **Hinweis**
   >
   > In der *Statusübersicht* oben auf der Seite werden die aktuellen ADS-Werte angezeigt, die sich von den Werten im Abschnitt *ADS-Datenbank* unterscheiden können, bis die CMS neu gestartet wurden.

21.3 Audit-Ereignisse

Die folgende Tabelle zeigt alle Audit-Ereignisse im System und enthält eine kurze Beschreibung für jedes Ereignis. Darauf folgt eine Liste der Diensttypen, die die Ereignisse erstellen.

Ereignis	Beschreibung sowie Server und Clients, die den Ereignistyp generieren
Audit-Änderung	Die Audit-Einstellungen des Systems werden geändert. • Central Management Service
Erstellen	Dem System wird ein neues Objekt hinzugefügt. • Central Management Service

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignis	Beschreibung sowie Server und Clients, die den Ereignistyp generieren
	• Dienst zum Anzeigen und Ändern von Crystal-Reports-Berichten • Desktop Intelligence • Information Engine-Dienst • Lifecycle-Management • Web Intelligence • Gemeinsamer Web-Intelligence-Dienst • Web-Intelligence-Kerndienst • Web-Intelligence-Verarbeitungsdienst
Cube-Verbindung	Ein OLAP-Cube-Verbindungsvorgang wird durchgeführt. • Multi-Dimensional Analysis Service • Analysis-Anwendungen
Benutzerdefinierte Zugriffsberechtigung geändert	Informationen über Rechte werden geändert. • Central Management Service
Löschen	Ein Objekt wird aus dem System entfernt. • Central Management Service • Lifecycle-Management-Dienst
Bereitstellen	Ein Objekt wird an ein Ziel gesendet/bereitgestellt. • Dienst für die zeitgesteuerte Verarbeitung von Authentifizierungsaktualisierungen • Central Management Service • Crystal Reports für Enterprise-Zeitsteuerungsdienst • Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-Berichten • Desktop Intelligence • Dienst für die zeitgesteuerte Verarbeitung der Zielbereitstellung • Dienst zur zeitgesteuerten Verarbeitung der Plattformsuche • Dienst für die zeitgesteuerte Verarbeitung von Diagnosen • Dienst zur zeitgesteuerten Verarbeitung von Programmen • Dienst zur zeitgesteuerten Verarbeitung von Sicherheitsabfragen • Dienst für die zeitgesteuerte Verarbeitung des Benutzer- und Gruppenimports • Web-Intelligence-Dienst für zeitgesteuerte Verarbeitung und Veröffentlichung
Drill außerhalb des Bereichs	Ein Benutzer eines Web-Intelligence-Dokuments hat einen Drill auf eine Detailebene außerhalb der vorab geladenen Daten des Berichts ausgeführt. • Web Intelligence • Web-Intelligence-Verarbeitungsdienst

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignis	Beschreibung sowie Server und Clients, die den Ereignistyp generieren
	• Gemeinsame Web-Intelligence-Dienste • Web-Intelligence-Kerndienste • Information-Engine-Dienst
Bearbeiten	Der Inhalt eines Objekts wird geändert. • BI-Arbeitsbereichsanwendung • Desktop Intelligence • Information-Engine-Dienst • Web Intelligence • Gemeinsamer Web-Intelligence-Dienst • Web-Intelligence-Kerndienst • Web-Intelligence-Verarbeitungsdienst
LCM-Konfiguration	Die Konfigurationsdetails der LifeCycle-Management-Console (LCM) werden geändert. • Lifecycle-Management
Anmelden	Ein Benutzer meldet sich am System an. • Central Management Service
Abmelden	Ein Benutzer meldet sich vom System ab. • Central Management Service
Ändern	Die Dateieigenschaften eines Objekts werden geändert. • Web Intelligence • Lifecycle-Management • Central Management Service
MDAS-Sitzung	Ein Multi-Dimensional Analysis Service-Vorgang wird durchgeführt. • Multi-Dimensional Analysis Service
Seite abgerufen	Ein SAP BusinessObjects Web Intelligence-Client ruft zusätzliche Informationen vom Repository ab. • Web-Intelligence-Verarbeitungsdienst • Gemeinsame Web-Intelligence-Dienste • Web-Intelligence-Kerndienste • Information-Engine-Dienst
Eingabeaufforderung	Für eine Objekteingabeaufforderung werden Informationen eingegeben. • Crystal-Reports-Cache-Dienst • Crystal Reports für Enterprise-Zeitsteuerungsdienst • Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-Berichten • Dashboard-Cache-Dienst • Desktop Intelligence • Information-Engine-Dienst • Live Office

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignis	Beschreibung sowie Server und Clients, die den Ereignistyp generieren
	• Web Intelligence • Gemeinsamer Web-Intelligence-Dienst • Web-Intelligence-Kerndienst • Web-Intelligence-Verarbeitungsdienst
Regenerieren	Die Daten in einem Objekt werden auf Anforderung des Benutzers von der Datenbank aktualisiert. • Crystal-Reports-Cache-Dienst • Crystal Reports für Enterprise-Zeitsteuerungsdienst • Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-Berichten • Dashboard-Cache-Dienst • Desktop Intelligence • Information-Engine-Dienst • Live Office • Web Intelligence • Gemeinsamer Web-Intelligence-Dienst • Web-Intelligence-Kerndienst • Web-Intelligence-Verarbeitungsdienst
Abrufen	Ein Objekt wird vom Repository abgerufen. • Central Management Service • Desktop Intelligence
Änderung von Rechten	Die Sicherheitsinformationen werden für einen Benutzer, eine Gruppe oder ein Objekt geändert. • Central Management Service
Rollback	Der LifeCycle Manager wird zum Wiederherstellen einer früheren Version eines Objekts verwendet. • Lifecycle-Management
Ausführen	Ein Auftrag wird ausgeführt. • Dienst für die zeitgesteuerte Verarbeitung von Authentifizierungsaktualisierungen • Crystal Reports für Enterprise-Zeitsteuerungsdienst • Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-Berichten • Desktop Intelligence • Dienst für die zeitgesteuerte Verarbeitung der Zielbereitstellung • Dienst zur zeitgesteuerten Verarbeitung von LCM • Lifecycle-Management • Dienst zur zeitgesteuerten Verarbeitung der Plattformsuche • Dienst für die zeitgesteuerte Verarbeitung von Diagnosen • Dienst zur zeitgesteuerten Verarbeitung von Programmen

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignis	Beschreibung sowie Server und Clients, die den Ereignistyp generieren
	• Dienst zur zeitgesteuerten Verarbeitung von Veröffentlichungen • Replikationsdienst • Dienst zur zeitgesteuerten Verarbeitung von Sicherheitsabfragen • Dienst für die zeitgesteuerte Verarbeitung des Benutzer- und Gruppenimports • Dienst zur zeitgesteuerten Verarbeitung für den grafischen Vergleich • Web-Intelligence-Dienst für zeitgesteuerte Verarbeitung und Veröffentlichung
Speichern	Ein Objekt wird gespeichert, nachdem es aktualisiert oder geändert wurde. • Analysis, Edition für OLAP • Crystal-Reports-Cache-Dienst • Crystal Reports für Enterprise-Zeitsteuerungsdienst • Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-Berichten • Dienst zum Anzeigen und Ändern von Crystal-Reports-Berichten • Dashboards • Desktop Intelligence • Information-Engine-Dienst • Lifecycle-Management • Multi-Dimensional Analysis Service • SAP BusinessObjects Mobile • Web Intelligence • Gemeinsamer Web-Intelligence-Dienst • Web-Intelligence-Kerndienst • Web-Intelligence-Verarbeitungsdienst
Suchen	Eine Suche wird durchgeführt. • Suchdienst • Explorer • Lifecycle-Management
Auslösen	Ein Dateiereignis wird ausgelöst. • Ereignisdienst • Central Management Service
Anzeigen	Ein Objekt wird angezeigt. • Analysis-Anwendungen • Analysis, Edition für OLAP • BI-Launchpad • BI-Arbeitsbereichsanwendung • CMC • Crystal-Reports-Cache-Dienst

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignis	Beschreibung sowie Server und Clients, die den Ereignistyp generieren
	• Dienst zum Anzeigen und Ändern von Crystal-Reports-Berichten • Dashboard-Cache-Dienst • Desktop Intelligence • Information-Engine-Dienst • Open Document • SAP BusinessObjects Mobile • Web Intelligence • Gemeinsamer Web-Intelligence-Dienst • Web-Intelligence-Kerndienst • Web-Intelligence-Verarbeitungsdienst
Zu VMS hinzufügen	Dem LCM-Versionsverwaltungssystem wird ein Objekt hinzugefügt. • Lifecycle-Management
In VMS einchecken	Es wird ein Objekt in das LCM-Versionsverwaltungssystem eingecheckt. • Lifecycle-Management
Aus VMS auschecken	Es wird ein Objekt aus dem LCM-Versionsverwaltungssystem ausgecheckt. • Lifecycle-Management
Aus VMS exportieren	Eine Ressource wird aus dem VMS exportiert. • Lifecycle-Management
In VMS sperren	Eine Ressource im VMS wird gesperrt. • Lifecycle-Management
Sperrung in VMS aufheben	Die Sperrung einer Ressource im VMS wird aufgehoben. • Lifecycle-Management
Aus VMS abrufen	Es wird ein Objekt aus dem LCM-Versionsverwaltungssystem abgerufen. • Lifecycle-Management
VMS löschen	Es wird ein Objekt aus dem LCM-Versionsverwaltungssystem gelöscht. • Lifecycle-Management

Ereignisse nach Diensttyp

Diensttyp	Generierte Ereignistypen
Analysis-Anwendungen	• Anzeigen

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Diensttyp	Generierte Ereignistypen
	• Cube-Verbindung
Dienst für die zeitgesteuerte Verarbeitung von Authentifizierungsaktualisierungen	• Bereitstellen • Ausführen
BI-Launchpad	Anzeigen
Central Management Service	• Audit-Änderung • Erstellen • Benutzerdefinierte Zugriffsberechtigung geändert • Löschen • Bereitstellen • Anmelden • Abmelden • Ändern • Abrufen • Änderung von Rechten • Auslösen
Central Management Console	Anzeigen
Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-Berichten	• Bereitstellen • Eingabeaufforderung • Regenerieren • Ausführen • Speichern
Crystal-Reports-Cache-Dienst	• Eingabeaufforderung • Regenerieren • Speichern • Anzeigen
Crystal Reports für Enterprise-Zeitsteuerungsdienst	• Bereitstellen • Eingabeaufforderung • Regenerieren • Ausführen • Speichern
Dienst für die zeitgesteuerte Verarbeitung von Crystal-Reports-Berichten	• Bereitstellen • Eingabeaufforderung • Regenerieren • Ausführen • Speichern
Dienst zum Anzeigen und Ändern von Crystal-Reports-Berichten	• Erstellen • Speichern • Anzeigen
Dashboard-Cache-Dienst	• Eingabeaufforderung • Regenerieren • Anzeigen

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Diensttyp	Generierte Ereignistypen
Dashboards-Anwendung	• Speichern
Desktop Intelligence (Client)	• Bereitstellen • Eingabeaufforderung • Abrufen • Ausführen
Desktop-Intelligence-Scheduler-Prozess	• Bereitstellen • Ausführen
Dienst für die zeitgesteuerte Verarbeitung der Zielbereitstellung	• Bereitstellen • Ausführen
Ereignisdienst	Auslösen
Information-Engine-Dienst	• Erstellen • Drill außerhalb des Bereichs • Bearbeiten • Seite abgerufen • Eingabeaufforderung • Regenerieren • Speichern • Anzeigen
Dienst zur zeitgesteuerten Verarbeitung von LCM	Ausführen
LCM-Dienst	• Erstellen • Löschen • LCM-Konfiguration • Ändern • Rollback • Ausführen • Speichern • Zu VMS hinzufügen • In VMS einchecken • Aus VMS auschecken • VMS löschen • Aus VMS exportieren • In VMS sperren • Aus VMS abrufen • Sperrung in VMS aufheben • Suchen
Live Office	• Eingabeaufforderung • Regenerieren
Multi-Dimensional Analysis Service	• Cube-Verbindung • MDAS-Sitzung • Speichern
OpenDocument	Anzeigen

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Diensttyp	Generierte Ereignistypen
Dienst zur zeitgesteuerten Verarbeitung der Plattformsuche	• Bereitstellen • Ausführen
Plattformsuchdienst	Suchen
Dienst für die zeitgesteuerte Verarbeitung von Diagnosen	• Bereitstellen • Ausführen
Dienst zur zeitgesteuerten Verarbeitung von Programmen	• Bereitstellen • Ausführen
Dienst zur zeitgesteuerten Verarbeitung von Veröffentlichungen	Ausführen
Replikationsdienst	Ausführen
SAP BusinessObjects Design Studio, Version 1.3 und höher	• Anmelden • Abmelden
Dienst zur zeitgesteuerten Verarbeitung von Sicherheitsabfragen	• Ausführen • Bereitstellen
Dienst für die zeitgesteuerte Verarbeitung des Benutzer- und Gruppenimports	• Ausführen • Bereitstellen
Dienst zur zeitgesteuerten Verarbeitung für den grafischen Vergleich	Ausführen
Web Intelligence-Anwendung	• Erstellen • Drill außerhalb des Bereichs • Bearbeiten • Ändern • Eingabeaufforderung • Regenerieren • Speichern • Anzeigen
Gemeinsamer Web-Intelligence-Dienst	• Erstellen • Drill außerhalb des Bereichs • Bearbeiten • Seite abgerufen • Eingabeaufforderung • Regenerieren • Speichern • Anzeigen
Web-Intelligence-Kerndienst	• Erstellen • Drill außerhalb des Bereichs • Bearbeiten • Seite abgerufen • Eingabeaufforderung • Regenerieren • Speichern

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Diensttyp	Generierte Ereignistypen
	• Anzeigen
Web-Intelligence-Verarbeitungsdienst	• Erstellen • Drill außerhalb des Bereichs • Bearbeiten • Seite abgerufen • Eingabeaufforderung • Regenerieren • Speichern • Anzeigen
Web-Intelligence-Dienst für zeitgesteuerte Verarbeitung und Veröffentlichung	• Bereitstellen • Ausführen

Ereigniseigenschaften und -details

Jedes von der BI-Plattform aufgezeichnete Ereignis enthält eine Reihe von Ereigniseigenschaften und -details.

Ereigniseigenschaften werden stets mit einem Ereignis generiert, jedoch enthalten sie möglicherweise keine Werte, wenn die Information nicht auf ein bestimmtes Ereignis anwendbar ist. Im ADS sind die Ereigniseigenschaften in der Tabelle enthalten, in der das Ereignis gespeichert ist, so dass sie bei der Berichterstellung zum Sortieren und Gruppieren von Ereignissen verwendet werden können.

Ereignisdetails zeichnen zusätzliche Informationen über das Ereignis auf, die nicht in den Ereigniseigenschaften enthalten sind. Falls ein Ereignisdetail nicht spezifisch für ein bestimmtes Ereignis ist, wird das Ereignisdetail nicht generiert. Es gibt eine Reihe allgemeiner Ereignisdetails, die bei Bedarf für alle Ereignistypen generiert werden können. Es gibt außerdem eine Reihe zusätzlicher Ereignisdetails, die für bestimmte Ereignistypen generiert werden. Beispielsweise zeichnen Eingabeaufforderungsereignisse die in einem Ereignisdetail für die Eingabeaufforderung eingegebenen Werte auf, es generiert jedoch kein anderer Ereignistyp ein Eingabeaufforderungswert-Ereignisdetail. Im ADS werden Details in einer separaten Tabelle gespeichert, die mit dem übergeordneten Ereignis verknüpft ist.

In einigen Fällen können die Ereignisdetails mehrere Werte enthalten. Diese Details können mit der Bunch-ID gruppiert werden. Weitere Informationen zu Bunch-IDs finden Sie im verwandten Thema.

Jegliche mehrsprachige Daten (z.B. Objekt- oder Ordnernamen) werden in der Standardsprache für das Gebietsschemas des CMS-Auditors aufgezeichnet.

Weitere Informationen

ADS-Tabellen (Audit-Datenspeicher) [Seite 1022]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

21.3.1 Überwachungsereignisse und -details

In den folgenden Abschnitten werden die Ereignistypen gefolgt von einer Beschreibung ihrer Eigenschaften und Ereignisdetails aufgeführt, die spezifisch für diese Ereignisse sind. Am Anfang jedes Abschnitts befindet sich eine Liste der Eigenschaften und Details, die allgemein für alle Ereignistypen gelten.

> **Hinweis**
>
> Einige Clientprogramme verfügen über keine spezifischen Ereignisse und greifen auf die allgemeinen und Plattformereignisse zurück, um relevante Informationen über ihre Operationen zu erfassen.

Universelle Ereigniseigenschaften und -details

Die folgende Tabelle zeigt an, welche Eigenschaften und Ereignisdetails für alle Ereignisse aufgezeichnet werden.

> **Hinweis**
>
> Die Eigenschaften in dieser Tabelle sind Spalten in der ADS_EVENT-Tabelle im Audit-Datenspeicher.

Ereigniseigenschaft	Beschreibung
Event_ID	Eine eindeutige ID für das Ereignis.
Client_Type_ID	ID für den Anwendungtyp, der das Ereignis ausgeführt hat
Service_Type_ID	Zeigt die ID des Dienst- oder Anwendungstyps an, der das Ereignis ausgelöst hat.
Start_Time	Das Startdatum und die Startuhrzeit, zu der das Ereignis gestartet wurde (in GMT)
Duration	Dauer des Ereignisses in Millisekunden.
Session_ID	ID der Sitzung, während der das Ereignis ausgelöst wurde.
Event_Type_ID	Ereignistyp (z.B. 1002 für "Anzeigen").
Status_ID	Zeichnet auf, ob die Aktion erfolgreich ist oder fehlschlägt ("0" = erfolgreich, "1" = fehlgeschlagen). Manche Ereignisse haben zusätzliche Statustypen. Diese werden zusammen mit einer Beschreibung dieser Ereignisse aufgeführt.
Object_ID	CUID des betroffenen Objekts (falls anwendbar). CUID des Warnereignisses für auslösende Ereignisse. **Hinweis** Alle nicht im CMS-Repository gespeicherten Objekte weisen eine ID mit dem Wert "0" auf. Diese Objekte können Objekte sein, die noch nicht in der CMS-Datenbank oder z.B. lokal auf einem Clientrechner gespeichert wurden. Verwenden Sie die Eigenschaft "Object_Name", um diese Objekte zu differenzieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereigniseigenschaft	Beschreibung
User_ID	CUID des Benutzers, der das Ereignis durchgeführt hat.
User_Name	Der Benutzername des Benutzers, der das Ereignis durchgeführt hat.
Object_Name	Name des betroffenen Objekts (falls vorhanden). Name des Warmmeldungsereignisses für auslösende Ereignisse.
Object_Type_ID	CUID des Objekttyps (z.B. Dokument, Ordner usw.).
Object_Folder_Path	Vollständiger Ordnerpfad zu dem Verzeichnis des betroffenen Objekts im CMS-Repository. Beispiel: `Umsatz/Nordamerika/Ostküste`
Folder_ID	Die CUID des Ordners, in dem das Objekt gespeichert ist.
Top_Folder_Name	Name des Ordners auf der obersten Ebene, in dem das betroffene Objekt gespeichert ist. Wenn das Objekt beispielsweise im Ordner `Umsatz/Nordamerika/Ostküste` gespeichert ist, würde der Wert `Umsatz` lauten.
Top_Folder_ID	Die CUID des Ordners auf der obersten Ebene, in dem das betroffene Objekt gespeichert ist. Wenn das Objekt beispielsweise im Ordner `Umsatz/Nordamerika/Ostküste` gespeichert ist, wäre der Wert die CUID des Ordners `Umsatz`.
Cluster ID	Die CUID des CMS-Clusters, das das Ereignis aufgezeichnet hat.
Action_ID	Eine eindeutige ID, die zur Verknüpfung einer Reihe von Ereignissen verwendet werden kann, die durch eine einzige Benutzeraktion initiiert wurden.

Hinweis

Die Eigenschaften in dieser Tabelle sind Spalten in der ADS_EVENT_DETAIL_TYPE_STR-Tabelle im Audit-Datenspeicher.

Ereignisdetail	ID	Beschreibung
Fehler	1	Wird nur aufgezeichnet, wenn die Aktion fehlschlägt; Text von Fehlermeldungen, die aus dem Versuch resultieren.
Element-ID	2	Name eines Objekts, das in einem Containerobjekt gespeichert ist (z.B. Live Office-Dokument oder Dashboard).
Elementname	3	Für ein Objekt, das in einem Containerobjekt gespeichert ist (z.B. Live Office-Dokument oder Dashboard) generierte ID.
Elementtyp-ID	5	Der Typ von Objekt in einem Containerobjekt, das gerade angezeigt oder geändert wird. Wird nur generiert, falls anwendbar.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
ID des übergeordneten Dokuments	12	• Für eine Dokumentinstanz: die CUID des übergeordneten Dokuments. • Für übergeordnete Dokumente: die eigene CUID.
Universums-ID	13	Die CUID des vom Dokument oder Objekt verwendeten Universums Ein Ereignisdetail wird für jedes Universum generiert, falls mehrerere verwendet werden.
Universumsname	14	Der Name des vom Dokumentobjekt verwendeten Universums. Ein Ereignisdetail wird für jedes Universum generiert, falls mehrerere verwendet werden.
Benutzergruppenname	15	Der Name der Benutzergruppe, zu der der Benutzer gehört, der die Aktion durchführt. Wenn der Benutzer mehreren Gruppen angehört, wird für jede Gruppe ein Ereignisdetail generiert.
Benutzergruppen-ID	16	Die ID der Benutzergruppe, zu der der Benutzer gehört, der die Aktion durchführt. Wenn der Benutzer mehreren Gruppen angehört, wird für jede Gruppe ein Ereignisdetail generiert.

Allgemeine Ereignisse

Die folgenden Ereignistypen gelten allgemein für alle SAP-BusinessObjects-Server und -Clients.

Ansicht

Der Benutzer hat ein Dokument/Objekt angezeigt.

- Ereignistyp-ID: 1002

Ereignisdetail	ID	Beschreibung
Größe	17	Die Größe des Objekts (in Byte), das im Fokus des Ereignisses ist.
Container-ID	32	Die CUID des Containerobjekts (z.B. Dashboard), in dem das Objekt gespeichert ist (falls anwendbar).
Containertyp	33	Der Anwendungstyp des Containers für das Objekt (falls anwendbar).

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Wenn Sie während der Dokumentenindizierung einen Suchdienst verwenden, bemerken Sie u.U. eine große Anzahl an vom "Systemkonto" generierten Anzeigeereignissen. Ursache hierfür ist der Suchindizierungsdienst, mit dem Dokumente geöffnet werden, um den Suchindex zu generieren.

Regenerieren

Ein Objekt der Datenbank wurde aktualisiert.

- Ereignistyp-ID: 1003

Ereignisdetail	ID	Beschreibung
Größe	17	Die Größe des Objekts (in Byte), das im Fokus des Ereignisses ist. **Hinweis** Für Crystal-Reports-Berichte, deren Daten mit jedem erneuten Öffnen neu regeneriert werden, ist diese Einstellung 0.
Zeilenanzahl	63	Die Anzahl der Datensätze, die der Datenbankserver zurückgegeben hat **Hinweis** Für Crystal-Reports-Berichte, deren Daten mit jedem erneuten Öffnen neu regeneriert werden, ist diese Einstellung 0.
Abfrage	25	Zeichnet die SQL-Abfrage auf, die zum Regenerieren der Daten verwendet wurde (optional, wird in der CMC eingestellt)
Universumsobjektname	31	Der Name des Universums, das das Dokument oder Objekt verwendet. Ein Ereignisdetail wird für jedes Universum generiert, auf das das Dokument oder Objekt zugreift.
Dokumentumfang	36	Zeichnet Informationen über den geplanten Umfang des Dokuments anhand seiner Publishing-Einstellungen auf (z.B.: Land=USA, Rolle=Manager). Nur für Publishing-Workflows.
Veröffentlichungsinstanz-ID	37	ID dieser Instanz der Veröffentlichung. Nur für Publishing-Workflows.
Live Office-Objekttyp	10701	Identifiziert den Objekttyp, der in einem Live Office-Dokument regeneriert wird (z.B. ein Crystal-Reports-Bericht). Wird

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
		nur für Live Office-Dokumente generiert.

Eingabeaufforderung

Es wurde ein Wert für eine Eingabeaufforderung eingegeben.

- Ereignistyp-ID: 1004

Ereignisdetail	ID	Beschreibung
Eingabeaufforderungsname	26	Der der Eingabeaufforderung zugeordnete Name (z.B. "Datum"). Für jede Eingabeaufforderung in einem Dokument oder Objekt wird ein separates Detail generiert, und sie werden gruppiert.
Wert der Eingabeaufforderung	27	Der für eine Eingabeaufforderung eingegebene Wert. Für jeden eingegebenen Wert wird ein separates Detail generiert. Sie können zusammen gruppiert und auf den Eingabeaufforderungsnamen zurück bezogen werden.
Dokumentumfang	36	Informationen über den geplanten Bereich des Dokuments (z.B. Land=USA, Rolle=Manager).
Veröffentlichungsinstanz-ID	37	ID dieser Instanz der Veröffentlichung. Nur für Publishing-Workflows.
Name zur Entwurfszeit	90	Der Name des Dashboards-Dokuments zum Zeitpunkt des Entwurfs. Wird nur für Dashboards-Aktualisierungen oder ein Dashboards- oder Live-Office-Dokument generiert, das eine Eingabeaufforderung enthält.
Live Office-Objekttyp	10701	Identifiziert den Objekttyp, der in einem Live Office-Dokument regeneriert wird (z.B. ein Crystal-Reports-Bericht). Wird nur für Live Office-Dokumente generiert, bei denen ein eingebettetes Objekt eine Eingabeaufforderung enthält.

Erstellen

Der Benutzer hat ein Objekt erstellt.

- Ereignistyp-ID: 1005

Ereignisdetail	ID	Beschreibung
Größe	17	Die Größe des Objekts (in Byte), das im Fokus des Ereignisses ist.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
Überschreiben	21	Zeichnet auf, ob das Dokument oder Objekt neu ist oder ein vorhandenes Objekt überschreibt (0=Neues Dokument oder Objekt, 1=Vorhandes Dokument oder Objekt überschreiben).
Beim Öffnen regenerieren	23	Zeichnet auf, ob das Dokument oder Objekt automatisch beim Öffnen regeneriert werden soll (0=Keine Regenerierung, 1=Beim Öffnen regenerieren). Wird nur generiert, falls anwendbar.
Beschreibung	24	Zeichnet Informationen im Dokument oder im Beschreibungsfeld des Objekts auf.

Löschen

Der Benutzer hat ein Objekt gelöscht.

- Ereignistyp-ID: 1006

Ändern

Der Benutzer hat eine Dateieigenschaft bzw. die Dateieigenschaften eines Objekts geändert.

- Ereignistyp-ID: 1007

Ereignisdetail	ID	Beschreibung
Eigenschaftsname	28	Der Name der Eigenschaft wurde geändert. Für jede geänderte Eigenschaft wird ein Ereignisdetail generiert.
Eigenschaftenwert	29	Der neue Wert für eine geänderte Eigenschaft des Dokuments oder Objekts. Für jede geänderte Eigenschaft wird ein Ereignisdetail generiert.

Speichern

Lokales oder remotes Speichern oder Exportieren eines Dokuments oder Objekts bzw. Speichern oder Exportieren eines Dokuments oder Objekts in das CMS-Repository, entweder im vorhandenen Format oder in einem anderen Format.

- Ereignistyp-ID: 1008
- Status:
  - "0" zeigt an, dass das Objekt erfolgreich lokal gespeichert wurde
  - "1" zeigt an, dass der Versuch fehlgeschlagen ist
  - "2" zeigt an, dass das Objekt erfolgreich gespeichert oder in ein Repository exportiert wurde
  - "3" zeigt an, dass das Objekt erfolgreich gespeichert oder in ein neues Format exportiert wurde

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
Größe	17	Größe des gespeicherten oder exportierten Objekts (in Byte).
Dateiname	18	Der vollständige Name, unter dem das Dokument oder Objekt gespeichert wurde. Wenn die Datei lokal durch eine Clientanwendung gespeichert wird, enthält der Name auch den Dateipfad.
Überschreiben	21	Zeichnet auf, ob das Dokument oder Objekt neu ist oder eine vorhandene Datei überschreibt. "0"=Neues Dokument oder Objekt, "1"=Vorhandenes Dokument oder Objekt überschreiben.
Format	22	Gibt das Format des gespeicherten/ exportierten Dokuments in Form einer aus drei Buchstaben bestehenden Dateierweiterung an (z.B. "doc" für eine Microsoft Word-Datei oder "pdf" für eine Adobe PDF-Datei).
Beim Öffnen regenerieren	23	Zeichnet auf, ob das Dokument oder Objekt automatisch beim Öffnen regeneriert werden soll ("0"=Keine Regenerierung, "1"=Beim Öffnen regenerieren). Wird nur erfasst, falls anwendbar.

Suchen

Es wurde eine Suche durchgeführt.

- Ereignistyp-ID: 1009

Ereignisdetail	ID	Beschreibung
Schlüsselwort	19	Die Schlüsselwörter der durchgeführten Suche.
Kategorie	20	Für die Suche verwendete Kategorie (falls anwendbar).
Zeilenanzahl	63	Die Anzahl der von der Suche zurückgegebenen Zeilen.

Bearbeiten

Der Benutzer hat den Inhalt eines Objekts bearbeitet.

- Ereignistyp-ID: 1010

Ereignisdetail	ID	Beschreibung
Größe	17	Die Größe des Objekts (in Byte), das im Fokus des Ereignisses ist.
Abfrage	25	Wenn durch die Bearbeitung eine SQL-Abfrage geändert wird, wird die neue

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
		Abfrage aufgezeichnet. (Diese Einstellung ist optional und kann auf der CMC-Überwachungsseite ausgewählt werden.)
Universumsobjektname	31	Der Name des Universums, das das Dokument oder Objekt verwendet. Ein separates Detail wird für jedes Universum generiert, auf das das Dokument oder Objekt zugreift.
Container-ID	32	Die CUID des Containers (z.B. Dashboard), der das Objekt verwendet (falls anwendbar).
Containertyp	34	Der Anwendungstyp des Containers für das Objekt (falls anwendbar).
Container-Ordnerpfad	64	Ordnerpfad für den Container des Objekts (falls anwendbar).

Ausführen

Es wurde ein Auftrag ausgeführt.

- Ereignistyp-ID: 1011
- Status:
  - "0" zeigt an, dass der Auftrag erfolgreich war
  - "1" zeigt an, dass der Auftrag fehlgeschlagen ist
  - "2" zeigt an, dass der Auftrag fehlgeschlagen ist, jedoch ein erneuter Versuch der Durchführung unternommen wird
  - "3" zeigt an, dass der Auftrag abgebrochen wurde

Ereignisdetail	ID	Beschreibung
Größe	17	Größe des Dokuments (in Byte), das ausgeführt wurde.
Dokumentumfang	36	Informationen über den geplanten Bereich des Dokuments (z.B. Land=USA, Rolle=Manager).

Bereitstellen

Ein Objekt wurde bereitgestellt.

- Ereignistyp-ID: 1012

Ereignisdetail	ID	Beschreibung
Größe	17	Größe des bereitgestellten Objekts (in Byte).
Zieltyp	35	Das Ziel der Dokument- oder Objektinstanz. Beispielsweise E-Mail, FTP, nicht verwalteter Datenträger, Posteingang oder Drucker.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
Dokumentumfang	36	Informationen über den geplanten Anwendungsbereich des Dokuments (z.B. Land=USA, Rolle=Manager).
Veröffentlichungsinstanz-ID	37	ID dieser Instanz des Dokuments oder Objekts.
Domäne	38	Zeichnet den Namen der SMTP-Serverdomäne für per E-Mail versendete Dokumente/Objekte auf (falls anwendbar).
Hostname	39	Zeichnet den Namen des SMTP- oder FTP-Hosts für per E-Mail oder FTP versendete Dokumente/Objekte auf (falls anwendbar).
Port	40	Zeichnet den Port der SMTP- oder FTP-Serverdomäne für per E-Mail oder FTP versendete Dokumente oder Objekte auf (falls anwendbar).
Senderadresse	41	Zeichnet die Adresse des Absenders für per E-Mail versendete Dokumente/ Objekte auf (falls anwendbar).
Empfängeradresse	42	Zeichnet die Adresse des Empfängers für per E-Mail versendete Dokumente/ Objekte auf (falls anwendbar). Gibt an, ob die Adresse in den Feldern "An", "CC" oder "BCC" enthalten ist. Für jeden geplanten Empfänger wird ein Ereignisdetail generiert.
Dateiname	18	Zeichnet den Dateinamen der per E-Mail oder FTP versendeten Dokumente/ Objekte oder der Dokumente/Objekte auf, die direkt auf einem nicht zur BusinessObjects-Implementierung gehörenden Datenträger gespeichert werden.
Kontoname	45	Zeichnet eines der folgenden Details auf: • Für über den **Posteingang** bereitgestellte Objekte eine Liste der Namen der BusinessObjects-Benutzerkonten. • Für über **FTP** bereitgestellte Objekte den Namen des FTP-Kontos. • Für über einen **nicht verwalteten Datenträger** bereitgestellte Objekte das verwendete Anmeldekonto.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
		• Für über **SMTP** bereitgestellte Objekte das für den SMTP-Server verwendete Anmeldekonto.
Druckername	46	Der Name des Druckers, für den das Dokument oder Objekt bereitgestellt wurde (falls anwendbar).
Anzahl der Exemplare	47	Die Anzahl der Kopien des gedruckten Dokuments oder Objekts (falls anwendbar).
Empfängername	48	Die Benutzernamen der Empfänger des Dokuments oder Objekts. Für jeden geplanten Empfänger wird ein Ereignisdetail generiert.
Warnereignis-ID	92	Die CUID des Warnereignisses. Diese wird nur generiert, wenn das Ereignis durch eine Warnmeldung ausgelöst wurde.
Warnereignisname	93	Der Name des Warnereignisses. Diese wird nur generiert, wenn das Ereignis durch eine Warnmeldung ausgelöst wurde.
Bereitstellungstyp	75	Zeigt an, wie die Bereitstellung eingeleitet wurde: • "0" zeigt zeitgesteuert an • "1" zeigt an ein Ziel gesendet an • "2" zeigt veröffentlicht an • "3" zeigt an, dass eine Warnmeldung ausgelöst wurde

Abrufen

Ein Objekt wurde vom CMS abgerufen.

- Ereignistyp-ID: 1013

Anmelden

Ein Benutzer meldet sich an.

- Ereignistyp-ID: 1014
- Status:
  - "0" zeigt an, dass die Anmeldung eines Zugriffslizenzbenutzers erfolgreich war
  - "1" zeigt einen fehlgeschlagnenen Anmeldeversuch an
  - "2" zeigt an, dass die Anmeldung eines Namenslizenzbenutzers erfolgreich war
  - "3" zeigt an, dass eine Systemanmeldung (keine Benutzeranmeldung) erfolgreich war

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
Anzahl Zugriffslizenzbenutzer	50	Die Anzahl der Benutzer im System zu dem Zeitpunkt, an dem das Ereignis ausgelöst wurde.
Von Client gemeldeter Client-Hostname	51	Vom Client gemeldeter Hostname des Clients.
Von Server aufgelöster Client-Hostname	52	Vom Server aufgelöstger Hostname des Clients. Wenn der Hostname des Clients nicht aufgelöst werden kann, wird kein Wert aufgezeichnet.
Von Client gemeldete Client-IP-Adresse	53	Vom Client gemeldete IP-Adresse des Clients
Von Server aufgelöste Client-IP-Adresse	54	Vom Server aufgelöste IP-Adresse des Clients Wenn die Client-IP nicht aufgelöst werden kann, wird kein Wert aufgezeichnet.

Abmelden

Ein Benutzer meldet sich ab.

- Ereignistyp-ID: 1015

Ereignisdetail	ID	Beschreibung
Anzahl Zugriffslizenzbenutzer	50	Die Anzahl der Zugriffslizenzbenutzer im System zu dem Zeitpunkt, an dem das Ereignis ausgelöst wurde.

Auslösen

Ein Dateiereignis wird ausgelöst.

- Ereignistyp-ID: 1016

Ereignisdetail	ID	Beschreibung
Dateiname	18	Der Name der überwachten Datei, die das Ereignis ausgelöst hat.

21.3.1.1 Plattformereignisse

Die folgenden Ereignisse sind für die BI-Plattform spezifisch.

Änderung von Rechten

Ein oder mehrere Rechte für ein Objekt wurden geändert.

- Ereignistyp-ID 10003

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
Hinzugefügte Rechte	55	Typ des hinzugefügten Rechts, Umfang des neuen Rechts (welche Objekte) und der Objekttyp, auf den es angewendet wurde. Die Daten werden gemäß dem folgenden Beispiel strukturiert: *added right=Exportieren; new value=Gewährt; scope=Aktuelles Objekt; applicable object type=alle Objekttypen*.
Entfernte Rechte	56	Typ des entfernten Rechts, Umfang des neuen Rechts (welche Objekte) und der Objekttyp, auf den es angewendet wurde. Die Daten werden gemäß dem folgenden Beispiel strukturiert: *removed right=Exportieren; previous value=Verweigert; scope=Aktuelles Objekt; applicable object type=Alle Objekttypen*.
Geänderte Rechte	57	Typ des geänderten Rechts, Umfang des neuen Rechts (welche Objekte) und der Objekttyp, auf den es angewendet wurde. Die Daten werden gemäß dem folgenden Beispiel strukturiert: *modified right=Exportieren; previous value=Gewährt; scope=Aktuelles Objekt; applicable object type=alle Objekttypen*.
Prinzipal	118	Die ID eines Benutzers oder einer Benutzergruppe (Prinzipal), deren Sicherheitsrechte geändert wurden.
Prinzipalname	119	Der Name eines Benutzers oder einer Benutzergruppe (Prinzipal), deren bzw. dessen Sicherheitsrechte geändert wurden.

Benutzerdefinierte Zugriffsberechtigung geändert

Eine benutzerdefinierte Zugriffsberechtigung wurde geändert.

- Ereignistyp-ID 10004

Ereignisdetail	ID	Beschreibung
Hinzugefügte Rechte	55	Typ des hinzugefügten Rechts, Umfang des neuen Rechts (welche Objekte) und der Objekttyp, auf den es angewendet wurde. Die Daten werden gemäß dem folgenden Beispiel strukturiert: *added right=Exportieren; new value=Gewährt; scope=Aktuelles Objekt; applicable object type=alle Objekttypen*

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
Entfernte Rechte	56	Typ des entfernten Rechts, Umfang des neuen Rechts (welche Objekte) und der Objekttyp, auf den es angewendet wurde. Die Daten werden gemäß dem folgenden Beispiel strukturiert: *removed right=Exportieren; previous value=Verweigert; scope=Aktuelles Objekt; applicable object type=Alle Objekttypen*.
Geänderte Rechte	57	Typ des geänderten Rechts, Umfang des neuen Rechts (welche Objekte) und der Objekttyp, auf den es angewendet wurde. Die Daten werden gemäß dem folgenden Beispiel strukturiert: *modified right=Exportieren; previous value=Gewährt; scope=Aktuelles Objekt; applicable object type=alle Objekttypen*.
Prinzipal	118	Die ID eines Benutzers oder einer Benutzergruppe (Prinzipal), deren Sicherheitsrechte geändert wurden.

Überwachungsänderung

Die Überwachungseinstellungen des Systems wurden geändert.

- Ereignistyp-ID 10006

Ereignisdetail	ID	Beschreibung
Ereignistyp-ID	58	Aufzeichnen der ID des Überwachungsereignistyps, der aktiviert oder deaktiviert wurde. Wenn mehrere Ereignistypen in einer Aktion aktiviert oder deaktiviert werden, wird für jeden Ereignistyp ein Detail generiert.
Aktion	59	Aufzeichnen der Überwachungsereignisse, die aktiviert oder deaktiviert wurden.
Neue Überwachungsebene	60	Wenn die Überwachungsebene eines Details geändert wurde, wird die neue Ebeneneinstellung (z.B. Aus, Minimal oder Standard) aufgezeichnet.
Alte Überwachungsebene	61	Wenn die Überwachungsebene eines Details geändert wurde, wird die vorherige Ebeneneinstellung (z.B. Aus, Minimal oder Standard) aufgezeichnet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
Überwachungsoption	62	Wenn ein optionales Detail aktiviert oder deaktiviert wird, wird das geänderte Detail bzw. ob es aktiviert und deaktiviert wurde, aufgezeichnet. Wenn mehrere Details in einer Aktion aktiviert oder deaktiviert werden, wird für jedes geänderte Detail eine Detaildatensatz erzeugt.
ADS-Verbindung	78	Wenn die Verbindung zum Überwachungs-Datenspeicher geändert wird, werden hiermit die neuen Verbindungseinstellungen im folgenden Format aufgezeichnet: `DBType=Oracle,DBName=MeinADS,Username=BEN1,Password="*****",SSO=aus,DBReconnect=ein`. Nur die geänderten Details werden aufgezeichnet. Beispiel: Wenn nur der Benutzername aktualisiert wird, wird nur `Username="neu"` aufgezeichnet. **Hinweis** Die Kennwortinformationen werden stets mit dem Zeichen `*` in der Datenbank verborgen.
Intervall für automatisches Löschen	105	Dieses Detail zeichnet alle im Feld **Ereignisse älter als x Tage** auf der Seite "Überwachung" der CMC vorgenommenen Änderungen auf. Dies legt fest, wie viele Tage die Überwachungsinformationen im ADS aufbewahrt werden.

21.3.1.2 SAP BusinessObjects Web-Intelligence-Ereignisse

Die folgenden Ereignisse kommen nur in der Komponente SAP BusinessObjects Web Intelligence vor.

Drill außerhalb des Bereichs

Der Benutzer hat einen Drill-Vorgang außerhalb des Bereichs des Berichts ausgeführt.

- Ereignistyp-ID: 10201

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
Objektinstanz	11	Zeichnet auf, ob das Ereignis auf eine geplante Aktualisierung oder einen Benutzer zurückgeht, der das Objekt anzeigt ("0" = aufgrund eines Benutzers, der das Objekt anzeigt, "1" = aufgrund einer geplanten Aktualisierung des Objekts)
Zeilenanzahl	63	Die Anzahl der Zeilen, die der Datenbankserver zurückgegeben hat
Abfrage	25	Zeichnet die Abfrage auf, die zum Regenerieren der Daten verwendet wurde (optional, wird in der CMC eingestellt)
Universumsobjektname	31	Der Name des Universums, das das Dokument verwendet. Für jedes Universum, auf das das Dokument zugreift, wird eine Instanz aufgezeichnet.
Universums-ID	32	Die CUID des Universums, das das Dokument verwendet. Für jedes Universum, auf das das Dokument zugreift, wird eine Instanz aufgezeichnet.

Seite abgerufen

Die Web-Intelligence-Dokumentseite wurde abgerufen.

- Ereignistyp-ID: 10202

21.3.1.3 SAP BusinessObjects Analysis, Edition für OLAP-Ereignisse

MDAS-Sitzung

Ein MDAS-Sitzungsvorgang wird ausgeführt.

- Ereignistyp-ID: 10300
- Status:
  - "0" = Eine neue Sitzung wurde erfolgreich geöffnet.
  - "1" = Eine neue Sitzung ist fehlgeschlagen.
  - "2" = Eine vorhandene Sitzung ist geschlossen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

MDAS-Cube-Verbindung

Ein Cube-Verbindungsvorgang wird ausgeführt.

- Ereignistyp-ID: 10301
- Status:
  - "0" = Eine neue Verbindung wurde erfolgreich geöffnet.
  - "1" = Eine neue Verbindung ist fehlgeschlagen.
  - "2" = Eine vorhandene Verbindung ist geschlossen.

Ereignisdetail	ID	Beschreibung
Verbindungs-ID	94	Eindeutiger Identifikator der Verbindung
Verbindungsname	95	Der Name der Verbindung
Providertyp	96	Der Providertyp für den Cube
Cube-Name	97	Der vollständige Name des verwendeten Cubes

21.3.1.4 Ereignisse der SAP-BusinessObjects-Hochstufverwaltungs-Console

Die folgenden Ereignisse kommen nur in der Hochstufverwaltung für SAP-BusinessObjects-Komponenten zum Einsatz.

Gemeinsame Details der SAP-BusinessObjects-Hochstufverwaltung

Alle Ereignisse der Hochstufverwaltung weisen die folgenden zusätzlichen Ereignisdetails auf.

Ereignisdetail	ID	Beschreibung
Element-Cluster	6	Die CUID von betroffenen Clustern, wenn die Hochstufverwaltungs-Console einen Vorgang für Objekte in anderen Clustern ausführt. Für jeden betroffenen Cluster wird ein Ereignisdetail generiert.
Elementkommentar	7	Zusätzliche Informationen zum Objekt
Primärelement	8	Wenn das Element ein Primärelement ist, wird dieses Detail auf "1" eingestellt. Wenn es sich um ein abhängiges Element handelt, wird es auf "0" eingestellt.
Elementstatus	9	Falls das Vorgangselement fehlschlägt, wird dieses Detail auf "1" eingestellt, ansonsten auf "0".

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
Vorgang	10	Beschreibt den Typ des ausgeführten Vorgangs (zum Beispiel Löschen, Hinzufügen oder Ändern).

Konfiguration der SAP-BusinessObjects-Hochstufverwaltung

Die Konfiguration der Hochstufverwaltung hat sich geändert.

- Ereignistyp-ID: 10900

Ereignisdetail	ID	Beschreibung
Konfiguration	100	Ein Benutzer sieht sich die Konfiguration der Hochstufverwaltungs-Console an. Die Konfiguration wird in Form von kommagetrennten Wertepaaren angezeigt. Beispiel: Rollbackeinstellungen=aktiviert, Port=900.
Konfiguration vor	101	Wenn Sie die Einstellungen der Hochstufverwaltungs-Console für ein Objekt ändern, werden die vorherigen Konfigurationseinstellungen aufgezeichnet. Verwendet dasselbe Format wie "Konfiguration".
Konfiguration nach	102	Wenn Sie die Einstellungen der Hochstufverwaltungs-Console für ein Objekt ändern, werden die neuen Konfigurationseinstellungen aufgezeichnet. Verwendet dasselbe Format wie "Konfiguration".
VMS-Typ	10900	Der Typ des Versionsverwaltungssystems.

Rollback

Ein Objekt wurde per Rollback auf eine vorherige Version des Versionsverwaltungssystems (VMS) zurückgesetzt.

- Ereignistyp-ID: 10901

Zu VMS hinzufügen

Dem VMS wird eine Ressource hinzugefügt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Ereignistyp-ID: 10902

Ereignisdetail	ID	Beschreibung
Version	104	Zeichnet die Versionsnummer des Dokuments im Versionsverwaltungssystem auf.

Aus VMS abrufen

Eine Ressource wird aus dem VMS abgerufen.

- Ereignistyp-ID: 10903

Ereignisdetail	ID	Beschreibung
Gelöschtes Objekt wiederherstellen	103	Gibt darüber Aufschluss, ob ein abgerufendes Objekt aus dem System gelöscht wurde. "0" gibt an, dass das Objekt nicht gelöscht wurde. "1" gibt an, dass das Objekt gelöscht wurde.
Version	104	Zeichnet die Versionsnummer des Dokuments im VMS auf.

In VMS einchecken

Eine Ressource wird in das VMS eingecheckt.

- Ereignistyp-ID: 10904

Ereignisdetail	ID	Beschreibung
Version	104	Zeichnet die Versionsnummer des Dokuments im VMS auf.

Aus VMS auschecken

Eine Ressource wird aus dem VMS ausgecheckt.

- Ereignistyp-ID: 10905

Ereignisdetail	ID	Beschreibung
Version	104	Zeichnet die Versionsnummer des Dokuments im VMS auf.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Aus VMS exportieren

Eine Ressource wird aus dem VMS exportiert.

- Ereignistyp-ID: 10906

Ereignisdetail	ID	Beschreibung
Version	104	Zeichnet die Versionsnummer des Dokuments im VMS auf.

In VMS sperren

Eine Ressource im VMS wurde gesperrt, um eine Bearbeitung durch Benutzer zu verhindern.

- Ereignistyp-ID: 10907

Ereignisdetail	ID	Beschreibung
Version	104	Zeichnet die Versionsnummer des Dokuments im VMS auf.
Gesperrt durch	10901	Der Benutzername des Benutzers, der die Aktion ausgeführt hat

Sperrung in VMS aufheben

Die Sperrung einer Ressource im VMS wurde aufgehoben, um eine Bearbeitung durch Benutzer zu erlauben.

- Ereignistyp-ID: 10908

Ereignisdetail	ID	Beschreibung
Version	104	Zeichnet die Versionsnummer des Dokuments im VMS auf.
Entsperrt durch	10902	Der Benutzername des Benutzers, der die Aktion ausgeführt hat

VMS löschen

Eine Ressource wird aus dem VMS gelöscht.

- Ereignistyp-ID: 10909

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ereignisdetail	ID	Beschreibung
Version	104	Zeichnet die Versionsnummer des Dokuments im Versionsverwaltungssystem auf.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

22 Plattformsuche

22.1 Plattformsuche

Mit der Plattformsuche können Sie das Repository der BI-Plattform nach Inhalten durchsuchen. Die Suchergebnisse werden verfeinert, indem sie in Kategorien gruppiert und nach Relevanz sortiert werden.

In dieser Version der BI-Plattform wurde die Plattformsuche um die folgenden Funktionen erweitert:

- Suche nach BI-Plattform- und Explorer-Inhalten
- Vorschlagen einer Abfrage zum Erstellen eines Dokuments, wenn kein vorhandenes Dokument gefunden werden kann
- Unterstützung der fortlaufenden Indizierung und der auf der zeitgesteuerten Verarbeitung basierenden Indizierung
- Unterstützung der Indizierung in einer geclusterten Umgebung
- Einstellen und Ändern der Indizierungsebene
- Bereitstellung erweiterter Suchkonfigurationsoptionen
- Unterstützung der mehrsprachigen Suche und Indizierung
- Bereitstellung einer erweiterten Suchsyntax
- Unterstützung von Metadaten, Inhalten und dynamischen Facetten
- Unterstützung der Selbstreparatur auf Basis der Systemlast

> **Hinweis**
>
> Bei der Migration von der Vorgängerversion auf eine neue Version wird der Index nicht migriert.

22.1.1 Plattformsuche-SDK

Von der Plattformsuche wird ein öffentliches SDK unterstützt, das als Schnittstelle zwischen der Clientanwendung und der Plattformsuche fungiert. Es wird öffentlich bereitgestellt, um Sie bei der Anpassung des Suchdiensts und bei der Integration in Ihre Anwendung zu unterstützen.

Wenn ein Suchanfrageparameter über die Clientanwendung an die SDK-Schicht gesendet wird, konvertiert die SDK-Schicht den Anfrageparameter in ein XML-codiertes Format und übermittelt ihn an den Plattformsuchdienst.

Weitere Informationen zur Plattformsuche-API finden Sie in der *Business Intelligence platform Java API Reference*.

22.1.2 Geclusterte Umgebung

Die Plattformsuche kann die Last auf mehrere Knoten in einer geclusterten Umgebung verteilen. Die Implementierung in einer geclusterten Umgebung gewährleistet die optimale Nutzung der Systemressourcen und steigert die Serverleistung.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Die Plattformsuche unterstützt sowohl das horizontale als auch das vertikale Clustern für Such- und Indizierungsfunktionen. In der geclusterten Umgebung optimiert sie die Leistung von Such- und Indizierungsprozessen.

Lastausgleich

Die Plattformsuche unterstützt den Lastausgleich für Indizierung und Suche. In einer geclusterten Umgebung können Indizierungs- und Suchanfragen zur Lastenverteilung auf mehreren Knoten ausgeführt werden. Jeder Knoten ist unabhängig bei der Indizierung des Inhalts und der Erstellung von Delta-Indizes. Es fungiert jedoch nur ein Knoten des Clusters als Masterindex und führt die Deltaindizes im Masterindex zusammen. Alle Knoten können auf den Hauptindex zugreifen. Dies ermöglicht simultane Suchanfragen.

Failover

Der Failover-Mechanismus stellt sicher, dass die Benutzer die Suchfunktion und den Indizierungsvorgang ohne Unterbrechung weiterhin verwenden können. Wenn ein Knoten in einem Cluster aufgrund eines technischen Fehlers oder aufgrund von Wartungsaktivitäten nicht zur Verfügung steht, übernimmt ein anderer Knoten automatisch die Verarbeitung der Indizierungs- und Suchanfragen.

22.2 Einrichten der Plattformsuche

22.2.1 Implementieren von OpenSearch

Die Plattformsuche unterstützt den OpenSearch-Standard, und Clientanwendungen können den OpenSearch-Standard oder das Format verwenden, um mit der Plattformsuche zu kommunizieren. Da OpenSearch nicht standardmäßig mit SAP BusinessObjects Business Intelligence installiert wird, müssen die Benutzer es manuell als separate WAR-Datei (`opensearch.war`) auf einem Anwendungsserver wie Tomcat oder mit dem WDeploy-Tool implementieren. Diese Datei wird vom Installationsprogramm in das Verzeichnis **`<INSTALLVERZ>`** `\warfiles\OpenSearch` kopiert.

> **Hinweis**
>
> Clientprogramme müssen die OpenSearch-Standards einhalten, um mit der Plattformsuche zu kommunizieren.

> **Hinweis**
>
> Der Tomcat-Anwendungsserver wird standardmäßig bei der Installation der BI-Plattform installiert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

22.2.1.1 Manuelle Implementierung

Um OpenSearch in einer BI-Plattform-Umgebung zu implementieren, führen Sie folgende Schritte aus:

1. Wechseln Sie in das folgende Verzeichnis: **<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\.
2. Kopieren Sie den OpenSearch-Ordner nach **<INSTALLVERZ>**\tomcat\webapps\.
3. Ändern Sie die Konfigurationsparameter in der Datei \OpenSearch\WEB-INF\config.properties:
   - CMS: der CMS-Name mit der Portnummer: <CMS-Name>:<Portnummer>.
   - OpenDocURL: die URL der OpenDocument-Anwendung: http://<TomcatHost>:<Connector Port>/BOE/OpenDocument/opendoc/openDocument.jsp.
   - Proxy.rpurl: Der Name des Reverse-Proxy-Servers ist dann erforderlich, wenn Sie einen Reverse Proxy verwenden möchten.
   - Proxy.opendoc.rpurl: Der Name des opendoc-Reverse Proxy-Servers ist dann erforderlich, wenn Sie den Reverse Proxy verwenden möchten.
4. Starten Sie den Tomcat-Anwendungsserver zur Implementierung von OpenSearch neu.

22.2.1.2 Implementierung mit WDeploy

Gehen Sie zum Implementieren von OpenSearch mithilfe von WDeploy wie folgt vor.

> **Hinweis**
>
> Befehle haben für Windows und UNIX jeweils das Format wdeploy.bat <Parameter> und wdeploy.sh <Parameter>.

1. Aktualisieren Sie die Datei config.**<Anwendungsserver>**, die sich unter **<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf befindet, mit den erforderlichen Webanwendungsserver-Parametern wie Installationsverzeichnis, Instanzname, Admin-Port, Admin-Benutzername und -Kennwort.
2. Ändern Sie die Konfigurationsparameter in der Datei **<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\OpenSearch\WEB-INF\config.properties:
   - CMS: der CMS-Name mit der Portnummer: <CMS-Name>:<Portnummer>.
   - OpenDocURL: die URL der OpenDocument-Anwendung: http://<Webanwendungsserver-Host>:<Connectorport>/BOE/OpenDocument/opendoc/openDocument.jsp.
   - Proxy.rpurl: Der Name des Reverse-Proxy-Servers ist dann erforderlich, wenn Sie einen Reverse Proxy verwenden möchten.
   - Proxy.opendoc.rpurl: Der Name des opendoc-Reverse Proxy-Servers ist dann erforderlich, wenn Sie einen Reverse Proxy verwenden möchten.
3. Führen Sie den Befehl *wdeploy.bat <Webanwendungsserver> -Dapp_source_tree=<übergeordneter Ordner der OpenSearch-Webanw.> -DAPP=OpenSearch deploy* vom Speicherort **<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\wdeploy aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Mit dem folgenden Befehl wird OpenSearch beispielsweise auf einem WebSphere 7-Webanwendungsserver implementiert:

```
wdeploy.bat websphere7 -Dapp_source_tree="<INSTALLDIR>\SAP BusinessObjects
Enterprise XI 4.0\warfiles" -DAPP=OpenSearch deploy
```

4. Starten Sie den Anwendungsserver neu.

22.2.2 Konfigurieren von Reverse-Proxy-Servern

Um Webanwendungen auf einem Webanwendungsserver zu implementieren, der sich hinter einem Reverse-Proxy-Server befindet, müssen Sie den Reverse-Proxy-Server so konfigurieren, dass eingehende URL-Anforderungen der entsprechenden WAR-Datei zugeordnet werden.

Zur Abbildung der Konfigurationsschritte verwenden wir als Beispiel einen Apache 2.2-Reverse Proxy-Server. Konfigurieren des Apache 2.2-Reverse Proxy-Servers für OpenSearch:

1. Richten Sie den Reverse-Proxy-Server ein, und nehmen Sie die Änderungen an der Datei `WEB-INF\config.properties` von OpenSearch vor.
2. Aktivieren Sie die folgenden Kontextparameter, und ändern Sie die Werte entsprechend.
   - `proxy.rpurl`: Dies ist die Reverse-Proxy-URL für OpenSearch (z.B. `http://RechnerIPAdresse/RP/OpenSearch/`).
   - `proxy.opendoc.rpurl`: Dies ist die Reverse-Proxy-URL für Open Doc (z.B. `http://RechnerIPAdresse/RP/BOE/`).
3. Aktualisieren Sie die Datei `httpd.conf` im Installationsordner des Apache-Reverse-Proxys mit den folgenden Einstellungen:
   - `ProxyPass /RP/BOE/OpenDocument/ http://<Tomcat-Host>:<Connector-Port>/BOE/OpenDocument/`
   - `ProxyPass /RP/OpenSearchRP/ http://<Tomcat-Host>:<Connector-Port>/OpenSearch/`
   - `ProxyPassReverseCookiePath /BOE /RP/BOE`
   - `ProxyPassReverseCookiePath /OpenSearchRP /RP/OpenSearchRP`
4. Starten Sie den Apache 2.2-Reverse Proxy-Server neu.

22.2.3 Konfigurieren von Anwendungseigenschaften in der CMC

Zum Konfigurieren der Anwendungseigenschaften der Plattformsuche führen Sie die folgenden Schritte aus:

1. Wechseln Sie zum Bereich *Anwendungen* der CMC.
2. Wählen Sie **Anwendung zur Plattformsuche**.
3. Klicken Sie auf **Verwalten** > **Eigenschaften**. Das Dialogfeld *Eigenschaften* wird angezeigt.
4. Konfigurieren Sie die Plattformsucheinstellungen:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung
Suchstatistiken	Die Plattformsuche bietet die folgenden Suchstatistiken: ○ Indizierungsstatus: zeigt den Status des Indizierungsvorgangs an. ○ Anzahl der indizierten Dokumente: zeigt die Anzahl der Dokumente an, die indiziert wurden. ○ Zeitstempel der letzten Indizierung: zeigt den Zeitstempel des Zeitpunkts an, an dem das Dokument zum letzten Mal indiziert wurde.
Indizierung starten/Indizierung stoppen	Mit den Optionen "Indizierung starten" und "Indizierung stoppen" können Sie Indizierungsprozesse zu Wartungszwecken starten bzw. stoppen oder wenn Sie vom kontinuierlichen Crawling zum zeitgesteuert verarbeiteten Crawling wechseln möchten. Um die Indizierung zu stoppen, klicken Sie auf **Indizierung stoppen**.
Standardindexgebietsschema	Die Plattformsuche verwendet das in der CMC angegebene Gebietsschema für die Indizierung aller nicht lokalisierten BI-Dokumente. Nach der Lokalisierung des Dokuments wird die entsprechende Sprachanalyse für die Indizierung verwendet. Die Suche basiert auf dem Produktgebietsschema des Clients, und die Gewichtung wird dem Produktgebietsschema des Clients zugewiesen. Sie können die Gewichtung in den Konfigurationseigenschaften der CMC konfigurieren.
Crawling-Frequenz	Sie können das gesamte BI-Plattform-Repository mithilfe der folgenden Optionen indizieren: ○ Kontinuierliches Crawling: Mit dieser Option wird kontinuierlich indiziert. Das Repository wird jedes Mal indiziert, wenn ein Objekt hinzugefügt, geändert oder gelöscht wird. Die Option bietet Ihnen die Möglichkeit, den aktuellen Inhalt der BI-Plattform anzuzeigen bzw. damit zu arbeiten. Das standardmäßig aktivierte fortlaufende Crawling aktualisiert ständig das Repository mit den von Ihnen ausgeführten Aktionen. Das kontinuierliche Crawling erfordert keinen Benutzereingriff und verkürzt die zur Indizierung eines Dokuments benötigte Zeit. ○ Zeitgesteuert verarbeitetes Crawling: Mit dieser Option wird auf der Grundlage eines Zeitplans indiziert, der durch die Optionen der zeitgesteuerten Verarbeitung festgelegt wird. Weitere Informationen darüber, wie Objekte zeitgesteuert verarbeitet werden, finden Sie im Abschnitt *Zeitgesteuertes Verarbeiten eines Objekts* unter "Plattformsuche" in der *Onlinehilfe für die CMC von SAP BusinessObjects Business Intelligence*. Hinweis ○ Wenn Sie **Zeitgesteuert verarbeitetes Crawling** auswählen und **Wiederholung** auf eine andere Option als **Jetzt** setzen, zeigt die Platt-

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung
	formsuche das Datum und den Zeitstempel für die nächste zeitgesteuerte Indizierung des Dokuments an. ○ Wenn Sie **Kontinuierliches Crawling** auswählen, wird die Schaltfläche **Indizierung starten** aktiviert und die Schaltfläche **Indizierung stoppen** deaktiviert. ○ Nach Abschluss der zeitgesteuerten Verarbeitung ist die Schaltfläche **Indizierung stoppen** deaktiviert.
Index-Speicherort	Die Indizes werden in freigegebenen Ordnern an den folgenden Speicherorten abgelegt: ○ Speicherort des Hauptindex (Indizes, Rechtschreibprüfungen): An diesem Speicherort werden der Hauptindex und der Rechtschreibprüfungsindex gespeichert. Bei einer Suche werden die anfänglichen Ergebnisse mit dem Hauptindex und die Vorschläge mit den Rechtschreibprüfungsindizes abgerufen. In einer geclusterten Implementierung der BI-Plattform sollte sich dieser Speicherort in einem freigegebenen Dateisystem befinden, das für alle Knoten im Cluster zugänglich ist. ○ Speicherort für persistente Daten (Inhaltsspeicher): Der Inhaltsspeicher befindet sich an diesem Speicherort. Er wird auf Basis des Speicherorts des Hauptindex erstellt und bleibt mit diesem synchronisiert. Der Inhaltsspeicher dient zum Generieren von Facetten und zur Verarbeitung der anfänglichen Treffer, die aus dem Speicherort des Hauptindex generiert wurden. In einer geclusterten BI-Plattform-Implementierung werden Inhaltsspeicher auf jedem Knoten generiert. Der Speicherort für persistente Daten ist der einzige Indexspeicherort, der von der geclusterten Umgebung betroffen ist, da er die Inhaltsspeicherordner enthält. Wenn ein Rechner nur über einen Suchdienst verfügt, gibt es auch nur einen Speicherort für den Inhaltsspeicher. Zum Beispiel: {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores. Wenn jedoch in einer geclusterten Umgebung mehrere Suchdienste vorhanden sind, gibt es für jeden Suchdienst einen Speicherort für den Inhaltsspeicher. Sollten Sie zwei Instanzen eines Servers ausführen, lauten die Speicherorte für den Inhaltsspeicher: 1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores. 2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name 1>\ContentStores. ○ Kein persistenter Datenspeicherort (temporäre Ersatzdateien, Delta-Indizes): An diesem Speicherort werden die Delta-Indizes erstellt und temporär gespeichert, bevor sie mit dem Hauptindex zusammengeführt werden. Die Indizes von diesem Speicherort werden nach dem Zusammenführen mit dem Hauptindex gelöscht. Außerdem werden an diesem Speicherort Ersatzdateien (Ausgabe der Extraktoren) erstellt und temporär gespeichert, bis sie in Delta-Indizes konvertiert werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung
	Hinweis ○ Alle Speicherorte von Indizes müssen freigegeben sein. ○ Sie müssen auf **Indizierung stoppen** klicken, um den Indexspeicherort zu ändern. ○ Wenn Sie einen Indexspeicherort ändern, kopieren Sie den Inhalt an einen neuen Speicherort, sonst gehen die vorhandenen Indexinformationen verloren.

Indizierungsebene	Sie könne den Suchinhalt abstimmen, indem Sie die Indizierungsebene wie folgt festlegen:
	○ Plattform-Metadaten: Ein Index wird ausschließlich für die Plattform-Metadateninformationen wie Titel, Schlüsselwörter und Beschreibungen von Dokumenten erstellt.
	○ Plattform- und Dokument-Metadaten: Dieser Index beinhaltet sowohl die Plattform- als auch die Dokument-Metadaten. Zu den Dokument-Metadaten gehören Erstellungsdatum, Änderungsdatum und Name des Autors.
	○ Gesamter Inhalt: Dieser Index beinhaltet die Plattform-Metadaten, Dokument-Metadaten und andere Inhalte wie:
	  ○ den tatsächlichen Inhalt des Dokuments
	  ○ den Inhalt von Eingabeaufforderungen und Wertelisten
	  ○ Diagramme, Grafiken und Beschriftungen
	Hinweis
	Wenn Sie die Indizierungsebene ändern, wird die Indizierung für die Regenerierung des gesamten BI-Plattform-Repositorys initialisiert.

Inhaltstypen	Für die Indizierung stehen folgende Inhaltstypen zur Auswahl: ○ Crystal Reports ○ Web Intelligence ○ Universum ○ BI-Arbeitsbereich ○ Microsoft PowerPoint ○ Adobe Acrobat ○ Rich Text ○ Text ○ Microsoft Word ○ Microsoft Excel
Index neu erstellen	Mit dieser Option wird der gesamte Index gelöscht und das gesamte Repository neu indiziert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung
	Sie können die Option **Index neu erstellen** unabhängig davon auswählen, ob die Indizierung ausgeführt wird oder gestoppt wurde. Der vorhandene Index wird gelöscht, wenn Sie Ihre Änderungen auf der Eigenschaftenseite speichern. Wenn die Indizierung jedoch derzeit gestoppt ist, wird der Index erst dann wieder neu erstellt, wenn Sie die Indizierung erneut starten. Falls die Dokumente nicht mit der Plattformsuche neu indiziert werden sollen, heben Sie die Auswahl der Option **Index neu erstellen** auf, bevor Sie auf **Indizierung starten** klicken.
Von der Indizierung ausgeschlossene Dokumente	Die Option **Von der Indizierung ausgeschlossene Dokumente** schließt Dokumente von der Indizierung aus. Es könnte z. B. sein, dass Sie extrem große Crystal-Reports-Berichte von der Suche ausschließen möchten, um die Report-Application-Server-Ressourcen nicht zu überlasten. Außerdem möchten Sie möglicherweise Veröffentlichungen mit Hunderten von personalisierten Berichten indizieren. Durch Ausschließen bestimmter Dokumente können Sie den Zugriff auf diese Dokumente über die Plattformsuche verhindern. Wenn ein Dokument jedoch indiziert wurde, bevor es dieser Gruppe zugewiesen wurde, kann es weiterhin durchsuchbar sein. Damit sichergestellt ist, dass die Dokumente in der Gruppe **Von der Indizierung ausgeschlossene Dokumente** nicht durchsuchbar sind, müssen Sie den Index neu erstellen. Das Administratorkonto hat standardmäßig vollständige Kontrolle über die Option **Von der Indizierung ausgeschlossene Dokumente**. Andere Benutzer mit den folgenden Rechten können lediglich Dokumente zu der Gruppe **Von der Indizierung ausgeschlossene Dokumente** hinzufügen: ○ Ansichts- und Bearbeitungsrechte für die Kategorie ○ Direkte Bearbeitung des Dokuments

5. Klicken Sie auf **Speichern und schließen**.

> **Hinweis**
>
> Wenn ein Benutzer die Option **Index neu erstellen** nicht auswählt und die Indizierungsebene ändert oder Extraktoren aktiviert oder deaktiviert, wird der Index schrittweise aktualisiert, ohne dass der vorhandene Index gelöscht wird.

22.3 Arbeiten mit der Plattformsuche

22.3.1 Indizierung von Inhalten im CMS-Repository

Die Indizierung ist ein fortlaufender Vorgang, der folgende Aufgabenabfolge beinhaltet:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Crawling: Crawling bezeichnet einen Mechanismus für die Abfrage des CMS-Repositorys und die Identifizierung von Objekten, die veröffentlicht, geändert oder gelöscht wurden. Es gibt zwei Varianten: kontinuierliches und zeitgesteuert verarbeitetes Crawling.

   Weitere Informationen zum kontinuierlichen oder zeitgesteuert verarbeiteten Crawling finden Sie unter dem Thema *Konfigurieren von Anwendungseigenschaften* in den verwandten Themen.
2. Extrahierung: Extrahierung bezeichnet einen Mechanismus für den Aufruf der Extraktoren auf Grundlage des Dokumenttyps. Für jeden im Repository verfügbaren Dokumenttyp ist ein spezieller Extraktor vorhanden. Durch die Definition neuer Extraktor-Plugins können neue Dokumenttypen für die Suche verfügbar gemacht werden. Jeder dieser Extraktoren ist skalierbar genug, um Inhalt aus großen Dokumenten mit vielen Datensätzen zu extrahieren.

   Folgende Extraktoren werden unterstützt:

   - Metadaten-Extraktor
   - Crystal-Reports-Extraktor
   - Web-Intelligence-Extraktor
   - Universe-Extraktor
   - Extraktoren von Drittherstellern (MS Office 2003 und 2007 und PDF-Dokumente)

   Weitere Informationen zu durchsuchbaren Dokumenttypen finden Sie im Thema *Durchsuchbare Inhaltstypen* in den verwandten Themen.
3. Indizierung: Die Indizierung ist ein Mechanismus, mit dem alle extrahierten Inhalte über eine Bibliothek eines Drittanbieters, Apache Lucene Engine, indiziert werden. Die Zeit für die Indizierung variiert und ist von der Anzahl der Objekte im System, von deren Größe und dem Typ der Dokumente abhängig.

   Die Indizierung kann nur erfolgreich ausgeführt werden, wenn die folgenden Server ausgeführt werden und aktiv sind:

   - Input File Repository Server (IFRS)
   - Output File Repository Server (OFRS)
   - Central Management Server (CMS)
   - Der Adaptive Processing Server (APS), von dem der Plattformsuchdienst gehostet wird

   Wenn als Objekttyp Web-Intelligence- oder Crystal-Reports-Bericht festgelegt wurde, muss der entsprechende Web Intelligence Processing Server oder Crystal Reports Application Server für die entsprechenden ausgewählten Objekttypen ausgeführt werden und aktiviert sein.
4. Inhaltsspeicher: Der Inhaltsspeicher enthält aus dem Hauptindex extrahierte Informationen wie ID, CUID, Name, Art und Instanz in einem leicht lesbaren Format. Auf diese Weise wird der Suchvorgang beschleunigt.

Weitere Informationen

Konfigurieren von Anwendungseigenschaften in der CMC [Seite 624]
Durchsuchbare Inhaltstypen [Seite 744]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

22.3.2 Liste der Indizierungsfehler

Die "Liste der Indizierungsfehler" enthält eine Auflistung der Dokumente, die nicht indiziert werden konnten. Die Plattformsuche ermöglicht drei Versuche für die Indizierung eines Dokuments. Wenn ein Dokument aufgrund eines Fehlers nicht indiziert werden kann, wird es in der Liste der Indizierungsfehler aufgeführt.

Zum Anzeigen der Liste der Indizierungsfehler führen Sie die folgenden Schritte durch:

1. Wechseln Sie zum Bereich "Anwendungen" der CMC.
2. Wählen Sie **Anwendung zur Plattformsuche**.
3. Wählen Sie **Aktionen > Liste der Indizierungsfehler**.

   Das Dialogfeld "Anwendung zur Plattformsuche", in dem eine Liste von Dokumenten mit folgenden Details eingeblendet wird, wird angezeigt:

   - Titel: Zeigt den Titel des Dokuments an, das nicht indiziert werden konnte.
   - Typ: Zeigt den Namen des Dokumenttyps, z.B. Crystal-Reports-Bericht oder Web Intelligence, zusammen mit dem Speicherort des Dokuments an.
   - Fehlertyp: Zeigt den Fehlergrund sowie den Grund des Indizierungsfehlers des Dokuments an. Klicken Sie auf den Hyperlink "Weitere Infos", um weitere Informationen über die Stapel-Ablaufverfolgung des Grunds des Fehlers anzuzeigen.
   - Uhrzeit des letzten Versuchs: Zeigt den Zeitstempel des letzten Versuchs der Indizierung eines Dokuments an.

22.3.3 Suchergebnisse

22.3.3.1 Vorabsuche

22.3.3.1.1 Vorgeschlagene Abfragen

Wenn ein Benutzer die Plattformsuche verwendet, möchte er vielleicht Antworten auf eine bestimmte Frage finden, und nicht nach einem bestimmten Objekt suchen. Diese Fragen können in den im BI-Plattform-Repository verfügbaren Berichten beantwortet werden oder nicht.

Die Plattformsuche analysiert die Struktur von Universen und bestehenden Berichten in Ihrem Repository und vergleicht diese Informationen mit der Suchanfrage des Benutzers, um somit neue SAP-BusinessObjects-Web-Intelligence-Abfragen vorzuschlagen, mit deren Hilfe Benutzer die Antworten zu ihren Fragen finden können.

Zur Erstellung möglicher Berichte gleicht die Plattformsuche die Wörter in allen Universen bezüglich Dimension, Kennzahl, Bedingung und Filterwert ab.

Die Plattformsuche durchsucht folgende Informationen nach Übereinstimmungen mit Universen oder vorhandenen Web-Intelligence-Dokumenten:

- Kennzahlen in Universen, die mit den eingegebenen Suchbegriffen übereinstimmen

  Wenn eine Kennzahl mit einem der Suchbegriffe übereinstimmt, wird diese Kennzahl im resultierenden Web-Intelligence-Dokument verwendet.
- Dimensionsnamen in Universen, die mit den eingegebenen Suchbegriffen übereinstimmen

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wenn ein Dimensionsname mit einem der Suchbegriffe übereinstimmt, werden im resultierenden Web-Intelligence-Dokument die Informationen zu dieser Dimension aufgeschlüsselt.

- Zum gezielten Anzeigen bestimmter Daten im Dokument können Abfragefilter verwendet werden. Diese Abfragefilter werden durch Analysieren der eingegebenen Suchbegriffe erzeugt.
  - Wenn der Name einer Universumsbedingung mit einem der Suchbegriffe übereinstimmt, wird die Bedingung als Filter verwendet.
  - Wenn Web-Intelligence-Dokumente, deren Namen mit Suchbegriffen übereinstimmen, Feldwerte enthalten, wird ein Filter aus der Dimension des Verlaufsberichts mit dem übereinstimmenden Wert erstellt. Als Bedingungsoperator wird "Gleich" verwendet.

Wenn bei der Plattformsuche genügend Übereinstimmungen gefunden wurden, sodass das resultierende Dokument zwei Ergebnisfelder und einen Filter enthält, ist die Abfrage bereit zur Ausführung. In diesem Fall kann der Benutzer durch Klicken den fertig gestellten Bericht anzeigen.

Wenn nicht genügend Übereinstimmungen zwischen den Universen und dem Dokument gefunden wurden, können Sie die Abfrage vor der Ausführung bearbeiten.

Bei der Plattformsuche werden mehrere Abfragen vorgeschlagen, wenn mehrere Universen mit den eingegebenen Suchbegriffen übereinstimmen, oder wenn das gleiche Wort in zwei unterschiedlichen Übereinstimmungen auftritt, z.B. im Namen einer Dimension und als Filterwert.

22.3.3.1.2 Durchsuchbare Inhaltstypen

Die in der BI-Plattform veröffentlichten Inhalte können mit der Plattformsuche durchsucht werden. Die Objekttypen sind unten mit dem entsprechenden indizierten Inhalt aufgelistet:

Objekttyp	Indizierter Inhalt
Crystal Reports (2008, 2011 und 2013)	Titel, Beschreibung, Auswahlformel, gespeicherte Daten, Textfelder in beliebigen Abschnitten, Parameterwerte und Unterberichte.
Web-Intelligence-Dokumente	Titel, Beschreibung, Namen der im Bericht verwendeten Universumsfilter, gespeicherte Daten, Konstanten in der lokal im Bericht definierten Filterbedingung, Namen der im Bericht verwendeten Universumskennzahlen, Namen der im Bericht verwendeten Universumsobjekte, Daten in Datensätzen und statischer Text in Zellen.
Microsoft Excel-Dokumente (2003 und 2007)	Daten in allen nicht leeren Zellen, Felder auf der Seite "Zusammenfassung" der Dokumenteigenschaften (Titel, Thema, Autor, Firma, Kategorie, Stichwörter und Kommentare) sowie Text in Kopf- und Fußzeilen von Dokumenten. Bei Zellen, die eine Berechnung oder Formel verwenden, kann der Wert nach der Auswertung durchsucht

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Objekttyp	Indizierter Inhalt
	werden. Für Zahlen- sowie Datums-/Uhrzeitwerte können die Rohdaten durchsucht werden.
Microsoft Word-Dokumente (2003 und 2007)	Text in allen Abschnitten und Tabellen, Felder auf der Seite "Zusammenfassung" der Dokumenteigenschaften (Titel, Thema, Autor, Firma, Kategorie, Stichwörter und Kommentare), Text in Kopf- und Fußzeilen von Dokumenten sowie numerischer Text.
RTF-, PDF-, PPT- und TXT-Dateien	Sämtlicher Text in diesen Dateien kann durchsucht werden.
LCMJob, AFDashboard Page, Dashboards, ObjectPackage, Webdienstabfrage (QaaWS), Profile, Diskussionen, InformationDesigner, Widgets für SAP BusinessObjects Business Intelligence, MDAnalysis, Veröffentlichungen, Flash, Analytic und Hyperlink	Metadateninhalt kann durchsucht werden.
Ereignisse	Sämtliche Ereignisse, wie benutzerdefinierte Ereignisse, Systemereignisse, Crystal-Reports-Ereignisse und Überwachungsereignisse können durchsucht werden. Wenn ein Ereignis mit einer Quelle verbunden ist, berücksichtigt die Plattformsuche die Quelle gemeinsam mit dem Ereignis. **Hinweis** Die Plattformsuche unterstützt Ereignisse für Crystal Reports für Enterprise.
BI-Arbeitsbereich	• Der Titel, die Beschreibung und der Inhalt der folgenden BIW-Module werden indiziert: ○ Textmodul ○ Webseitenmodul ○ Navigationslistenmodul ○ Viewer-Modul • Der Titel und die Beschreibung eines zusammengesetzten Moduls werden indiziert. • Nur der Titel eines Arbeitsbereichsvorlagenmoduls wird indiziert. • Im Fall eines Gruppenmoduls werden der Titel und die Metadaten der darin enthaltenen Module indiziert. • Der Titel, die Beschreibung und die CUID der InfoObject-Module in BIW werden indiziert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Objekttyp	Indizierter Inhalt
	Hinweis Da nur der Titel und die Beschreibung eines eingebetteten InfoObject-Moduls indiiziert werden, werden beim Versuch, den InfoObject-Inhalt zu durchsuchen, keine Verweise auf das eingebettete Modul zurückgegeben. Wenn z.B. ein Crystal-Reports-Bericht in BIW eingefügt wird, werden sein Titel und seine Beschreibung indiziert. Beim Versuch, nach dem Inhalt des Crystal-Reports-Berichts zu suchen, werden keine Verweise auf die eingebetteten Module zurückgegeben. • Wenn ein BIW mehrere Registerkarten und Unterregisterkarten enthält, werden der Titel und der Inhalt jeder Registerkarte und Unterregisterkarte ebenfalls indiziert.
Crystal-Reports-Berichte im Next-Gen-Format	Titel, Beschreibung, Auswahlformel, gespeicherte Daten, Textfelder in beliebigen Abschnitten, Parameterwerte und Unterberichte. Folgende Objekte in einem Crystal-Reports-Bericht im Next-Gen-Format werden nicht unterstützt: • Kreuztabellenbericht • Diagrammdatenextraktion • Extraktion von Bildern und zugehörigen Metadaten • Eingebettete OLE-Funktionalität (z.B. ein in einen Crystal-Reports-Bericht eingebettetes Word-Dokument) • Extraktion von Flash-Objekten Außerdem ist das seitenweise Lesen von Daten eines Crystal-Reports-Berichts im Next-Gen-Format nicht möglich.
Universum	Dateninhalt kann durchsucht werden. **Hinweis** Die Universumsindizierungsoption ist standardmäßig aktiviert. Wenn Sie bemerken, dass die Ausführung von Abfragen, die von der Plattformsuche zur Indizierung von Universumsinhalten verwendet werden, längere Zeit in Anspruch nimmt und dadurch die Datenbankserverleistung beeinträchtigt, deaktivieren Sie die Universumsindizierungsoption in der

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Objekttyp	Indizierter Inhalt
	Central Management Console (CMC). Ein Beispiel für eine von der Plattformsuche bei der Indizierung von Universumsinhalten verwendete Abfrage ist **Select distinct SampleColumnName from SampleTableName LIMIT 1000**. Führen Sie die folgenden Schritte aus, um die Universumsindizierung zu deaktivieren: 1. Melden Sie sich an der Central Management Console (CMC) an. 2. Wählen Sie **Anwendungen** aus. 3. Navigieren Sie zu den Plattformsuchanwendungen und wählen **Eigenschaften**. 4. Navigieren Sie zu den Inhaltstypen und deaktivieren Sie **Universum**. 5. Wählen Sie **Speichern & schließen**.

Hinweis

Die maximal unterstützte Größe für Drittherstellerdokumente (MAS Office 2003 und 2007 und PDF-Dokumente) beträgt 15 MB.

22.3.3.2 Suchen

Wenn ein Benutzer in BI-Launchpad oder einer anderen Anwendung, die das Plattformsuche-SDK verwendet, nach einem Schlüsselwort sucht, wird der Masterindex nach den Suchbegriffen durchsucht. Auf der Grundlage der Ansichtsrechte des Benutzers zeigt die Such-Engine nur solche Dokumente an, für die der Benutzer über Zugriffsrechte verfügt.

22.3.3.3 Nach der Suche

22.3.3.3.1 Facetten

Die Plattformsuche verfeinert die Suchergebnisse, indem sie sie in Kategorien oder Facetten ähnlicher Objekttypen gruppiert und sie nach der Anzahl der Wiederholungen der Kategorie in den zurückgegebenen Ergebnissen des Suchbegriffs sortiert. Facetten bieten Ihnen die Möglichkeit, zum exakten Ergebnis zu navigieren.

Die Plattformsuche generiert Facetten aus InfoObject-Metadaten, Dokument-Metadaten und Dokumentinhalt. Sie zeigt nur diejenigen Facetten an, die mehr als zwei Dokumente enthalten, die einer angegebenen Abfrage entsprechen. Facetten werden dynamisch auf Basis der Dokumente, die der Suchabfrage entsprechen, angezeigt und nach Dokumentanzahl sortiert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Die Dokumente können in folgende generische Facetten oder Kategorien gruppiert werden:

- Persönlich oder öffentlich (wie etwa Personal, Corporate und Finanzen): Diese basieren auf den BI-Plattform-Dokumentkategorien.
- Dokumenttyp: Diese Kategorie basiert auf dem Dokumenttyp, z.B. Web Intelligence, Crystal Reports, Microsoft Word (2003 und 2007), Microsoft Excel (2003 und 2007) und Dashboards.
- Universen und Verbindungen: Diese basieren auf der Inhaltsquelle.
- Datum: Umfasst das letzte Regenerierungsdatum: (Jahr, Quartal und Monat).
- Zeit: Umfasst die letzte Regenerierungszeit wie die letzten 24 Stunden und letzte Woche.
- Autor: Name des Benutzers, der das Dokument erstellt hat.

22.3.3.3.2 Normalisieren der Rangfolge von Suchergebnissen

Bei der Plattformsuche wird die Stelle des Vorkommens des gesuchten Begriffs für die Rangfolge eines Dokuments berücksichtigt. Der Inhalt wird basierend auf der Stelle seines Vorkommens im Dokument in folgende Kategorien eingeteilt:

1. Plattform-Metadaten
2. Dokument-Metadaten
3. Inhalts-Metadaten
4. Inhalt

Sie können die Gewichtung für diese Kategorien in der CMC konfigurieren.

22.3.3.3.2.1 Anpassen der Gewichtung der Rangfolge von Suchergebnissen

Mit der Plattformsuche können Gewichtungen für in Kategorien gruppierten Inhalten basierend auf dem Vorkommen des Inhalts im Dokument festgelegt werden, indem Sie einen höheren Wert für die gewünschte Kategorie festlegen, um zugehörige Suchergebnisse schneller abzurufen.

Führen Sie folgende Schritte durch, um die Gewichtung festzulegen:

1. Klicken Sie im Bereich *Verwalten* der CMC auf **Anwendungen**.
2. Öffnen Sie **Anwendung zur Plattformsuche**.
3. Wählen Sie **Rangfolge**.

   Die Gewichtungen verschiedener Inhaltskategorien wie Plattformmetadaten, Dokumentmetadaten, Inhaltsmetadaten und Inhalt werden angezeigt. Das *Benutzer-Gebietsschema* ist das in den BI-Launchpad-Einstellungen festgelegte Gebietsschema.
4. Legen Sie die Gewichtungen Ihren Anforderungen entsprechend fest.
5. Wählen Sie **Speichern**.

Wenn in einem Upgradeszenario Rangfolgen für bereits indizierte Dokumente angewendet werden sollen, erstellen Sie den Index erneut. Weitere Informationen zur Neuerstellung des Index finden Sie im Abschnitt *Konfigurieren von Anwendungseigenschaften in der CMC* [Seite 624].

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

22.3.3.3.3 Unterstützung für mehrere Sprachen

Die Plattformsuche bietet Unterstützung für mehrere Sprachen, um Inhalt zu indizieren, Sucherergebnisse abzurufen und Vorschläge in der gewünschten Sprache zu unterbreiten. Um alle nicht lokalisierten BI-Plattform-Dokumente zu indizieren, wird das im **standardmäßigen Index-Gebietsschema** in der CMC festgelegte Gebietsschema verwendet.

Nach der Lokalisierung des InfoObjects wird das Dokument anhand des entsprechenden Sprachanalysierers von der Plattformsuche indiziert.

Die Suche basiert auf dem als Produkt-Gebietsschema des Client festgelegten Gebietsschema. Bei der Plattformsuche wird während des Abrufens der Suchergebnisse mehr Gewicht auf das Produkt-Gebietsschema des Client gelegt. Sie können die Gewichtungen in der CMC konfigurieren.

22.3.3.3.4 Vorschläge

Die Plattformsuche bietet Vorschläge, wenn Suchabfragen falsch geschrieben sind. Wenn die ursprüngliche Suchabfrage zu keinen Ergebnissen führt, schlägt die Plattformsuche die wahrscheinlichsten Begriffe auf Basis des indizierten Inhalts vor.

Vorschläge werden als Schlüsselwörter mit Hyperlinks angezeigt. Klicken Sie auf einen Hyperlink, um eine Liste der Dokumente mit dem Schlüsselwort anzuzeigen, das möglicherweise mit der Originalabfrage übereinstimmt. Diese Vorschläge werden algorithmisch auf Basis verschiedener objektiver Faktoren bestimmt.

Falls mehrere Begriffe vorliegen, die möglicherweise der ursprünglichen Anfrage entsprechen, unterbreitet die Plattformsuche die obersten drei Vorschläge in der Sprache, die in der CMC als **Standardmäßiges Index-Gebietsschema** festgelegt wurde.

> **Hinweis**
>
> In diesen Fällen werden in der Plattformsuche keine Vorschläge erzeugt:
>
> - Falls die Suchabfragen weniger als drei Buchstaben umfassen
> - Für attributierte Suchvorgänge wie "Typ: Crystal-Reports-Bericht"
> - Für Universumsmetadaten und -inhalte
> - Für Multibyte-Sprachen wie Chinesisch, Japanisch und Koreanisch

22.3.3.3.5 Föderieren von Suchergebnissen aus SAP BusinessObjects Explorer

Die Plattformsuche föderiert die Suchanfrage aus SAP BusinessObjects Explorer und Oberflächen-InfoSpaces gemeinsam mit den Inhalten aus der BI-Plattform.

Die Suchergebnisse aus SAP BusinessObjects Explorer werden nach Metadatenkategorien gruppiert. Zu den unterstützten Facetten für InfoSpaces zählen Typ, Speicherort und Regenerierungszeit.

SAP BusinessObjects Explorer sendet die Begriffshäufigkeit zu jedem Suchbegriff in der Suchabfrage an die Plattformsuche. Die Plattformsuche berechnet die Relevanz anhand einer Summe der Quadratwurzel der

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Begriffshäufigkeiten. Der Ergebniswert wird jedem InfoSpace als Punktzahl zugeordnet. Die Ergebnisse werden anschließend nach Punktzahl sortiert und an den Client gesendet.

22.4 Integration der Plattformsuche mit SAP NetWeaver Enterprise Search

SAP NetWeaver Enterprise Search 7.20 und höhere Versionen können einen auf OpenSearch (RSS und ATOM) basierenden Suchdienst verwenden. Suchanforderungen können Remote-Suchdienstproviderrsystemen delegiert werden. In diesem Fall ist OpenSearch der Dienstprovider, NetWeaver Enterprise Search ist der Suchergebnisconsumer und die SAP BusinessObjects-Plattformsuche ist der Suchdienstprovider.

Wenn ein Benutzer eine Suchanforderung sendet, leitet SAP NetWeaver Enterprise Search diese direkt an den OpenSearch-Provider weiter. Der Provider antwortet auf die Suchanforderung und sendet die Antwort an SAP NetWeaver Enterprise Search zurück. Anschließend wird sie mit den Ergebnissen, die aus anderen Suchobjekt-Connectoren abgerufen wurden, zu einem Suchergebnis zusammengeführt und auf der Benutzeroberfläche angezeigt.

Gehen Sie wie folgt vor, um SAP NetWeaver Enterprise Search und die Plattformsuche zu integrieren:

1. Erstellen Sie in SAP NetWeaver Enterprise Search einen Connector.
2. Importieren einer Benutzerrolle in die BI-Plattform

22.4.1 Erstellen eines Connectors in SAP NetWeaver Enterprise Search

Sie können einen Suchobjekt-Connector vom Typ OpenSearch zur Integration externer Suchprovider verwenden, die eine Suchfunktion über OpenSearch bereitstellen.

Zum Erstellen eines Connectors in SAP NetWeaver Enterprise Search ist Folgendes erforderlich:

1. Die URL des OpenSearch-Beschreibungsdiensts.
2. Der OpenSearch-Beschreibungsdienst darf nur im RSS- oder ATOM-Format vorliegen.

Führen Sie die folgenden Schritte aus, um einen Connector in SAP NetWeaver Enterprise Search zu erstellen:

1. Starten Sie das Administrations-Cockpit, und wählen Sie "Create" (Erstellen) aus.
2. Wählen Sie "OpenSearch" als Suchobjekt-Connector-Typ aus.
3. Wählen Sie **Next** (Weiter) aus.
4. Geben Sie die URL des OpenSearch-Beschreibungsdienst für den OpenSearch-Provider ein.
5. Wählen Sie eine der folgenden Authentifizierungseinstellungen zum Starten der Beschreibungsdienst-URL aus:
   - No Authentication (Keine Authentifizierung): Es findet keine Authentifizierung statt.
   - SAP Authentication Assertion Ticket (SAP-Authentifizierungszusicherungsticket): Dieser Benutzer wird über die Einzelanmeldung zur Authentifizierung verwendet.
   - User/Password (Benutzer/Kennwort): Ein vordefinierter Benutzer wird für die Authentifizierung verwendet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

6. Wählen Sie "Launch Search URL" (Such-URL starten) aus den OpenSearch-URL-Einstellungen aus.
   Der OpenSearch-Beschreibungsdienst wird dann für einen geeigneten Suchdienst validiert. Das System gibt automatisch einen Wert für die Such-URL-Vorlage und die zugehörige Beschreibung ein.
7. Wählen Sie eine der folgenden Authentifizierungeinstellungen zum Einrichten eines Connectors aus:
   - No Authentication (Keine Authentifizierung): Es findet keine Authentifizierung statt.
   - SAP Authentication Assertion Ticket (SAP-Authentifizierungszusicherungsticket): Dieser Benutzer wird über die Einzelanmeldung zur Authentifizierung verwendet.
   - User/Password (Benutzer/Kennwort): Ein vordefinierter Benutzer wird für die Authentifizierung verwendet.
8. Wählen Sie **Next** (Weiter) aus.
   Ein zusammenfassendes Dialogfeld mit den für diesen Suchobjekt-Connector eingegebenen Werten wird angezeigt.
9. Wählen Sie **Previous** (Zurück) aus, um die Einstellungen zu ändern, oder **Cancel** (Abbrechen), um alle eingegebenen Daten zu verwerfen.
10. Wählen Sie **Finish** (Fertig stellen) aus, um die Einstellungen zu speichern.

22.4.2 Importieren einer Benutzerrolle in die BI-Plattform

Führen Sie die folgenden Schritte aus, um eine Benutzerrolle in die BI-Plattform zu importieren:

> **Hinweis**
>
> Dem Administrator müssen die Benutzerdetails, Systeminformationen, Anwendungshostinformationen und Benutzeranmeldedaten vorliegen.

1. Wechseln Sie zum Bereich *Authentifizierung* der CMC.
2. Wählen Sie **SAP** aus.
3. Geben Sie Folgendes auf der Registerkarte *Berechtigungssysteme* an:
   - System
   - Client
   - Anwendungsserver
   - Systemnummer
   - Benutzername
   - Kennwort
   - Sprache
4. Wählen Sie **Aktualisieren** aus.
5. Wählen Sie die Registerkarte *Rollenimport*, und importieren Sie Benutzerrollen.
6. Wählen Sie **Aktualisieren** aus.
7. Wählen Sie **Verwalten** > **Benutzersicherheit** in der CMC aus, um die entsprechenden Benutzerrechte zuzuweisen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

22.5 Suchvorgänge über NetWeaver Enterprise Search

Führen Sie die folgenden Schritte aus, um Ergebnisse aus SAP NetWeaver Enterprise Search zu durchsuchen:

1. Melden Sie sich bei SAP NetWeaver Enterprise Search an.
2. Wählen Sie **Erweiterte Suche** aus.
3. Wählen Sie den Connector aus, der für die Plattformsuche erstellt wurde.
4. Suchen Sie nach einem Schlüsselwort.

   Die konsolidierten Ergebnisse für das Schlüsselwort enthalten die Ergebnisse aus der Plattformsuche, sofern eine Übereinstimmung mit dem Schlüsselwort vorliegt.

22.6 Auditing

Alle Ereignisse von Suchanfragen, die von Clientanwendungen gesendet wurden, die den Plattformsuchdienst verwenden, sowie die Suchantwort werden auditiert. Für die Plattformsuche wird das Auditing auf Dienstebene implementiert.

Der Plattformsuchdienst muss mit einem Proxydienst für das Client-Auditing auf demselben Server ausgeführt werden, damit Audit-Ereignisse versendet werden.

Es gibt eine Ereignistyp-ID 1009 für die Plattformsuche und vier für die Plattformsuche spezifische Ereignisdetailtyp-IDs:

- Keyword searched (ID: 19)
- Number of Search Results (ID: 63)
- Facet Search (ID: 20)
- Search Exception (ID: 1)

Neben obigen Ereignisdetails sind einige standardmäßige Ereignisdetails wie "sessionCuid" und "userCuid" vorhanden, die für jedes Auditing in jedem beliebigen BI-Plattform-Modul unterstützt werden.

Im folgenden Beispiel wird erläutert, wie das Auditing in der Plattformsuche funktioniert.

Die Suche nach dem Schlüsselwort "Umsatz" ergibt insgesamt 5 Suchergebnisse. In diesem Fall werden folgende Ereignisse auditiert:

- Ereignistyp-ID 1009
- Ereignisdetailtyp-ID 19 mit dem Wert "Umsatz"
- Ereignisdetailtyp-ID 63 mit dem Wert 5
- Sitzungs-CUID
- Benutzer-CUID
- Status mit Wert 0, was dem erfolgreichen Status entspricht
- Startzeit
- Dauer
- Objekt-ID mit Wert 0, da es sich um Auditing auf Dienstebene handelt

Wenn die Facetten generiert werden und Sie eine oder mehrere Facetten auswählen, werden folgende Ereignisse auditiert:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Ereignistyp-ID 1009
- Ereignisdetailtyp-ID 19 mit dem Wert "Umsatz"
- Ereignisdetailtyp-ID 63 mit dem Wert 5
- Ereignisdetailtyp-ID 20 mit kommagetrennter Zeichenfolge der Facetten
- Sitzungs-CUID
- Benutzer-CUID
- Status mit Wert 0, was dem erfolgreichen Status entspricht
- Startzeit
- Dauer
- Objekt-ID mit Wert 0, da es sich um Auditing auf Dienstebene handelt

Wenn aufgrund eines ungültigen Eintrags, z.B. *"a", eine Suchausnahme auftritt, werden folgende Ereignisdetails auditiert:

- Ereignistyp-ID 1009
- Ereignisdetailtyp-ID 19 mit dem Wert "Umsatz"
- Ereignisdetailtyp-ID 63 mit dem Wert 0
- Ereignisdetailtyp-ID 1 mit der Ausnahmemeldung
- Sitzungs-CUID
- Benutzer-CUID
- Status mit Wert 1, was dem Fehlerstatus entspricht
- Startzeit
- Dauer
- Objekt-ID mit Wert 0, da es sich um Auditing auf Dienstebene handelt

22.7 Fehlerbehebung

22.7.1 Selbstreparatur

Die Plattformsuche verfügt über einen eigenen Selbstreparaturmechanismus. Sie überwacht fortlaufend die Speicherauslastung des Suchdienstes und beendet die Indizierung automatisch, wenn die Speicherauslastung den Schwellenwert übersteigt. Sie wird automatisch wieder gestartet, sobald die Speicherauslastung wieder auf einen annehmbaren Wert gefallen ist. Benutzer können während dieses Prozesses weiterhin Suchvorgänge ausführen, jedoch keine Indizierung über einen bestimmten Zeitraum. Die Plattformsuche konfiguriert auf Basis des Dokumenttyps die Anzahl der Dokumente, die standardmäßig zu einem beliebigen Zeitpunkt indiziert werden können. Die Indizierung wird auf Basis der Systemressourcen wie CPU und Arbeitsspeicher initiiert.

22.7.2 Problemszenarios

In diesem Abschnitt werden die einzelnen Lösungsschritte für eine Reihe von Problemen erläutert, die beim Abrufen von Suchergebnissen mit der Plattformsuche auftreten können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Die Suchergebnisse können nicht aus dem neu hinzugefügten Dokument mit dem Schlüsselwort abgerufen werden

- Prüfen Sie, ob die Plattformsuche den Dokumenttyp des gesendeten Dokuments unterstützt. Wenn der Dokumenttyp nicht unterstützt wird, kann das Dokument nicht indiziert werden.

  Weitere Informationen zu unterstützten Dokumenttypen finden Sie im Thema *Durchsuchbare Inhaltstypen* in den unten aufgeführten verwandten Themen.
- Prüfen Sie die für **Crawling-Frequenz** ausgewählten Optionen. Wenn **Crawling-Frequenz** auf **Kontinuierliches Crawling** festgelegt ist, werden Dokumente umgehend zur Indizierung herangezogen. Wenn **Crawling-Frequenz** auf **Zeitgesteuert verarbeitetes Crawling** festgelegt ist, wird die Indizierung nur während des Zeitrahmens für die zeitgesteuerte Verarbeitung ausgeführt.

  Weitere Informationen zur *Crawling-Frequenz* finden Sie unter dem Thema *Konfigurieren von Anwendungseigenschaften* in den unten aufgeführten verwandten Themen.
- Prüfen Sie die Liste der Indizierungsfehler, um zu prüfen, ob das Dokument erfolgreich indiziert wurde. Wenn das Dokument in der Liste angezeigt wird, müssen Sie es entsprechend bearbeiten und erneut senden, sodass die Plattformsuche das Dokument für die Indizierung heranzieht.

  > **Hinweis**
  >
  > Sie können das Dokument ändern, indem Sie ein Feld hinzufügen oder löschen und das Dokument dann erneut speichern. Dadurch wird der Zeitstempel des Dokuments im BI-Plattform-Repository aktualisiert und die erneute Indizierung des Dokuments initiiert.

  Weitere Informationen zu den Dokumenten, für die die Indizierung nicht durchgeführt werden konnte, finden Sie unter dem Thema *Liste der Indizierungsfehler* in den unten aufgeführten verwandten Themen.
- Prüfen Sie die Ablaufverfolgungsprotokolle des Adaptive Processing Server. Diese enthalten Informationen zu den Indizierungsfehlern.

  1. Wechseln Sie in das Verzeichnis `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\logging\`, das das APS-Ablaufverfolgungsprotokoll mit einer .glf-Erweiterung enthält.
  2. Öffnen Sie die Ablaufverfolgungsprotokoll-Datei, und suchen Sie die SI_ID des Dokuments, die indiziert werden soll.

     > **Hinweis**
     >
     > Die SI_ID des Dokuments ist in den Dokumenteigenschaften enthalten.

Abrufen von Crystal-Reports-Dokumenten nicht möglich

Die Plattformsuche indiziert Crystal-Report-Inhalte nur für die Versionen 2008, 2011 und 2013. Sie indiziert keine Inhalte aus Crystal Reports für Enterprise.

Sie können jedoch bei Crystal Reports für Enterprise nach den Metadaten des Dokuments suchen, z.B. Titel, Beschreibung und Schlüsselwort, die Dokumenteigenschaften sind.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wenn das Dokument indizierbaren Inhalt enthält, müssen Sie dasselbe Verfahren wie oben unter *Die Suchergebnisse können nicht aus dem neu hinzugefügten Dokument mit dem Schlüsselwort abgerufen werden* beschrieben befolgen.

InfoSpaces von SAP BusinessObjects Explorer können nicht abgerufen werden

Überprüfen Sie, ob SAP BusinessObjects Explorer-Server gestoppt oder deaktiviert wurden. Aktivieren Sie die Server für die Plattformsuche, um die Suchergebnisse aus SAP BusinessObjects Explorer abzurufen.

SAP NetWeaver Enterprise Search kann Ergebnisse nicht aus dem BI-Plattform-Repository abrufen.

- Überprüfen Sie, ob die Plattformsuche die Suchergebnisse mithilfe von BI-Launchpad abruft, um herauszufinden, ob das Problem auf die Integration der Plattformsuche in SAP NetWeaver Enterprise Search zurückzuführen ist.
- Überprüfen Sie, ob OpenSearch korrekt auf dem Webanwendungsserver implementiert ist. Welche Schritte zur Validierung der OpenSearch-Implementierung genau auszuführen sind, hängt vom Typ des verwendeten Webanwendungsservers ab.
- Überprüfen Sie, ob der Connector in der SAP NetWeaver Enterprise Search-Konfiguration korrekt erstellt bzw. konfiguriert wurde. Sie müssen den richtigen Connector für SAP NetWeaver Enterprise Search verwenden, damit Ergebnisse aus der Plattformsuche föderiert werden können.
- Überprüfen Sie, ob die Rechner, auf denen SAP NetWeaver Enterprise Search und die BI-Plattform jeweils ausgeführt werden, korrekt miteinander kommunizieren. Falls in einer verteilten Umgebung Netzwerkprobleme vorliegen, kann SAP NetWeaver Enterprise Search die Ergebnisse unter Umständen nicht föderieren.
- Überprüfen Sie, ob Benutzer von SAP NetWeaver Enterprise Search mit den entsprechenden Rechten der BI-Plattform hinzugefügt wurden. Gehen Sie zur Validierung der Benutzerrechte zum Bereich **Authentifizierung** der CMC, und wählen Sie **SAP** aus.

Weitere Informationen

Liste der Indizierungsfehler [Seite 743]
Konfigurieren von Anwendungseigenschaften in der CMC [Seite 624]
Durchsuchbare Inhaltstypen [Seite 744]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

23 Föderation

23.1 Föderation

Föderation ist ein standortübergreifendes Replikationstool für den Einsatz mehrerer BI-Plattform-Implementierungen in einer globalen Umgebung.

Inhalt kann über eine BI-Plattform-Implementierung erstellt und verwaltet und nach einem wiederkehrenden Zeitplan über geografische Standorte hinweg in andere BI-Plattform-Implementierungen repliziert werden. Sie können Aufträge sowohl mit einseitiger Replikation als auch mit beidseitiger Replikation ausführen.

Die Verwendung von Föderation bietet folgende Vorteile:

- Reduzierter Netzwerkverkehr
- Erstellen und Verwalten von Inhalten an einem zentralen Ort
- Optimieren der Leistung für Endbenutzer

Das Replizieren von Inhalten mithilfe von Föderation bietet folgende Möglichkeiten:

- Vereinfachen der Verwaltungsanforderungen für mehrere Implementierungen
- Bereitstellen von Richtlinien zur Vergabe konsistenter Rechte für mehrere Niederlassungen in weltweiten Unternehmen
- Schnellerer Informationsabruf und Verarbeitung von Berichten an Remotesites, auf denen sich die Daten befinden
- Zeitersparnis durch schnelleres Abrufen lokaler und verteilter Daten
- Synchronisieren von Inhalten aus mehreren Implementierungen, ohne dass benutzerdefinierter Code erforderlich ist

Mit der Föderation können Sie separate Sicherheitsmodelle, Lebenszyklen, Test- und Implementierungszeiten sowie unterschiedliche Geschäftseigentümer und Administratoren verwalten. Beispielsweise können Sie Administrationsfunktionen delegieren, durch die der Administrator der Vertriebsanwendung daran gehindert wird, eine Anwendung der Personalabteilung zu ändern.

Mit Föderation können Sie eine Vielzahl von Objekten replizieren, wie in der folgenden Tabelle beschrieben.

Kategorie	Replizierbare Objekttypen	Zusätzliche Hinweise
Business Views	Business View Manager, DataConnection, Wertelisten, Datengrundlage usw.	Alle Objekte werden unterstützt, wenn auch nicht auf ihrer jeweiligen Ebene.
Berichte	Crystal-Reports-Berichte, Web Intelligence und Dashboard Design	Full Client-Add-In und Vorlagen werden unterstützt.
Drittanbieter-Objekte	Excel-, PDF-, PowerPoint-, Flash-, Word, Text-, RTF- und Shockwave Flash-Dateien	
Benutzer	Benutzer, Gruppen, Posteingang, Favoriten und Persönliche Kategorie	
BI-Plattform	Ordner, Ereignisse, Kategorien, Kalender, Zugriffsberechtigungen,	

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Kategorie	Replizierbare Objekttypen	Zusätzliche Hinweise
	Hyperlinks, Verknüpfungen, Programme, Profile, Objektpakete, Agnostisch	
Universum	Universum, Verbindungen und Universumszugriffsbeschränkung	

In den folgenden Szenarios werden zwei Beispiele für die Verwendung von Föderation im Unternehmen beleuchtet.

Szenario 1: Einzelhandel (zentralisiertes Design)

ACME möchte unter Verwendung der einseitigen Replikationsmethode monatliche Umsatzberichte an alle Filialen senden. Der Administrator auf der ursprünglichen Website erstellt einen Bericht, der von Administratoren auf den einzelnen Zielwebsites repliziert und gegen die Datenbank der jeweiligen Filiale ausgeführt wird.

> **Tipp**
>
> Lokalisierte Instanzen können an die ursprüngliche Website zurückgesendet werden, von der die replizierten Informationen jedes Objekts verwaltet werden. Beispielsweise werden das geeignete Logo, die entsprechenden Verbindungsinformationen für die Datenbank usw. angewendet.

Szenario 2: Remotezeitplan (verteilter Zugriff)

Die Daten befinden sich auf der ursprünglichen Website. Ausstehende Replikationsaufträge werden zur Ausführung an die ursprüngliche Website gesendet. Abgeschlossene Replikationsaufträge werden dann zur Anzeige an die Zielwebsites zurückgesendet. Beispiel: Die Daten für einen Bericht sind auf der Zielwebsite u.U. nicht verfügbar, der Benutzer kann jedoch festlegen, dass die Berichte auf der ursprünglichen Website ausgeführt werden, bevor der abgeschlossene Bericht wieder an die Zielwebsite gesendet wird.

23.2 Begriffe in Föderation

In der folgenden Liste werden Begriffe und Ausdrücke in Bezug auf Föderation eingeführt, die beim Navigieren und Verwenden von Föderation Unterstützung bieten können:

BI-Anwendung	Die logische Gruppierung verwandter BI-Inhalte, die einen speziellen Verwendungszweck und eine bestimmte Zielgruppe haben. Eine BI-Anwendung ist kein Objekt. Von einer BI-Plattform-Implementierung können mehrere BI-Anwendungen gehostet werden, die über getrennte Sicherheitsmodelle, Lebenszyklen, Test- und Implementierungszeitachsen sowie Business-Eigentümer und -Administratoren verfügen können.
Zielwebsite	Ein BI-System, das replizierte BI-Inhalte von einer Ursprungswebsite abruft.
Lokal	Das lokale System, über das ein Benutzer oder Administrator verbunden ist. Der Administrator einer Zielwebsite wird von der Zielwebsite beispielsweise als zum “lokalen” System gehörig angesehen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Lokal ausgeführte abgeschlossene Instanzen	Instanzen, die auf der Zielwebsite verarbeitet und dann an die ursprüngliche Website zurückgesendet werden.
Mehrere ursprüngliche Websites	Mehrere Websites können als ursprüngliche Website fungieren. Beispielsweise können mehrere Entwicklungszentren grundsätzlich über mehrere ursprüngliche Websites verfügen. Pro Replikation kann jedoch nur eine ursprüngliche Website vorhanden sein.
Einseitige Replikation	Objekte werden nur in eine Richtung repliziert, und zwar von der ursprünglichen Website auf die Zielwebsite. Alle an einer Zielwebsite vorgenommenen Aktualisierungen verbleiben auf dieser Zielwebsite.
Ursprüngliche Website	Das BI-System, aus dem der Inhalt stammt.
Remotesite	Ein System, das für einen Benutzer nicht "lokal" ist. Die ursprüngliche Website wird von Benutzern und Administratoren der Zielwebsite beispielsweise als " Remotesite" angesehen.
Remoteverbindung	Ein Objekt mit Informationen, die zum Herstellen einer Verbindung mit einer BI-Plattform-Implementierung verwendet werden, einschließlich Benutzername und Kennwort, CMS-Name, Webdienst-URI und Bereinigungsoptionen.
Remote-Zeitsteuerung	Zeitsteuerungsanforderungen, die von der Zielwebsite an die ursprüngliche Website gesendet werden. Berichte auf Zielwebsites können remote zeitgesteuert verarbeitet werden, wobei die Berichtsinstanz zur Verarbeitung zurück an die ursprüngliche Website gesendet wird. Anschließend wird die abgeschlossene Instanz wieder an die Zielwebsite gesendet.
Replikation	Das Kopieren von Inhalten aus einem BI-Plattform-System in ein anderes.
Replikationsauftrag	Ein Objekt, das Informationen über die Zeitsteuerung der Replikation enthält, welche Inhalte repliziert werden sollen sowie spezielle Bedingungen, die beim Replizieren von Inhalten berücksichtigt werden sollten.
Replikationsliste	Eine Liste der zu replizierenden Objekte. Die Replikationsliste verweist auf andere Inhalte wie Benutzer, Gruppen, Berichte usw. in der BI-Plattform-Implementierung, die zusammen repliziert werden sollen.
Replikationsobjekt	Ein Objekt, das von einer ursprünglichen Website auf eine Zielwebsite repliziert wird. Alle replizierten Objekte auf einer Zielwebsite werden durch ein Replikationssymbol gekennzeichnet. Wenn ein Konflikt eintritt, werden die Objekte durch ein Konfliktsymbol gekennzeichnet.
Replikationspaket	Das Replikationspaket wird während der Übertragung erstellt und enthält Objekte aus einem Replikationsauftrag. Es kann alle in der Replikationsliste definierten Objekte enthalten, wie dies bei sich ständig ändernden Umgebungen bzw. bei der Erstreplikation der Fall ist. Alternativ kann das Paket eine Teilmenge der Replikationsliste enthalten, wenn die Objekte im Vergleich zum Zeitplan des Replikationsauftrags selten geändert werden. Das Replikationspaket wird als BIAR-Datei (BI Application Resource) implementiert.
Replikationsregenerierung	Alle Objekte in einer Replikationsliste werden unabhängig von der zuletzt geänderten Version regeneriert.
Beidseitige Replikation	Funktioniert genauso wie die einseitige Replikation, bei der beidseitigen Replikation werden die Änderungen jedoch in beide Richtungen gesendet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Aktualisierungen auf der ursprünglichen Website werden auf die einzelnen Zielwebsites repliziert. Aktualisierungen und neue Objekte auf einer Zielwebsite werden an die ursprüngliche Website gesendet.

23.3 Verwalten von Sicherheitsrechten

Da durch Föderation Inhalte zwischen unterschiedlichen Implementierungen repliziert werden und außerdem eine Zusammenarbeit mit anderen Administratoren erforderlich ist, ist es wichtig, die Funktionsweise der Sicherheitsfeatures vor der Verwendung von Föderation zu verstehen.

Administratoren in unterschiedlichen Implementierungen müssen ihre Arbeit abstimmen, bevor Föderation aktiviert werden kann. Nach der Replikation der Inhalte können diese durch Administratoren geändert werden.

Sie benötigen spezifische Rechte auf der Implementierung der ursprünglichen Webste und der Zielwebsite, um bestimmte Aufgaben durchzuführen:

- Für die ursprüngliche Website erforderliche Rechte
- Für die Zielwebsite erforderliche Rechte
- Für Föderation-spezifische Objekte erforderliche Rechte
- Föderation-Szenarios

Tipp

Es wird empfohlen, dieses Kapitel vor dem Starten von Föderation zu lesen.

23.3.1 Für die ursprüngliche Website erforderliche Rechte

In diesem Abschnitt werden die Aktionen beschrieben, die auf der ursprünglichen Website ausgeführt werden, sowie die erforderlichen Rechte des Benutzerkontos, über das die Verbindung zur ursprünglichen Website hergestellt wird. Hierbei handelt es sich um das Konto, das Sie in das Remoteverbindungsobjekt auf der Zielwebsite eingeben.

Aktion	Beschreibung	Erforderliche Rechte
Einseitige Replikation	Ausführen einer ausschließlichen Replikation von der ursprünglichen auf die Zielwebsite. **Hinweis** “Ansichts”- und “Replikationsrechte” sind für alle replizierten Objekte erforderlich, einschließlich Objekte, die durch Abhängigkeitsberechnungen automatisch repliziert werden.	• “Ansichts”- und “ Replikationsrechte” für alle zu replizierenden Objekte • “Ansichtsrecht” für die Replikationsliste

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Aktion	Beschreibung	Erforderliche Rechte
Beidseitige Replikation	Ausführen einer Replikation von der ursprünglichen auf die Zielwebsite und von der Zielwebsite auf die ursprüngliche Website.	• "Ansichts"- und " Replikationsrechte" für alle zu replizierenden Objekte • "Ansichtsrecht" für die Replikationsliste • "Änderungsrechte" für Benutzerobjekte zum Replizieren von Kennwortänderungen
Zeitgesteuerte Verarbeitung	Ermöglichen der Remote-Zeitsteuerung von der Zielwebsite aus auf die ursprüngliche Website.	• "Zeitsteuerungsrechte" für alle Objekte, die Sie entfernt zeitgesteuert verarbeiten möchten.

Weitere Informationen

Für die Zielwebsite erforderliche Rechte [Seite 760]

23.3.2 Für die Zielwebsite erforderliche Rechte

In diesem Abschnitt werden die Aktionen beschrieben, die auf die Zielwebsite angewendet werden, sowie die erforderlichen Rechte des Benutzerkontos, über das der Replikationsauftrag ausgeführt wird. Hierbei handelt es sich um das Konto des Benutzers, der den Replikationsauftrag erstellt hat.

> **Hinweis**
>
> Replikationsaufträge können wie alle anderen Objekte, die zeitgesteuert verarbeitet werden können, in Vertretung eines anderen Benutzers zeitgesteuert verarbeitet werden.

Aktion	Beschreibung	Erforderliche Rechte
Alle Objekte	Repliziert sowohl Objekte mit einseitiger als auch mit beidseitiger Replikation.	• "Ansichts"-, "Hinzufüge"-, " Bearbeitungs"- und " Änderungsrechte" für alle Objekte • " Benutzerkennwortänderungsrecht" für alle Benutzerobjekte
Erstmalige Replikation	Bei der ersten Ausführung des Replikationsauftrags ist noch kein Objekt auf der Zielwebsite vorhanden. Daher benötigt das Benutzerkonto, unter dem der Replikationsauftrag ausgeführt wird, Rechte für alle Ordner auf oberster Ebene sowie für Objekte, denen Inhalt hinzugefügt wird.	• "Ansichts-", "Hinzufüge-"," Bearbeitungs-" und " Rechteänderungsrechte" für alle Ordner auf oberster Ebene sowie Standardobjekte

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Für die ursprüngliche Website erforderliche Rechte [Seite 759]

23.3.3 Föderation-spezifische Rechte

In diesem Abschnitt werden spezifische Föderation-Szenarios erläutert.

Aktion	Beschreibung	Erforderliche Rechte
Objektbereinigung	Die Objektbereinigung löscht Objekte auf der Zielwebsite.	• Das Konto, unter dem der Replikationsauftrag ausgeführt wird, benötigt "Löschrechte" für alle Objekte, die möglicherweise gelöscht werden.
Deaktivieren der Bereinigung für bestimmte Objekte	Beim Replizieren bestimmter Objekte von der ursprünglichen Website möchten Sie vielleicht verhindern, dass sie beim Löschen von der ursprünglichen Website auch von der Zielwebsite gelöscht werden. Zu diesem Zweck können Sie Rechte verwenden. Beispielsweise wählen Sie diese Option, wenn Benutzer auf der Zielwebsite ein Objekt unabhängig von den Benutzern auf der ursprünglichen Website verwenden. Beispiel: In einem replizierten Universum, in dem Benutzer auf der Zielwebsite eigene lokale Berichte unter Verwendung dieses Universums erstellen, soll das Universum auf der Zielwebsite erhalten bleiben, wenn es auf der ursprünglichen Website gelöscht wird.	• Verweigern Sie dem Benutzerkonto, unter dem der Replikationsauftrag ausgeführt wird, für die beizubehaltenden Objekte "Löschrechte".
Aktivieren der beidseitigen Replikation ohne Änderungen an der ursprünglichen Website	Unter bestimmten Umständen möchten Sie vielleicht die beidseitige Replikation verwenden und gleichzeitig verhindern, dass bestimmte Objekte auf der ursprünglichen Website geändert werden, obwohl sie auf der Zielwebsite geändert wurden. Ein Grund dafür könnte darin liegen, dass es sich um ein spezielles Objekt handelt, das nur von	• Verweigern Sie dem für die Verbindung verwendeten Benutzerkonto im Remoteverbindungsobjekt die " Bearbeitungsrechte".

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Aktion	Beschreibung	Erforderliche Rechte
	Benutzern auf der ursprünglichen Website geändert werden soll, oder dass Sie die Remote-Zeitsteuerung aktivieren möchten, ohne Änderungen zurückzuübertragen. **Hinweis** Bei der Remote-Zeitsteuerung können Sie einen Auftrag erstellen, durch den ausschließlich Objekte für die Remote-Zeitsteuerung verarbeitet werden. In diesem Fall werden Vorgängerobjekte jedoch trotzdem repliziert, einschließlich des Berichts, des Ordners, in dem der Bericht enthalten ist, sowie dessen übergeordneter Ordner. Alle an der Zielwebsite vorgenommenen Änderungen werden an die ursprüngliche Website zurückgesendet, und Änderungen an der ursprünglichen Website werden an die Zielwebsite gesendet.	

23.3.4 Replizieren der Sicherheit eines Objekts

Um die Sicherheitsrechte für ein Objekt beizubehalten, muss sowohl das Objekt als auch dessen Benutzer bzw. Gruppe gleichzeitig repliziert werden. Falls nicht, müssen sie auf der Website, auf die repliziert wird, bereits vorhanden sein und auf jeder Website über eindeutige CUIDs verfügen.

Wenn ein Objekt ohne Benutzer bzw. Gruppe repliziert wird oder diese auf der Website, auf die repliziert wird, noch nicht vorhanden sind, werden die Rechte ungültig.

Beispiel

Gruppe A und Gruppe B wurden Rechte für Objekt A zugewiesen. Gruppe A wurden “Ansichtsrechte” gewährt, und Gruppe B wurden “Ansichtsrechte” verweigert. Wenn der Replikationsauftrag lediglich Gruppe A und Objekt A repliziert, sind Objekt A auf der Zielwebsite lediglich “Ansichtsrechte” für Gruppe A zugeordnet.

Wenn Sie ein Objekt replizieren, besteht ein Sicherheitsrisiko, falls nicht alle Gruppen mit expliziten Rechten für das Objekt repliziert werden. Im oben aufgeführten Beispiel entsteht ein potenzielles Risiko. Wenn Benutzer A sowohl Gruppe A als auch Gruppe B angehört, ist er nicht berechtigt, Objekt A auf der ursprünglichen Website anzeigen zu lassen. Benutzer A wird jedoch auf die Zielwebsite repliziert, da er beiden Gruppen angehört. Sobald er auf der Website enthalten ist, und da Gruppe B nicht repliziert wurde, hat Benutzer A das Recht, Objekt A auf der Zielwebsite anzeigen zu lassen, ist aber nicht berechtigt, Objekt A auf der ursprünglichen Website einzusehen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Objekte, die auf andere, nicht in einem Replikationsauftrag eingeschlossene Objekte verweisen sowie Objekte, die nicht schon auf der Zielwebsite vorhanden sind, werden in einer Protokolldatei angezeigt. In der Protokolldatei wird angezeigt, dass von dem Objekt auf das nicht replizierte Objekt verwiesen und der Verweis entfernt wurde.

Die Sicherheit eines Objekts für einen bestimmten Benutzer oder eine bestimmte Gruppe wird nur von der ursprünglichen Website auf die Zielwebsite repliziert. Obwohl Sicherheitseinstellungen für replizierte Objekte auf der Zielwebsite festgelegt werden können, werden sie nicht auf die ursprüngliche Website repliziert.

23.3.5 Replizieren der Sicherheit durch Zugriffsberechtigungen

Um fortzubestehen, müssen Rechte von Zugriffsberechtigungen definiert werden. Objekt, Benutzer oder Gruppe und Zugriffsberechtigung müssen gleichzeitig repliziert werden, oder sie müssen auf der Website, auf die repliziert wird, bereits vorhanden sein.

Objekte, die einem Benutzer oder einer Gruppe explizite Rechte zuweisen, die nicht im Replikationsauftrag oder noch nicht auf der Zielwebsite enthalten sind, werden in der zugehörigen Protokolldatei angezeigt, in der aufgeführt ist, welche zugewiesenen Objektrechte nicht repliziert und welche Rechte verworfen wurden.

Außerdem können Sie für ein importiertes Objekt verwendete “Zugriffsberechtigungen” automatisch replizieren lassen. Diese Option ist für die Replikationsliste verfügbar.

> **Hinweis**
>
> Standardzugriffsberechtigungen werden nicht repliziert, Verweise bleiben jedoch erhalten.

23.4 Optionen für Replikationstypen und Replikationsmodi

Abhängig vom ausgewählten Replikationstyp und Replikationsmodus können Sie eine von vier unterschiedlichen Replikationsauftragsoptionen erstellen:

- Einseitige Replikation
- Beidseitige Replikation
- Von ursprünglicher Website aus regenerieren
- Von Ziel aus regenerieren

23.4.1 Einseitige Replikation

Bei der einseitigen Replikation können Inhalte nur in einer Richtung repliziert werden: von der ursprünglichen Website auf eine Zielwebsite. Alle Änderungen, die an Objekten in der Replikationsliste auf der ursprünglichen Website vorgenommen wurden, werden an die Zielwebsite gesendet. Änderungen, die an Objekten auf einer Zielwebsite vorgenommen wurden, werden allerdings nicht an die ursprüngliche Website zurückgesendet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Die einseitige Replikation eignet sich besonders für Implementierungen mit einer zentralen BI-Plattform-Implementierung, in der Objekte erstellt, geändert und verwaltet werden. Andere Implementierungen verwenden den Inhalt der zentralen Implementierung.

Zum Erstellen einer einseitigen Replikation wählen Sie die folgenden Optionen:

- Replikationstyp = Einseitige Replikation
- Replikationsmodus = Normale Replikation

23.4.2 Beidseitige Replikation

Mit der beidseitigen Replikation können Sie Inhalte in beide Richtungen zwischen ursprünglicher und Zielwebsite replizieren. Alle an den Objekten auf der ursprünglichen Website vorgenommenen Änderungen werden auf den Zielwebsites repliziert, und Änderungen auf einer Zielwebsite werden auf der ursprünglichen Website repliziert.

> **Hinweis**
>
> Zum Ausführen einer Remote-Zeitsteuerung und zum Replizieren lokal ausgeführter Instanzen an die ursprüngliche Website muss der beidseitige Replikationsmodus ausgewählt werden.

Falls Sie über mehrere BI-Plattform-Implementierungen verfügen, in denen Inhalte an beiden Standorten erstellt, geändert, verwaltet und verwendet werden, stellt die beidseitige Replikation die effizienteste Lösung dar. Außerdem erleichtert sie die Synchronisierung der Implementierungen.

Zum Erstellen einer beidseitigen Replikation wählen Sie die folgenden Optionen:

- Replikationstyp = Beidseitige Replikation
- Replikationsmodus = Normale Replikation

Weitere Informationen

Remote-Zeitsteuerung und lokale Ausführung von Instanzen [Seite 790]

23.4.3 "Von ursprünglicher Website aus aktualisieren" oder "Von Ziel aus aktualisieren"

Bei der Replikation von Inhalten im einseitigen oder beidseitigen Replikationsmodus werden die Objekte in der Replikationsliste auf eine Zielwebsite repliziert. Allerdings werden u.U. nicht immer alle Objekte repliziert, wenn der Replikationsauftrag ausgeführt wird.

Föderation verfügt über eine Optimierungs-Engine, die Sie dabei unterstützt, Ihre Replikationsaufträge schneller abzuschließen. Die Engine verwendet eine Kombination aus Objektversion und -zeitstempel, um festzustellen, ob das Objekt seit der letzten Replikation geändert wurde. Diese Überprüfung wird auf speziell aus der Replikationsliste ausgewählte Objekte sowie auf Objekte angewendet, die während der Abhängigkeitsprüfung repliziert wurden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

In einigen Fällen werden Objekte von der Optimierungs-Engine jedoch nicht berücksichtigt, sodass sie nicht repliziert werden. In diesen Fällen können Sie den Replikationsauftrag durch “Von ursprünglicher Website aus regenerieren” und “Von Ziel aus regenerieren” zwingen, Inhalte und deren Abhängigkeiten unabhängig von den Zeitstempeln zu replizieren.

Durch "Von ursprünglicher Website aus aktualisieren" werden Inhalte nur von der ursprünglichen Website an Zielwebsites gesendet. Durch "Von Ziel aus aktualisieren" werden Inhalte nur von den Zielwebsites an die ursprüngliche Website gesendet.

Beispiel

In den folgenden drei Beispielen werden Szenarios beschrieben, in denen “Von ursprünglicher Website aus regenerieren” und “Von Ziel aus regenerieren” verwendet und bestimmte Objekte aufgrund der Optimierung ausgelassen werden.

Szenario 1: Objekte, die andere Objekte enthalten, werden einem Bereich hinzugefügt, der repliziert wird.

Ordner A wird von der ursprünglichen Website auf die Zielwebsite repliziert. Jetzt ist der Ordner auf beiden Websites vorhanden. Ein Benutzer verschiebt oder kopiert Ordner B mit Bericht B in Ordner A auf der ursprünglichen Website. Während der nächsten Replikation stellt Föderation fest, dass der Zeitstempel von Ordner B geändert wurde und repliziert den Ordner auf die Zielwebsite. Der Zeitstempel von Bericht B wird jedoch nicht geändert. Aus diesem Grund wird er bei einem normalen einseitigen oder beidseitigen Replikationsauftrag nicht mitrepliziert.

Um sicherzustellen, dass der Inhalt von Ordner B ordnungsgemäß repliziert wird, sollte ein Replikationsauftrag mit der Option “Von ursprünglicher Website aus regenerieren” nur einmal verwendet werden. Danach werden normale einseitige oder beidseitige Replikationsaufträge ordnungsgemäß repliziert. Wird dieses Beispiel umgekehrt und Ordner B von der Zielwebsite verschoben oder kopiert, sollten Sie “Von Ziel aus regenerieren” verwenden.

Szenario 2: Neue Objekte werden über den LifeCycle Manager oder die BIAR-Befehlszeile hinzugefügt.

Wenn Sie einem zu replizierenden Bereich mit dem LifeCycle Manager oder über die BIAR-Befehlszeile Objekte hinzufügen, werden Objekte während eines normalen einseitigen oder beidseitigen Replikationsauftrags u.U. nicht ausgewählt. Dies kann passieren, wenn die internen Systemuhren des Quell- und Zielsystems bei der Verwendung des LifeCycle Managers oder der BIAR-Befehlszeile nicht synchronisiert sind.

Hinweis

Nach dem Import neuer Objekte in einen Bereich, der auf der ursprünglichen Website repliziert wird, wird empfohlen, einen Replikationsauftrag mit der Option “Von ursprünglicher Website aus regenerieren” auszuführen. Nach dem Import neuer Objekte in einen Bereich, der auf der Zielwebsite repliziert wird, wird empfohlen, einen Replikationsauftrag mit der Option “Von Ziel aus regenerieren” auszuführen.

Szenario 3: Zwischen geplanten Replikationszeiten.

Wenn Sie einem zu replizierenden Bereich Objekte hinzufügen und nicht bis zum nächsten geplanten Replikationstermin warten können, können Sie einen Replikationsauftrag mit der Option “Von ursprünglicher Website aus regenerieren” bzw. “Von Ziel aus regenerieren” verwenden. Durch die Auswahl des Bereichs, dem Objekte hinzugefügt wurden, können Inhalte schnell repliziert werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Hinweis

Da dieses Szenario bei umfangreichen Replikationslisten aufwändig sein kann, wird davon abgeraten, diese Option häufig einzusetzen. Beispielsweise ist es nicht erforderlich, Replikationsaufträge zu erstellen, um stündliche Regenerierungen von der ursprünglichen auf die Zielwebsite auszuführen. Diese Modi sollten bei “ sofortiger Ausführung” bzw. in seltener ausgeführten Zeitsteuerungen eingesetzt werden.

Hinweis

In einigen Fällen kann keine Konfliktauflösung verwendet werden: “Von ursprünglicher Website aus regenerieren” – die Option "Zielwebsite hat Vorrang" ist blockiert, oder “Von Ziel aus regenerieren” – die Option "Ursprüngliche Website hat Vorrang" ist blockiert.

23.5 Replizieren von Drittthersteller-Benutzern und -Gruppen

Föderation bietet die Möglichkeit, Benutzer und Gruppen von Drittherstellern, insbesondere AD und LDAP, zu replizieren.

Tipp

Wenn Sie beabsichtigen, diese Benutzer- und Gruppentypen oder deren persönliche Inhalte, wie Favoritenordner oder Posteingänge, zu replizieren, sollten Sie diesen Abschnitt lesen.

Zuordnen von Benutzern und Gruppen

1. Ordnen Sie Gruppen und Benutzer auf der ursprünglichen Website zu, damit sie von Föderation ordnungsgemäß repliziert werden können.
2. Replizieren Sie die zugeordneten Benutzer und Gruppen auf die Zielwebsite.

Hinweis

Gruppen und Benutzer sollten nicht getrennt auf der Zielwebsite zugeordnet werden. Andernfalls haben sie auf der Zielwebsite und der ursprünglichen Website unterschiedliche eindeutige Bezeichner (CUIDs), sodass Föderation nicht in der Lage ist, Benutzer oder Gruppen in Übereinstimmung zu bringen.

Beispiel

Der Administrator ordnet Gruppe A mit Benutzer A auf der ursprünglichen Website und der Zielwebsite zu. Sowohl Gruppe A als auch Benutzer A verfügen auf der ursprünglichen und der Zielwebsite über unterschiedliche eindeutige Bezeichner. Da sie während der Replikation von Föderation nicht zugeordnet werden können, werden Gruppe A oder Benutzer A aufgrund eines Aliaskonflikts nicht repliziert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Die Zielwebsite muss vor der Replikation von Benutzern und Gruppen von Drittherstellern für die Verwendung der AD- oder LDAP-Authentifizierung eingerichtet sein. Die Zielwebsite muss jedoch auch für die Verwendung von AD oder LDAP konfiguriert werden, um die Kommunikation mit dem Verzeichnisserver oder Domänencontroller zu ermöglichen.

> **Hinweis**
>
> Nachdem eine AD- oder LDAP-Gruppe erstmalig repliziert wurde, können sich Benutzer in dieser Gruppe erst anmelden, nachdem das AD/LDAP-Gruppendiagramm regeneriert wurde. Dieser Vorgang wird ca. alle 15 Minuten automatisch ausgeführt. Um das AD/LDAP-Gruppendiagramm manuell zu regenerieren, rufen Sie die Seite *Authentifizierung* der CMC auf, doppelklicken auf **Windows AD** oder **LDAP** und klicken dann auf **Aktualisieren**.

> **Hinweis**
>
> Beim Replizieren von Drittherstellergruppen ist Vorsicht geboten. Wenn Sie der Gruppe im Verzeichnisserver neue Benutzer hinzufügen, können sie sich bei beiden Websites anmelden. Dieses Sicherheitsproblem der AD- oder LDAP-Authentifizierung ist von Föderation unabhängig.
>
> Wenn Sie sich bei der Zielwebsite und der ursprünglichen Website getrennt anmelden oder die Gruppenmitgliedschaft mithilfe der Aktualisierungsschaltfläche auf der Seite für die CMC-Authentifizierung auf beiden Websites aktualisiert wird, wird auf beiden Websites ein Benutzerkonto erstellt. Die Konten verfügen über unterschiedliche CUIDs, und Föderation ist nicht in der Lage, diese ordnungsgemäß zu replizieren.
>
> Achten Sie unbedingt darauf, das Konto nur auf einer Website zu erstellen und dann auf die andere Website zu replizieren.

23.6 Replizieren von Universen und Universumsverbindungen

Für die Replikation von Universen zwischen BI-Plattform-Implementierungen unter Verwendung von Föderation ist eine gründliche Vorausplanung unerlässlich. Ein Universumsobjekt ist ohne eine zugrunde liegende Universumsverbindung nicht funktionsfähig.

Universumsverbindungsobjekte enthalten Informationen, die für die Verbindung zu einer Berichtsdatenbank erforderlich sind. Für eine korrekte Funktionsweise müssen die Universumsverbindungsobjekte gültige Informationen enthalten und die Einrichtung einer Datenbankverbindung ermöglichen.

> **Hinweis**
>
> Wenn Sie die beidseitige Replikation verwenden und ein Universum ohne Universumsverbindung von der ursprünglichen Website auf die Zielwebsite replizieren, kann die Beziehung zwischen dem Universum der ursprünglichen Website und der Universumsverbindung auf der ursprünglichen Website in nachfolgenden Replikationen überschrieben oder entfernt werden. Um dies zu verhindern, sollten Universumsverbindungen immer mit den Universen repliziert werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Um sicherzustellen, dass abhängige Universumsverbindungen mit den Universen repliziert werden, wählen Sie beim Erstellen oder Ändern der Replikationsliste, die das Universum enthält, immer folgende Optionen aus:

- **Von ausgewählten Universen verwendete Verbindungen einschließen**
- **Von ausgewählten Universen benötigte Universen einschließen**

> **Hinweis**
>
> Wenn die Beziehung eines Universums zur Universumsverbindung überschrieben oder entfernt wurde, öffnen Sie das Universum im Universe Designer und ändern die Verbindungsinformationen unter **Datei** > **Parameter** > .

Anhand der folgenden beiden Beispiele wird das Replizieren von Universen und der zugehörigen Universumsverbindungen veranschaulicht.

> **Beispiel**
>
> Wenn Sie Universen und Universumsverbindungen replizieren, sollten Sie sicherstellen, dass die Verbindungsumgebung auf der ursprünglichen Website mit der Verbindungsumgebung auf der Zielwebsite übereinstimmt.
>
> Wenn die Universumsverbindung beispielsweise eine ODBC-Verbindung mit dem Namen “TestODBC” verwendet, muss eine korrekt konfigurierte ODBC-Verbindung mit dem Namen “TestODBC” in der Zielumgebung vorhanden sein. Die ODBC-Verbindung kann in dieselbe Datenbank oder eine andere Datenbank aufgelöst werden. Um auszuschließen, dass Universen, die diese Verbindung verwenden, Konnektivitätsproblemen ausgesetzt sind, müssen die Datenbankschemas übereinstimmen.

> **Beispiel**
>
> Wenn das replizierte Universum auf der Zielwebsite eine andere Datenbank als die vom Universum auf der ursprünglichen Website verwendete nutzen soll, replizieren Sie die Universumsverbindung, wobei die Konnektivitätsinformationen für die Zielwebsite jedoch auf die gewünschte Datenbank verweisen müssen.
>
> Wenn die Universumsverbindung auf der ursprünglichen Website beispielsweise eine ODBC-Verbindung mit dem Namen “Test” verwendet, die auf “DatenbankA” verweist, stellen Sie sicher, dass auf der Zielwebsite ebenfalls eine ODBC-Verbindung mit dem Namen “Test” vorhanden ist, die jedoch auf “DatenbankB” verweist.

23.7 Verwalten von Replikationslisten

Replikationslisten enthalten Inhalte, z.B. Benutzer, Gruppen und Berichte, in der BI-Plattform-Umgebung, die zusammen repliziert werden können. Der Zugriff auf Replikationslisten erfolgt über die CMC.

In der folgenden Tabelle werden Inhaltstypen erklärt, die repliziert werden können.

Kategorie	Unterstützte Objekte
Repositoryobjekte	Objekte, einschließlich Business Views, Datenverbindungen, Wertelisten, Datengrundlagen usw.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Kategorie	Unterstützte Objekte
	Hinweis Alle Objekte werden unterstützt, wenn auch nicht auf ihrer jeweiligen Ebene.
Berichte	Crystal-Reports-Berichte, Web-Intelligence-Dokumente und Dashboards-Objekte. **Hinweis** Full Client-Add-In und Vorlagen werden unterstützt.
Objekte von Drittherstellern	Excel, PDF, PowerPoint, Flash, Word, Textdateien, RTF-Dateien, Shockwave Flash-Dateien.
Benutzer	Benutzer, Gruppen, Posteingänge, Favoriten, persönliche Kategorien.
BI-Plattform	Ordner, Ereignisse, Kategorien, Kalender, benutzerdefinierte Rollen, Hyperlinks, Verknüpfungen, Programme, Profile, Objektpakete, Agnostisch.
Universen	Universen, Verbindungen, Universumszugriffsbeschränkungen.

Hinweis

Folgende Objekte müssen auf der ursprünglichen Website erstellt und auf der Zielwebsite repliziert werden. Wenn Sie diese Objekte auf der Zielwebsite erstellen und dann auf die ursprüngliche Website replizieren, sind sie auf der ursprünglichen Website nicht funktionsfähig.

- Business Views
- Business Elements
- Datengrundlagen
- Datenverbindungen
- Wertelisten
- Universumszugriffsbeschränkungen

23.7.1 Erstellen von Replikationslisten

Die Replikationslisten sind im Bereich "Replikationslisten" der CMC abgelegt. Sie können Replikationslisten in dafür erstellten Ordnern und Unterordnern organisieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

23.7.1.1 Erstellen eines Replikationslisten-Ordners

1. Wechseln Sie zum Bereich *Replikationslisten* der CMC.
2. Klicken Sie auf **Replikationslisten**.
3. Klicken Sie auf **Verwalten** > **Neu** > **Ordner**.
   Das Dialogfeld *Ordner erstellen* wird angezeigt.
4. Geben Sie einen Ordnernamen ein, und klicken Sie auf **OK**.
   Nun können Sie in diesem Ordner Replikationslisten erstellen.

23.7.1.2 Erstellen von Replikationslisten

1. Wechseln Sie zum Bereich *Replikationslisten* der CMC.
2. Wählen Sie den Ordner, in dem die neue Replikationsliste gespeichert werden soll.
3. Klicken Sie auf **Verwalten** > **Neu** > **Neue Replikationsliste**.
   Das Dialogfeld *Neue Replikationsliste* wird angezeigt.
4. Geben Sie den Namen und die Beschreibung der Replikationsliste ein.
5. Klicken Sie für erweiterte Optionen auf die Verknüpfung **Replikationslisteneigenschaften**.

   Auf diese Weise können Sie angeben, welche Abhängigkeiten automatisch von der ursprünglichen Website auf die Zielwebsite repliziert werden sollen.
6. Wählen Sie die erforderlichen, in der Tabelle beschriebenen Optionen.

Optionen für Objektabhängigkeit	Definition
Persönliche Ordner für ausgewählte Benutzer einschließen	Repliziert die persönlichen Ordner eines ausgewählten Benutzers sowie deren Inhalt.
Persönliche Kategorien für ausgewählte Benutzer einschließen	Repliziert die persönlichen Kategorien eines ausgewählten Benutzers.
Universen für ausgewählte Berichte einschließen	Repliziert alle Universen, von denen die ausgewählten Berichtsobjekte abhängig sind.
Mitglieder ausgewählter Benutzergruppen einschließen	Repliziert Benutzer innerhalb einer ausgewählten Gruppe.
Für ausgewählte Universen erforderliche Universen einschließen	Repliziert alle Universen, die von anderen Universen abhängig sind.
Posteingänge für ausgewählte Benutzer einschließen	Repliziert den Posteingang eines ausgewählten Benutzers sowie dessen Inhalt.
Benutzergruppen für ausgewählte Universen einschließen	Repliziert die Benutzergruppen, die mit den Zugriffsbeschränkungen eines Universums verknüpft sind.
Für ausgewählte Objekte festgelegte Zugriffsberechtigungen einschließen	Repliziert alle für die ausgewählten Objekte verwendeten Zugriffsberechtigungen.
Dokumente für ausgewählte Kategorien einschließen	Repliziert alle Dokumente, einschließlich Word, Excel und PDF, die in ausgewählten Kategorien enthalten sind.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Optionen für Objektabhängigkeit	Definition
Unterstützte Abhängigkeiten für ausgewählte Flash-Objekte einschließen	Repliziert alle Crystal-Reports-Berichte, Hyperlinks, Web Intelligence-Dokumente oder -Universen, von denen das Flash-Objekt abhängig ist.
Profile für ausgewählte Benutzer und Benutzergruppen einschließen	Repliziert alle mit ausgewählten Benutzern oder Gruppen verknüpfte Profile.
Von ausgewählten Universen verwendete Verbindungen einschließen	Repliziert alle von ausgewählten Objekten verwendeten Universumsverbindungsobjekte.

> **Hinweis**
>
> Einige Objekte in der BI-Plattform sind abhängig von anderen Objekten. Beispielsweise hängt ein Web Intelligence-Dokument im Hinblick auf Struktur und Inhalt vom zugrunde liegenden Universum ab. Wenn Sie ein Web Intelligence-Dokument replizieren, ohne das von ihm verwendete Universum auszuwählen, kann die Replikation auf der Zielwebsite nur ausgeführt werden, wenn das Universum bereits auf die Zielwebsite repliziert wurde. Wenn Sie jedoch *Universen für ausgewählte Berichte einschließen* aktivieren, repliziert Föderation automatisch die Universen, von denen der Bericht abhängt.

7. Klicken Sie auf **Weiter**.
8. Wählen Sie ein oder mehrere Objekte, die zur Replikationsliste hinzugefügt werden sollen.
   - Verwenden Sie die Pfeilschaltflächen, um Objekte dem Ordner *Verfügbare Objekte* hinzuzufügen oder aus diesem zu entfernen.
   - Oder klicken Sie auf **Repository-Objekte** unter *Alle replizieren*, um alle Business-View-, Business-Element-, Datengrundlagen-, Datenverbindungs-, Wertelisten- und Repository-Objekte, einschließlich Berichtsbilder und -funktionen, zu replizieren.

> **Hinweis**
>
> Ordner der obersten Ebene unterhalb des Ordners *Verfügbare Objekte* können nicht repliziert werden.

9. Klicken Sie auf **Speichern und schließen**.

23.7.2 Ändern von Replikationslisten

Nachdem Sie eine Replikationsliste erstellt haben, können Sie deren Eigenschaften oder Objekte ändern.

23.7.2.1 Ändern von Eigenschaften in einer Replikationsliste

1. Wechseln Sie zum Bereich *Replikationslisten* der CMC.
2. Wählen Sie die zu ändernde **Replikationsliste**.
3. Klicken Sie auf **Verwalten** > **Eigenschaften**.
   Das Dialogfeld **Allgemeine Eigenschaften** wird angezeigt.
4. Ändern Sie Name und Beschreibung. Sie können auch andere Bereiche der Replikationsliste ändern, solange das Dialogfeld **Allgemeine Eigenschaften** geöffnet ist.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

5. Wenn Sie Abhängigkeitsoptionen ändern möchten, klickern Sie in der Navigationsliste auf **Replikationslisteneigenschaften**.
6. Klicken Sie auf **Speichern und schließen**.

Weitere Informationen

Erstellen von Replikationslisten [Seite 769]

23.7.2.2 Ändern von Objekten in einer Replikationsliste

1. Wechseln Sie zum Bereich *Replikationslisten* der CMC.
2. Wählen Sie eine **Replikationsliste** aus.
3. Klicken Sie auf **Aktionen** > **Replikationsliste verwalten**.
   Im Dialogfeld *Replikationsliste verwalten* wird eine Liste der in der Replikationsliste enthaltenen Objekte angezeigt.
4. Fügen Sie ggf. Objekte hinzu, bzw. entfernen Sie diese.
5. Klicken Sie auf **Speichern und schließen**.

Weitere Informationen

Erstellen von Replikationslisten [Seite 769]

23.8 Verwalten von Remoteverbindungen

Remoteverbindungsobjekte enthalten die erforderlichen Informationen für die Verbindung zu einer BI-Plattform-Implementierung.

> **Hinweis**
>
> Das Remoteverbindungsobjekt wird auf einer BI-Plattform-Implementierung einer Zielsite erstellt. Die Remoteverbindung ist die ursprüngliche Website.

Sie können Remoteverbindungen im Bereich *Föderation* der CMC anzeigen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

23.8.1 Erstellen von Remoteverbindungen

Eine Remoteverbindung in Föderation stellt eine Verbindung zu einer BI-Plattform-Remoteimplementierung her. Um eine Verbindung mit der ursprünglichen Website herzustellen, auf der sich der zu replizierende Inhalt befindet, erstellen Sie zunächst eine Remoteverbindung auf der Zielwebsite.

Zur Organisation der Remoteverbindungen können Sie Ordner und Unterordner erstellen.

23.8.1.1 Erstellen von Remoteverbindungsordnern

1. Wechseln Sie zum Bereich *Föderation* der CMC.
2. Klicken Sie auf **Remoteverbindungen**.
3. Klicken Sie auf **Verwalten** > **Neu** > **Ordner**.
   Das Dialogfeld **Ordner erstellen** wird angezeigt.
4. Geben Sie einen Ordnernamen ein, und klicken Sie auf **OK**.
   Nun können Sie in diesem Ordner Remoteverbindungen erstellen.

23.8.1.2 Erstellen von Remoteverbindungen

Um eine Verbindung zu einer BI-Plattform-Remoteimplementierung herzustellen, erstellen Sie eine Remoteverbindung in Föderation.

1. Wechseln Sie zum Bereich *Föderation* der CMC.
2. Klicken Sie auf **Remoteverbindungen**.
3. Klicken Sie auf **Verwalten** > **Neu** > **Neue Remoteverbindung**.
   Das Dialogfeld *Neue Remotesystem-Verbindung* wird angezeigt.
4. Geben Sie Titel, Beschreibung und zugehörige Felder nach Bedarf ein:

> **Hinweis**
>
> Alle Felder mit Ausnahme von “Beschreibung” und “Anzahl der Bereinigungsobjekte beschränken auf” sind obligatorisch.

Feld	Beschreibung
title	Name des Remoteverbindungsobjekts.
Beschreibung	Beschreibung des Remoteverbindungsobjekts. (Optional)
Webdienst-URI des Remotesystems	URL zu den Föderationswebdiensten, die automatisch auf dem Java-Anwendungsserver implementiert wird. Sie können beliebige Federation Web Services in der BI-Plattform – auf der ursprünglichen Website oder der Zielwebsite – oder in einer anderen Implementierung verwenden. Verwenden Sie folgendes Format:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Feld	Beschreibung
	`http://<Anwendung_IhrServer_RechnerName>:<Port>/dswsbobje`. Beispiel: `http://<MeinRechner.MeineDomäne.com>:<8080>/dswsbobje`
Remotesystem-CMS	Der Name des CMS, zu dem Sie eine Verbindung herstellen möchten, auf den über Föderationswebdienste zugegriffen werden kann. Dieser wird als CMS für die ursprüngliche Website behandelt. Das Format lautet: `CMS_Name:Port`. Beispiel: `<MeinRechner>:6400` **Hinweis** Wenn Sie den Standard-Port 6400 verwenden, ist die Angabe des Ports optional.
Benutzername	Der Benutzername, über den eine Verbindung zur ursprünglichen Website hergestellt wird. **Hinweis** Stellen Sie sicher, dass der verwendete Benutzername über Ansichtsrechte auf der Replikationliste in der Implementierung der ursprünglichen Website verfügt.
Kennwort	Das Kennwort des Benutzerkontos, über das eine Verbindung zur ursprünglichen Website hergestellt wird.
Authentifizierung	Der Typ der Kontoauthentifizierung, mit der eine Verbindung zur ursprünglichen Website hergestellt wird. Optionen: Enterprise, AD oder LDAP.
Bereinigungsfrequenz (in Stunden)	Gibt an, wie oft Replikationsaufträge, die dieses Remoteverbindungsobjekt verwenden, eine Objektbereinigung ausführen sollten. Geben Sie nur positive ganze Zahlen ein. Die Einheit lautet Stunden. Standard = 24.
Anzahl der Bereinigungsobjekte beschränken auf	Die Anzahl der Objekte, die von einem Replikationsauftrag bereinigt werden. (Optional)

5. Klicken Sie auf **OK**.

Weitere Informationen

Verwalten der Objektbereinigung [Seite 780]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

23.8.2 Ändern von Remoteverbindungen

Nachdem Sie eine Remoteverbindung erstellt haben, können Sie deren Eigenschaften und Sicherheitsoptionen ändern.

So ändern Sie eine Remoteverbindung:

1. Wechseln Sie zum Bereich *Föderation* der CMC.
2. Klicken Sie auf **Remoteverbindungen**.
3. Doppelklicken Sie auf die Remoteverbindung, die Sie ändern möchten.
   Das Dialogfeld *Eigenschaften der Remoteverbindung* wird angezeigt. Sie können die folgenden Eigenschaften ändern:
   - **Titel**
   - **Beschreibung**
   - **Webdienst-URI des Remotesystems**
   - **Remotesystem-CMS**
   - **Benutzername**
   - **Kennwort**
   - **Authentifizierung**
   - **Bereinigungsfrequenz (in Stunden)**
   - **Anzahl der Bereinigungsobjekte beschränken auf**
4. Nehmen Sie die Änderungen vor.
5. Klicken Sie auf **Speichern und schließen**.

23.9 Verwalten von Replikationsaufträgen

Bei einem Replikationsauftrag handelt es sich um einen Objekttyp, der nach einem Zeitplan ausgeführt und verwendet wird, um Inhalte zwischen zwei BI-Plattform-Implementierungen in Föderation zu replizieren.

> **Hinweis**
>
> Replizierte Objekte auf einer Zielwebsite werden mit einem Replikationssymbol gekennzeichnet, wie nachfolgend abgebildet: . Bei einem Konflikt wird ein Objekt mit einem Konfliktsymbol gekennzeichnet, wie nachfolgend abgebildet: .

Im Ordner **Remoteverbindung** im Bereich *Föderation* der CMC können Sie eine Liste der Replikationsaufträge anzeigen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

23.9.1 Erstellen von Replikationsaufträgen

Für die Replikation von Inhalten zwischen zwei BI-Plattform-Implementierungen in Föderation ist ein Replikationsauftrag erforderlich. Jedem Replikationsauftrag muss genau eine Remoteverbindung und eine Replikationsliste zugeordnet sein.

23.9.1.1 Erstellen von Replikationsaufträgen

1. Wechseln Sie zum Bereich *Föderation* der CMC.
2. Klicken Sie auf **Remoteverbindungen**.
3. Wählen Sie eine **Remoteverbindung**, in der der neue Replikationsauftrag enthalten sein soll.

   Achtung

   Damit Sie die Arbeit im Assistenten fortsetzen können, muss die CMC in der Lage sein, eine Verbindung zu Webdiensten im Remoteverbindungs-URI herzustellen.

4. Klicken Sie auf **Verwalten** > **Neu** > **Neuer Replikationsauftrag**.
   Das Dialogfeld *Neuer Replikationsauftrag* wird eingeblendet.
5. Geben Sie einen Namen und eine Beschreibung für den Replikationsauftrag ein.
6. Klicken Sie auf **Weiter**.
   Es wird eine Liste der auf der ursprünglichen Website verfügbaren Replikationslisten angezeigt.
7. Wählen Sie die **Replikationsliste** aus, die Sie für den Replikationsauftrag verwenden möchten.
8. Klicken Sie auf **Weiter**.
9. Wählen Sie aus den in der folgenden Tabelle beschriebenen Konfigurationsoptionen.

Option	Beschreibung
Objektbereinigung für Ziel aktivieren	Bewirkt, dass vom Replikationsauftrag alle replizierten Objekte auf der Zielwebsite gelöscht werden, deren zugehöriges ursprüngliches Objekt auf der ursprünglichen Website entfernt wurde. **Hinweis** Bei der Objektbereinigung werden keine Objekte gelöscht, die unter Verwendung von Abhängigkeiten oder von aus der Replikationsliste ausgewählten Objekten repliziert wurden.
Einseitige Replikation	Legt fest, dass ein Objekt nur von der ursprünglichen Website auf die Zielwebsite repliziert wird. Änderungen, die nach der Replikation des Objekts auf der ursprünglichen Website vorgenommen wurden, werden auf die Zielwebsite repliziert. Auf der Zielwebsite vorgenommene Änderungen werden jedoch nicht auf die ursprüngliche Website zurück repliziert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Beschreibung
Beidseitige Replikation	Legt fest, dass Objekte in beide Richtungen repliziert werden: von der ursprünglichen Website auf die Zielwebsite und von der Zielwebsite auf die ursprüngliche Website. Änderungen, die nach der Replikation an diesen Objekten auf einer Website vorgenommen wurden, werden automatisch auf die andere Website repliziert.
Ursprüngliche Website hat Vorrang	Legt fest, dass bei Auftreten eines Konflikts zwischen einem Objekt auf der ursprünglichen Website und dessen replizierter Version auf der Zielwebsite die Version auf der ursprünglichen Website Vorrang hat.
Keine automatische Konfliktauflösung	Legt fest, dass keine Maßnahmen zur Auflösung eventueller Konflikte unternommen werden.
Zielwebsite hat Vorrang (nur bei der beidseitigen Replikation verfügbar)	Legt fest, dass bei Auftreten eines Konflikts zwischen einem Objekt auf der ursprünglichen Website und dessen replizierter Version auf der Zielwebsite die Version auf der Zielwebsite Vorrang hat.
Normale Replikation	Legt fest, dass der Replikationsauftrag normal ausgeführt wird.
Von ursprünglicher Website aus regenerieren	Repliziert den gesamten Inhalt unabhängig davon, ob er geändert wurde, von der ursprünglichen Website auf die Zielwebsite. Sie können die Replikationsliste vollständig oder in Teilen replizieren.
Von Ziel aus regenerieren (nur bei der beidseitigen Replikation verfügbar)	Repliziert den gesamten Inhalt, unabhängig davon, ob er geändert wurde, von der Zielwebsite auf die ursprüngliche Website. Sie können die Replikationsliste vollständig oder in Teilen replizieren.
Alle Objekte replizieren (wird nur bei der beidseitigen Replikation angezeigt)	Repliziert die gesamte Replikationsliste. Hinweis Dies ist die umfassendste Option, erfordert jedoch auch die längste Ausführungszeit.
Remotezeitpläne replizieren (wird nur bei der beidseitigen Replikation angezeigt)	Repliziert ausstehende Remoteinstanzen von der Zielwebsite auf die ursprüngliche Website und erzwingt die Replikation abgeschlossener Instanzen von der ursprünglichen Website auf die Zielwebsite.
Dokumentvorlagen replizieren	Repliziert alle Objekte, die keine Instanzen sind (lokal ausgeführte Objekte oder Berichte, die für die zeitgesteuerte Remote-Verarbeitung vorgesehen sind). Dies umfasst Benutzer, Gruppen, Ordner, Berichte usw.
Lokal ausgeführte abgeschlossene Instanzen	Repliziert abgeschlossene Instanzen ausschließlich von der Zielwebsite auf die ursprüngliche Website.

10. Klicken Sie auf **OK**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Verwalten der Objektbereinigung [Seite 780]
Erkennen und Auflösen von Konflikten [Seite 782]
Remote-Zeitsteuerung und lokale Ausführung von Instanzen [Seite 790]

23.9.2 Zeitgesteuertes Verarbeiten von Replikationsaufträgen

Nachdem Sie einen Replikationsauftrag erstellt haben, können Sie ihn einmalig oder wiederholt zeitgesteuert verarbeiten lassen. Außerdem können Sie mehrere Replikationsaufträge auf einer Zielwebsite von einer ursprünglichen Website aus zeitgesteuert verarbeiten.

> **Hinweis**
>
> Bei der zeitgesteuerten Verarbeitung mehrerer Replikationsaufträge auf einer Zielwebsite kann immer nur ein Replikationsauftrag eine Verbindung mit der ursprünglichen Website herstellen. Alle anderen Replikationsaufträge, die versuchen, eine Verbindung herzustellen, werden in den Zustand "Ausstehend" versetzt und darin belassen, bis sie in der Lage sind, automatisch eine Verbindung mit der ursprünglichen Website herzustellen.

23.9.2.1 Zeitgesteuertes Verarbeiten eines Replikationsauftrags

1. Wechseln Sie zum Bereich *Föderation* der CMC.
2. Wählen Sie den **Replikationsauftrag**, der zeitgesteuert verarbeitet werden soll.
3. Klicken Sie auf **Aktionen** > **Zeitpläne**.
4. Wählen Sie die gewünschten Zeitsteuerungsoptionen.

23.9.3 Ändern von Replikationsaufträgen

Nach der Erstellung eines Replikationsauftrags in der Föderation können Sie dessen Eigenschaften ändern.

23.9.3.1 So ändern Sie einen Replikationsauftrag

1. Wechseln Sie zum Bereich *Föderation* der CMC.
2. Klicken Sie auf den Ordner **Remoteverbindungen**.
3. Wählen Sie das **Remoteverbindungsobjekt**, das den zu ändernden **Replikationsauftrag** enthält.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Wählen Sie den zu ändernden **Replikationsauftrag**.
5. Klicken Sie auf **Verwalten** > **Objekteigenschaften verwalten**.
6. Sie können **Eigenschaften**, **Zeitgesteuerte Verarbeitung**, **Verlauf**, **Replikationsliste** und **Benutzersicherheit** anzeigen lassen und Ihren Anforderungen entsprechend bearbeiten.

Sektionen	Beschreibung
Eigenschaften	Ändern von Namen, Beschreibung sowie anderen allgemeinen Eigenschaften und Optionen des Replikationsauftrags.
Zeitgesteuert verarbeiten	Festlegen, dass der Replikationsauftrag nach einem regelmäßigen Zeitplan ausgeführt wird.
Verlauf	Anzeigen und Verwalten aller Instanzen des Replikationsauftrags.
Replikationsliste	Ändern der ausgewählten Replikationsliste.
Benutzersicherheit	Festlegen von Rechten für den Replikationsauftrag.

23.9.4 Anzeigen eines Protokolls nach einem Replikationsauftrag

Bei jedem Ausführen eines Replikationsauftrags erstellt Föderation automatisch eine Protokolldatei, die auf der Zielwebsite angelegt wird. Die Protokolldateien entsprechen XML 1.1-Standards und erfordern einen Webbrowser, der XML 1.1 unterstützt.

So lassen Sie ein Replikationsprotokoll anzeigen:

1. Wechseln Sie zum Bereich *Föderation* der CMC.
2. Klicken Sie auf den Ordner **Alle Replikationsaufträge**.
3. Wählen Sie einen **Replikationsauftrag** aus der Liste aus.
4. Klicken Sie auf **Eigenschaften**.
   Die *Eigenschaftenseite* des Replikationsauftrags wird geöffnet.
5. Klicken Sie auf **Verlauf**.
6. Klicken Sie auf die **Instanzenzeit** der Protokolldatei, um erfolgreiche Replikationsaufträge anzeigen zu lassen, oder auf den Status **Fehlgeschlagen**, um eine Protokolldatei für fehlgeschlagene Replikationsaufträge aufzurufen.
7. Wählen Sie die gewünschte Instanz, um die Protokolldatei einzusehen.
   Die Protokolldatei wird im XML-Format ausgegeben und verwendet ein XLS-Formular, um die Informationen in einer HTML-Seite zu formatieren.

   Sie können von dem Computer, auf dem der Server Intelligence Agent mit dem Adaptive Job Server ausgeführt wird, auf das XML-Protokoll zugreifen. Die Protokolldatei finden Sie unter:

   - Unter Windows: `<InstallVerz>\SAP BusinessObjects XI 4.0\logging`
   - Unter Unix: `<InstallVerz>/sap_bobj/logging`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

23.10 Verwalten der Objektbereinigung

In Föderation sollte die Objektbereinigung während des gesamten Lebenszyklus des Replikationsprozesses ausgeführt werden, um sicherzustellen, dass alle Objekte, die Sie aus der ursprünglichen Website entfernen, auch aus den einzelnen Zielwebsites gelöscht werden.

Die Objektbereinigung beinhaltet zwei Elemente: eine Remoteverbindung und einen Replikationsauftrag. Durch ein Remoteverbindungsobjekt werden allgemeine Bereinigungsoptionen definiert. Die Bereinigung wird von einem Replikationsauftrag ausgeführt, wenn das entsprechende Intervall abläuft.

23.10.1 Verwenden der Objektbereinigung

Während der Objektbereinigung arbeiten getrennte Replikationsaufträge, die dieselbe Remoteverbindung verwenden, zusammen. Dies bedeutet, dass während des Replikationsauftrags sowohl Objekte innerhalb dessen Replikationsliste als auch Objekte innerhalb anderer Replikationslisten, die dieselbe Remoteverbindung verwenden, bereinigt werden. Eine Remoteverbindung wird nur als identisch angesehen, wenn das übergeordnete Element des Replikationsauftrags dem Remoteverbindungsobjekt entspricht.

Beispiel

Durch die Replikationsaufträge A und B werden Objekt A und Objekt B repliziert. Beide führen die Replikation von derselben ursprünglichen Website durch und verwenden dieselbe Remoteverbindung. Wenn Objekt B von der ursprünglichen Website gelöscht wird, ist für Replikationsauftrag A ersichtlich, dass Objekt B gelöscht wurde. Obwohl Objekt B von Replikationsauftrag B repliziert wird, wird Objekt B auch von der Zielwebsite gelöscht. Wenn Replikationsauftrag B ausgeführt wird, ist keine Objektbereinigung erforderlich.

Hinweis

Nur Objekte auf der Zielwebsite werden während der Objektbereinigung gelöscht. Wenn Sie ein Objekt von der ursprünglichen Website löschen, die Bestandteil der Replikation ist, wird das Objekt von der Zielwebsite gelöscht. Wenn ein Objekt jedoch von der Zielwebsite entfernt wird, wird es bei der Objektbereinigung nicht von der ursprünglichen Website entfernt, und zwar selbst dann nicht, wenn der Replikationsauftrag im beidseitigen Replikationsmodus ausgeführt wird.

Objekte, die aus der Replikationsliste gelöscht oder entfernt werden, werden nicht von der Zielwebsite gelöscht. Um ein in der Replikationsliste angegebenes Objekt ordnungsgemäß zu entfernen, sollten Sie es sowohl auf der Zielwebsite als auch auf der ursprünglichen Website löschen. Über Abhängigkeitsberechnungen replizierte Objekte werden nicht gelöscht.

23.10.2 Beschränkungen der Objektbereinigung

Im Remoteverbindungsobjekt können Sie die Anzahl der Objekte festlegen, die jeweils von einem Replikationsauftrag bereinigt werden. Von Federation wird automatisch nachverfolgt, wo der Bereinigungsauftrag endet. Wenn Sie einen Replikationsauftrag das nächste Mal ausführen, wird der nächste Bereinigungsauftrag folglich auch an diesem Punkt gestartet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Tipp

Um einen Replikationsauftrag schneller abzuschließen, sollten Sie die Anzahl der Bereinigungsobjekte einschränken.

Beispiel

Durch die Replikationsaufträge A und B werden Objekt A und Objekt B repliziert. Beide Objekte werden von derselben ursprünglichen Website repliziert und verwenden dieselbe Remoteverbindung.

Wenn Objekt B von der ursprünglichen Website gelöscht und der Objektgrenzwert auf 1 festgelegt ist, wird beim nächsten Ausführen von Replikationsauftrag A nur überprüft, ob Objekt A gelöscht wurde. Auf diese Weise wird Objekt B nicht überprüft und nicht gelöscht.

Als Nächstes wird Replikationsauftrag B ausgeführt und beginnt mit der Objektbereinigung an der Stelle, an der Replikationsauftrag A beendet wurde. Es wird überprüft, ob Objekt B gelöscht wurde, und das Objekt wird von der Zielwebsite entfernt. Sie finden diese Option in der Eigenschaft "Anzahl der Bereinigungsobjekte beschränken auf" des Remoteverbindungsobjekts.

Hinweis

Wenn Sie diese Option nicht auswählen, werden von sämtlichen Replikationsaufträgen, die diese Remoteverbindung verwenden, alle Objekte auf eine potenzielle Bereinigung überprüft.

23.10.3 Häufigkeit der Objektbereinigung

Im Feld "Bereinigungsfrequenz" der Remoteverbindung können Sie festlegen, wie oft die Objektbereinigung von einem Replikationsauftrag ausgeführt wird.

Hinweis

Geben Sie eine positive ganze Zahl ein, durch die die Anzahl der Stunden dargestellt wird, die zwischen den Verarbeitungsgängen der Objektbereinigung gewartet wird.

Beispiel

Durch die Replikationsaufträge A und B werden Objekt A und Objekt B repliziert. Beide Objekte werden von derselben ursprünglichen Website repliziert und verwenden dieselbe Remoteverbindung.

Wird Objekt B von der ursprünglichen Website gelöscht und alle folgenden Bedingungen sind wahr, überprüft der Replikationsauftrag, ob Objekt A gelöscht wurde.

- Das Grenzwert für das Objekt ist 1
- Die Bereinigungsfrequenz beträgt 150 Stunden
- Replikationsauftrag A wird als Nächstes ausgeführt.

Da der Grenzwert für das Objekt 1 ist, wird Objekt B auf der Zielwebsite weder überprüft noch gelöscht.

Die nächste Bereinigung wird 150 Stunden nach der ersten Prüfung durch Replikationsauftrag A ausgeführt. Obwohl Replikationsaufträge A und B vor Ablauf der 150 Stunden viele Male ausgeführt werden können, wird in

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

keinem Fall versucht, eine Objektbereinigung durchzuführen. Nach 150 Stunden wird der nächste Replikationsauftrag ausgeführt und eine Bereinigung gestartet. Anschließend ermittelt er, dass Objekt B auf der ursprünglichen Website gelöscht wurde, und löscht das Objekt anschließend auf der Zielwebsite.

Aktivieren und Deaktivieren von Optionen

Jeder Replikationsauftrag kann an der Objektbereinigung beteiligt sein. Verwenden Sie die Option " Objektbereinigung für Ziel aktivieren" für einen Replikationsauftrag, um anzugeben, ob eine Objektbereinigung ausgeführt werden soll. In einigen Fällen verfügen Sie vielleicht über Replikationsaufträge mit hoher Priorität, die nicht von der Objektbereinigung berücksichtigt werden sollen, damit sie so schnell wie möglich ausgeführt werden können. Dazu deaktivieren Sie die Objektbereinigung.

Weitere Informationen

Beschränkungen der Objektbereinigung [Seite 780]

23.11 Erkennen und Auflösen von Konflikten

In Föderation kann ein Konflikt auftreten, wenn Sie die Eigenschaften eines Objekts sowohl auf der ursprünglichen Website als auch auf der Zielwebsite ändern. Eigenschaften der obersten Ebene und verschachtelte Eigenschaften eines Objekts werden auf Konflikte überprüft. Es kann beispielsweise ein Konflikt auftreten, wenn ein Bericht oder der Name eines Berichts sowohl auf der ursprünglichen als auch auf der Zielwebsite geändert wird.

In einigen Fällen wird kein Konflikt verursacht. Wenn beispielsweise der Name eines Berichts auf der ursprünglichen Website geändert wird, und die Beschreibung der replizierten Version auf der Zielwebsite geändert wird, werden die Änderungen zusammengeführt und es tritt kein Konflikt auf.

23.11.1 Konfliktauflösung bei der einseitigen Replikation

Bei der einseitigen Replikation können Sie Konflikte auf zwei Arten auflösen.

Ursprüngliche Website hat Vorrang

Wenn während einer einseitigen Replikation ein Konflikt auftritt, hat das Objekt der ursprünglichen Website Vorrang. Alle Änderungen an Objekten auf der Zielwebsite werden mit den Informationen der ursprünglichen Website überschrieben. Wenn ein Bericht beispielsweise sowohl auf der ursprünglichen als auch auf der

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Zielwebsite geändert wird, wird nach dem nächsten Replikationsauftrag die Änderung der Zielwebsite durch die Version der ursprünglichen Website überschrieben.

> **Hinweis**
>
> Da der Konflikt automatisch aufgelöst wird, wird er nicht in der Protokolldatei generiert und nicht in der Liste konfliktverursachender Objekte angezeigt.

Keine automatische Konfliktauflösung

Wenn ein Konflikt auftritt und Sie “Keine automatische Konfliktauflösung” auswählen, wird der Konflikt nicht aufgelöst, es wird keine Protokolldatei generiert, und der Konflikt wird nicht in der Liste konfliktverursachender Objekte angezeigt.

Im Bereich "Föderation" der CMC kann der Administrator auf eine Liste aller replizierten Objekte zugreifen, die miteinander in Konflikt stehen. Konfliktverursachende Objekte werden nach der Remoteverbindung gruppiert, über die sie mit der ursprünglichen Website verbunden wurden. Um diese Listen aufzurufen, wechseln Sie im Bereich "Föderation" der CMC zum Ordner "Replikationsfehler" und wählen die gewünschte Remoteverbindung aus. Alle replizierten Objekte auf einer Zielwebsite werden mit einem Replikationssymbol gekennzeichnet. Bei einem Konflikt werden Objekte mit einem Konfliktsymbol gekennzeichnet. Außerdem wird in der *Eigenschaftenseite* eine Warnmeldung angezeigt.

> **Hinweis**
>
> Die Liste wird nach Abschluss eines Replikationsauftrags, der eine Remoteverbindung verwendet, aktualisiert. Sie enthält alle konfliktverursachenden Objekte für alle Replikationsaufträge, die die jeweilige Remoteverbindung verwenden.

> **Hinweis**
>
> Das im Protokolldateiverzeichnis ausgegebene XML-Protokoll kann von allen Benutzern geöffnet werden, die Zugriff auf die CMC und Instanzen des Replikationsauftrags haben. Die Kennzeichnung eines Objekts auf der Zielwebsite mit einem Symbol weist auf einen Konflikt hin. Während der Verarbeitung wird ein Konfliktprotokoll erstellt.

Abdul ändert Bericht A auf der ursprünglichen Website. Maria ändert die replizierte Version auf der Zielwebsite. Beim nächsten Ausführen des Replikationsauftrags verursacht der Bericht einen Konflikt, da er auf beiden Websites geändert wurde und nicht aufgelöst wird.

Der Zielbericht wird beibehalten, und Änderungen am Bericht auf der ursprünglichen Website werden nicht repliziert. Nachfolgende Replikationsaufträge verhalten sich bis zur Lösung des Konflikts gleich. Alle Änderungen auf der ursprünglichen Website werden erst repliziert, nachdem der Konflikt manuell aufgelöst wurde.

> **Hinweis**
>
> In diese Fall wird das gesamte Objekt nicht repliziert. Sonstige Änderungen, die keinen Konflikt verursachen, werden nicht importiert.

Sie haben drei Möglichkeiten, einen Konflikt manuell aufzulösen:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

1. Erstellen Sie einen Replikationsauftrag, durch den nur die konfliktverursachenden Objekte repliziert werden. Dabei muss dasselbe Remoteverbindungsobjekt und dieselbe Replikationsliste verwendet werden.

   Um die Änderungen der ursprünglichen Website beizubehalten, erstellen Sie einen Replikationsauftrag. Legen Sie "Replikationsmodus" anschließend auf “Von ursprünglicher Website aus regenerieren” und "Automatische Konfliktauflösung" auf “Ursprüngliche Website hat Vorrang” fest.

   Um die Änderungen auf der Zielwebsite beizubehalten, erstellen Sie einen Replikationsauftrag mit dem Replikationstyp “Beidseitige Replikation”, dem Replikationsmodus “Von Ziel aus regenerieren” und der automatischen Konfliktauflösung “Zielwebsite hat Vorrang”.

   > **Hinweis**
   >
   > Legen Sie im Replikationsmodus “Von ursprünglicher Website aus regenerieren” oder “Von Ziel aus regenerieren” fest, um nur die Objekte auszuwählen, die auf der Replikationsliste als konfliktverursachend gekennzeichnet sind. Dadurch werden alle anderen Objekte nicht repliziert. Als Nächstes sollten Sie den Replikationsauftrag zeitgesteuert verarbeiten. Dabei werden nur die ausgewählten Objekte repliziert und Konflikte wie angegeben gelöst.

2. Erstellen Sie einen Replikationsauftrag, durch den nur die konfliktverursachenden Objekte repliziert werden. Dabei muss dasselbe Remoteverbindungsobjekt verwendet werden. Im Gegensatz zu Option 1 können Sie jedoch eine neue Replikationsliste auf der ursprünglichen Website erstellen. Verwenden Sie nur die Objekte, die in Konflikt stehen, und erstellen Sie einen neuen Replikationsauftrag, der diese fokussierte Replikationsliste verwendet.

   Um die Änderungen auf der ursprünglichen Website beizubehalten, legen Sie die automatische Konfliktauflösung auf “Ursprüngliche Website hat Vorrang” fest.

   Um die Änderungen auf der Zielwebsite beizubehalten, legen Sie die automatische Konfliktauflösung auf “ Zielwebsite hat Vorrang” und den Replikationstyp auf “Beidseitige Replikation” fest.
3. Bei einseitigen Replikationsaufträgen löschen Sie vielleicht nur das Objekt auf der Zielwebsite. Beim nächsten Ausführen des Replikationsauftrags wird das Objekt von der ursprünglichen Website auf die Zielwebsite repliziert.

   > **Hinweis**
   >
   > Achten Sie beim Löschen eines Objekts darauf, dass andere Objekte, die davon abhängig sind, entfernt werden können, vielleicht nicht mehr funktionieren oder ihre Sicherheitseinstellungen verlieren. Option 1 und 2 werden empfohlen.

23.11.2 Konfliktauflösung bei der beidseitigen Replikation

Bei Konflikten in der beidseitigen Replikation können Sie den Konflikt auf drei Weisen erkennen:

- Ursprüngliche Website hat Vorrang
- Zielwebsite hat Vorrang
- Keine automatische Konfliktauflösung

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ursprüngliche Website hat Vorrang

Wenn ein Konflikt auftritt, hat die ursprüngliche Website Vorrang, und Änderungen auf der Zielwebsite werden überschrieben.

Beispiel

Lilly ändert den Namen eines Berichts in Bericht A. Malik ändert den Namen der replizierten Version auf der Zielwebsite in Bericht B. Nach Ausführung des nächsten Replikationsauftrags wird die replizierte Version auf der Zielwebsite in Bericht A zurückversetzt.

Dadurch wird weder ein Konflikt in der Protokolldatei generiert noch in der Liste der konfliktverursachenden Objekte angezeigt, da der Konflikt entsprechend den Anweisungen des Benutzers auf der ursprünglichen Website aufgelöst wurde.

Zielwebsite hat Vorrang

Wenn ein Konflikt auftritt, werden die Änderungen auf der Zielwebsite beibehalten und Änderungen auf der ursprünglichen Website überschrieben.

Beispiel

Kamal ändert den Namen eines Berichts in Bericht A. Peter ändert den Namen der replizierten Version auf der Zielwebsite in Bericht B. Beim Ausführen des Replikationsauftrags wird ein Konflikt festgestellt. Der Name des Berichts auf der Zielwebsite lautet weiterhin Bericht B.

Bei der beidseitigen Replikation werden Änderungen auch an die ursprüngliche Website zurückgesendet. In diesem Szenario wird die ursprüngliche Website aktualisiert und ihr Berichtname in Bericht B geändert. Dadurch wird kein Konflikt in der Protokolldatei generiert und kein Konflikt in der Liste konfliktverursachender Objekte angezeigt, da der Konflikt gemäß den Benutzerhinweisen aufgelöst wurde.

Keine automatische Konfliktauflösung

Wenn “Keine automatische Konfliktauflösung” ausgewählt wird, wird kein Konflikt aufgelöst. Der Konflikt wird in einer Protokolldatei für den Administrator festgehalten und kann vom Administrator manuell aufgelöst werden.

Hinweis

Durch das Konfliktsymbol wird angezeigt, dass ein Konflikt aufgetreten ist.

Hinweis

Obwohl Änderungen bei der beidseitigen Replikation sowohl auf die ursprüngliche als auch auf die Zielwebsite repliziert werden, werden nur die Versionen auf der Zielwebsite als konfliktverursachend gekennzeichnet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Hinweis

Das im Protokolldateiverzeichnis ausgegebene XML-Protokoll kann von allen Benutzern geöffnet werden, die Zugriff auf die CMC und Instanzen des Replikationsauftrags haben. Die Kennzeichnung eines Objekts auf der Zielwebsite mit einem Symbol weist auf einen Konflikt hin. Während der Verarbeitung wird ein Konfliktprotokoll erstellt.

Im Bereich "Föderation" der CMC kann der Administrator auf eine Liste aller replizierten Objekte zugreifen, die miteinander in Konflikt stehen. Konfliktverursachende Objekte werden nach der Remoteverbindung gruppiert, über die sie mit der ursprünglichen Website verbunden wurden. Um auf diese Listen zuzugreifen, rufen Sie **CMC** > **Föderation** > **Replikationsfehler** > **Remoteverbindung** auf.

Hinweis

Die Liste wird nach Abschluss eines Replikationsauftrags, der eine Remoteverbindung verwendet, aktualisiert. Sie enthält alle konfliktverursachenden Objekte für alle Replikationsaufträge, die die jeweilige Remoteverbindung verwenden. Alle replizierten Objekte auf einer Zielwebsite werden durch ein Replikationssymbol gekennzeichnet. Wenn ein Konflikt eintritt, werden die Objekte durch ein Konfliktsymbol gekennzeichnet.

Beispiel

Michael ändert Bericht A auf der ursprünglichen Website. Damien ändert die replizierte Version auf der Zielwebsite. Beim Ausführen des nächsten Replikationsauftrags verursacht der Bericht einen Konflikt, da er auf beiden Websites geändert wurde und nicht aufgelöst wird.

Der Zielbericht wird beibehalten, und Änderungen am Bericht auf der ursprünglichen Website werden nicht repliziert. Nachfolgende Replikationsaufträge verhalten sich bis zur Lösung des Konflikts gleich. Alle Änderungen an der ursprünglichen Website werden erst repliziert, nachdem der Konflikt vom Administrator oder delegierten Administrator manuell aufgelöst wurde.

Hinweis

In diese Fall wird das gesamte Objekt nicht repliziert. Sonstige Änderungen, die keinen Konflikt verursachen, werden nicht repliziert.

Hinweis

Das im Protokolldateiverzeichnis ausgegebene XML-Protokoll kann von allen Benutzern geöffnet werden, die Zugriff auf die CMC und Instanzen des Replikationsauftrags haben. Die Kennzeichnung eines Objekts auf der Zielwebsite mit einem Symbol weist auf einen Konflikt hin. Während der Verarbeitung wird ein Konfliktprotokoll erstellt.

Im Bereich "Föderation" der CMC kann der Administrator auf eine Liste aller replizierten Objekte zugreifen, die miteinander in Konflikt stehen. Konfliktverursachende Objekte werden nach der Remoteverbindung gruppiert, über die sie mit der ursprünglichen Website verbunden wurden. Um auf diese Listen zuzugreifen, rufen Sie **CMC** > **Föderation** > **Replikationsfehler** > **Remoteverbindung** auf.

Hinweis

Die Liste wird nach Abschluss eines Replikationsauftrags, der eine Remoteverbindung verwendet, aktualisiert. Sie enthält alle konfliktverursachenden Objekte für alle Replikationsaufträge, die die jeweilige

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Remoteverbindung verwenden. Alle replizierten Objekte auf einer Zielwebsite werden durch ein Replikationssymbol gekennzeichnet. Wenn ein Konflikt eintritt, werden die Objekte durch ein Konfliktsymbol gekennzeichnet.

Sie haben drei Möglichkeiten, einen Konflikt manuell aufzulösen:

1. Erstellen Sie einen Replikationsauftrag, durch den nur die konfliktverursachenden Objekte repliziert werden. Dabei muss dasselbe Remoteverbindungsobjekt und dieselbe Replikationsliste verwendet werden.

   Um die Änderungen der ursprünglichen Website beizubehalten, erstellen Sie einen Replikationsauftrag. Legen Sie den Replikationsmodus anschließend auf “Von ursprünglicher Website aus regenerieren” und "Automatische Konfliktauflösung" auf “Ursprüngliche Website hat Vorrang” fest.

   Um die Änderungen auf der Zielwebsite beizubehalten, erstellen Sie einen Replikationsauftrag mit dem Replikationstyp “Beidseitige Replikation”, dem Replikationsmodus “Von Ziel aus regenerieren” und der automatischen Konfliktauflösung “Zielwebsite hat Vorrang”.

   > **Hinweis**
   >
   > Legen Sie im Replikationsmodus “Von ursprünglicher Website aus regenerieren” oder “Von Ziel aus regenerieren” fest, um nur die Objekte auszuwählen, die auf der Replikationsliste als konfliktverursachend gekennzeichnet sind. Dadurch werden alle anderen Objekte nicht repliziert. Als Nächstes sollten Sie den Replikationsauftrag zeitgesteuert verarbeiten. Dabei werden nur die ausgewählten Objekte repliziert und Konflikte wie angegeben gelöst.

2. Erstellen Sie einen Replikationsauftrag, durch den nur die konfliktverursachenden Objekte repliziert werden. Dabei muss dasselbe Remoteverbindungsobjekt verwendet werden. Im Gegensatz zu Option 1 können Sie jedoch eine neue Replikationsliste auf der ursprünglichen Website erstellen. Verwenden Sie nur die Objekte, die in Konflikt stehen, und erstellen Sie einen neuen Replikationsauftrag, der diese fokussierte Replikationsliste verwendet.

   Um die Änderungen der ursprünglichen Website beizubehalten, stellen Sie für die Automatische Konfliktauflösung ein: “Ursprüngliche Website hat Vorrang”.

   Um die Änderungen der Zielwebsite beizubehalten, stellen Sie für die Automatische Konfliktauflösung ein: “ Zielwebsite hat Vorrang” und für den Replikationstyp: “Beidseitige Replikation”..
3. Löschen Sie das Objekt auf der Site, auf der es nicht vorkommen soll.

> **Hinweis**
>
> Achten Sie beim Löschen eines Objekts darauf, dass andere Objekte, die davon abhängig sind, entfernt werden können, vielleicht nicht mehr funktionieren oder ihre Sicherheitseinstellungen verlieren. Option 1 und 2 werden empfohlen.

Um die Änderungen der Zielwebsite beizubehalten, können Sie das Objekt auf der ursprünglichen Website löschen. Beim nächsten Ausführen des Replikationsauftrags wird das Objekt von der Zielwebsite auf die ursprüngliche Website repliziert.

> **Hinweis**
>
> Gehen Sie mit Sorgfalt vor, wenn Sie die Kopie auf einer ursprünglichen Website löschen, da andere Zielwebsites, auf denen das Objekt repliziert wird, ihre Replikationsaufträge ausführen können, bevor die Kopie zurückrepliziert wurde. Dies führt dazu, dass die anderen Zielwebsites ihre Kopie löschen, die erst bei Rückgabe der Kopie wieder verfügbar ist.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Um die Änderungen der ursprünglichen Website beizubehalten, können Sie das Objekt auf der Zielwebsite löschen.

23.12 Verwenden von Web Services in Föderation

Föderation verwendet Web Services zum Versenden von Objekten und Objektänderungen zwischen der ursprünglichen Website und der Zielwebsite. Bei der Installation der BI-Plattform werden föderationsspezifische Webdienste automatisch installiert und implementiert. Sie können auch Eigenschaften in Web Services ändern oder Implementierungen anpassen, um die Funktionalität zu verbessern, wie in diesem Abschnitt beschrieben.

> **Tipp**
>
> Um die Dateiverwaltungsfunktionen zu verbessern, aktivieren Sie die Zwischenspeicherung von Dateien in der Datenföderation.

23.12.1 Sitzungsvariablen

Wenn zahlreiche Inhaltsdateien in einem Replikationsauftrag übertragen werden, können Sie den Zeitüberschreitungswert der Sitzung der Föderation Web Services erhöhen.

Die Eigenschaft befindet sich in der Datei `dsws.properties`:

```
<Anwendungsserver-Installationsverzeichnis>\dswsbobje\Web-INF\classes
```

Beispiel:

```
C:\Programme\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles
\webapps\dswsbobje\WEB-INF\classes
```

Geben Sie Folgendes ein, um eine Sitzungsvariable zu aktivieren:

```
session.timeout = x
```

Dabei entspricht “x” der gewünschten Zeit. “x” wird in Sekunden gemessen. Falls nicht angegeben, lautet der Standardwert 1200 Sekunden oder 20 Minuten.

Die neuen Eigenschaften werden erst wirksam, nachdem die geänderte Webanwendung erneut auf dem Rechner implementiert wird, auf dem der Webanwendungsserver ausgeführt wird. Implementieren Sie die WAR-Datei mit WDeploy erneut auf dem Webanwendungsserver. Informationen zum Umgang mit WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen*.

23.12.2 Zwischenspeichern von Dateien

Das Zwischenspeichern von Dateien bietet Web Services die Möglichkeit, sehr große Anlagen zu verarbeiten, ohne sie im Speicher zu puffern. Falls die Zwischenspeicherung während der Übertragung großer Datenmengen nicht aktiviert ist, wird u.U. der gesamte Java Virtual Machine-Speicher belegt, und die Replikation kann fehlschlagen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Das Zwischenspeichern von Dateien beeinträchtigt die Leistung, da die Daten von den Web Services in Dateien anstatt in den Arbeitsspeicher verarbeitet werden. Es ist möglich, eine Kombination aus beiden Optionen zu verwenden und größere Übertragungen an eine Datei und kleinere an den Arbeitsspeicher zu senden.

Um die Dateizwischenspeicherung zu aktivieren, bearbeiten Sie die Datei `Axis2.xml` unter:

```
<Anwendungsserver-Installationsverzeichnis>\dswsbobje\Web-Inf\conf
```

Beispiel:

```
C:\Programme\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles
\webapps\dswsbobje\WEB-INF\conf
```

Geben Sie Folgendes ein:

```
<parameter name="cacheAttachments" locked="false">true</parameter>

<parameter name="attachmentDIR" locked="false">temp directory</parameter>

<parameter name="sizeThreshold" locked="false">4000</parameter>
```

> **Hinweis**
>
> Die Größe des Schwellenwerts wird in Byte gemessen.

Die neuen Eigenschaften werden erst wirksam, nachdem die geänderte Webanwendung erneut auf dem Rechner implementiert wird, auf dem der Webanwendungsserver ausgeführt wird. Implementieren Sie die WAR-Datei mit WDeploy erneut auf dem Webanwendungsserver. Informationen zum Umgang mit WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen*.

23.12.3 Benutzerdefinierte Implementierung

Föderation Web Services können automatisch implementiert werden und erfordern die Aktivierung der Dienste “ federation”, “biplatform” und “session”. Zum Deaktivieren von Föderation oder anderer Web Services bearbeiten Sie die Datei `service.xml` des entsprechenden Webdiensts.

Die BI-Plattform-Webdienste befinden sich im folgenden Verzeichnis:

```
<Anwendungsserver-Installationsverzeichnis>\dswsbobje\WEB-INF\services
```

Beispiel:

```
C:\Programme\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles
\webapps\dswsbobje\WEB-INF\services
```

So deaktivieren Sie Web Services:

- Fügen Sie die “activate”-Eigenschaft in das "service name"-Tag der Datei `service.xml` ein, und legen Sie sie auf "false" fest.
- Starten Sie den Java-Anwendungsserver neu.

So deaktivieren Sie z.B. Föderation:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Die Datei `services.xml` befindet sich unter:

```
C:\Programme\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles
\webapps\dswsbobje\WEB-INF\services\federator\META-INF
```

Ändern Sie "service name" von:

```
<service name="Federator">
```

In:

```
<service name="Federator" activate="false">
```

Die neuen Eigenschaften werden erst wirksam, nachdem die geänderte Webanwendung erneut auf dem Rechner implementiert wird, auf dem der Webanwendungsserver ausgeführt wird. Implementieren Sie die WAR-Datei mit WDeploy erneut auf dem Webanwendungsserver. Informationen zum Umgang mit WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen*.

23.13 Remote-Zeitsteuerung und lokale Ausführung von Instanzen

In diesem Abschnitt werden die Remote-Zeitsteuerung, lokal ausgeführte Instanzen und Instanzenfreigaben erläutert. Durch diese Funktionen können Berichte am Speicherort der Daten ausgeführt und abgeschlossene Berichtsinstanzen an die geeigneten Standorte gesendet werden.

23.13.1 Remote-Zeitsteuerung

Mithilfe von Föderation können Sie einen Bericht auf der Zielwebsite zeitsteuern und auf der ursprünglichen Website verarbeiten lassen. Die abgeschlossene Instanz wird an die Zielwebsite zurückgesendet.

Um die Remote-Zeitsteuerung zu aktivieren, lassen Sie einen Bericht normal zeitgesteuert verarbeiten und aktivieren die Option “Auf ursprünglicher Website ausführen”. Um diese Option zu aktivieren, klicken Sie auf **Zeitgesteuerte Verarbeitung** > **Zeitsteuerungsservergruppe** > **Auf ursprünglicher Website ausführen**. Nachdem die zeitgesteuerten Instanzen erstellt wurden, weisen sie den Zustand "Ausstehend" auf.

Während der Remote-Zeitsteuerung werden die auf der Zielwebsite übergebenen Informationen ignoriert, und die Berichtsinstanz befindet sich weiterhin im Status "Ausstehend".

Wenn der nächste Replikationsauftrag, durch den der Bericht verwaltet wird, für die Remote-Zeitsteuerung aktiviert wird, wird die Instanz zur Verarbeitung auf die ursprüngliche Website kopiert. Die Instanz bleibt so lange im ausstehenden Zustand, bis sie vom Scheduler verarbeitet wird. In der Zwischenzeit gibt der Replikationsauftrag, von dem die Instanz gesendet wurde, alle zuvor abgeschlossenen Instanzen und Objektänderungen zurück.

Nachdem die Instanz auf der ursprünglichen Website verarbeitet wurde, befindet sie sich in einem abgeschlossenen Zustand. Wenn der nächste Replikationsauftrag, der den Bericht verwaltet, für die Remote-Zeitsteuerung aktiviert wird, wird die abgeschlossene Instanz zum Aktualisieren der Kopie auf der Zielwebsite verwendet. Nach der Aktualisierung wird die Instanz auf der Zielwebsite in einen abgeschlossenen Zustand versetzt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Hinweis

Ein Replikationsauftrag muss zweimal ausgeführt werden, damit eine abgeschlossene Instanz zurückgegeben wird.

Beispiel

1. Tom lässt Bericht A für die Remote-Zeitsteuerung zeitgesteuert verarbeiten.
2. Bericht A wird auf der Zielwebsite erstellt und befindet sich im Zustand "Ausstehend".
3. Replikationsauftrag A wird ausgeführt. Zuerst werden Änderungen (einschließlich bereits abgeschlossener Instanzen) von der ursprünglichen auf die Zielwebsite repliziert. Anschließend werden die Instanz im ausstehenden Zustand sowie die Änderungen, die von der Zielwebsite auf die ursprüngliche Website repliziert werden sollen, auf die ursprüngliche Website kopiert.
4. Auf der ursprünglichen Website wählt der Scheduler die Instanz im ausstehenden Zustand aus und sendet sie zur Verarbeitung an den geeigneten Job Server. Die Instanz wird dann verarbeitet und auf der ursprünglichen Website in den abgeschlossenen Zustand versetzt.
5. Replikationsauftrag A wird erneut ausgeführt. Beim Replizieren von Inhalten von der ursprünglichen auf die Zielwebsite wird die abgeschlossene Instanz Bericht A übernommen und die Änderungen auf die Version der Zielwebsite angewendet.
6. Nachdem diese Aufgabe erledigt wurde, ist die Zielversion abgeschlossen.

Die Remote-Zeitsteuerung wird nur bei beidseitigen Replikationsaufträgen unterstützt. Die Option “ Remotezeitpläne replizieren” muss aktiviert werden. Diese Option befindet sich im Bereich *Replikationsfilter* auf der Seite “Eigenschaften des Replikationsauftrags”. In einigen Szenarien können Sie Aufträge, die remote zeitgesteuert verarbeitet wurden, auch häufiger als andere Objekte in der Replikationsliste replizieren. Dazu erstellen Sie zwei Replikationsaufträge. Aktivieren Sie einen Replikationsauftrag mit “Remotezeitpläne replizieren”, der ausschließlich für die Remote-Zeitsteuerung vorgesehen ist. Aktivieren Sie den zweiten Auftrag mit “Dokumentvorlagen replizieren” oder “Alle Objekte replizieren (kein Filter)”.

Hinweis

Wenn Sie die Remote-Zeitsteuerung aktivieren, werden abgeschlossene und fehlgeschlagene Instanzen sowohl auf der ursprünglichen als auch auf der Zielwebsite angezeigt.

Wenn ein Benutzer auf der Zielwebsite einen Bericht für die Remote-Zeitsteuerung plant und auf der ursprünglichen Website nicht vorhanden ist, schlägt die Instanz auf der ursprünglichen Website fehl. Der Eigentümer der fehlgeschlagenen Instanz entspricht dem Benutzerkonto des Remoteverbindungsobjekts, das für die Verbindung mit der ursprünglichen Website verwendet wurde.

Ein Replikationsauftrag kann zwar ausschließlich für die Remote-Zeitsteuerung konfiguriert werden, die Vorgängerobjekte der Berichtsinstanz werden jedoch immer mitrepliziert. Wenn Änderungen zwischen Replikationen stattfinden, bedeutet dies, dass der tatsächliche Ordner, Berichtsordner usw. repliziert werden. Wenn dieÄnderungen auf der Zielwebsite nicht auf der ursprünglichen Website repliziert werden sollen, können Sie über Sicherheitsrechte steuern, welche Änderungen repliziert werden.

Weitere Informationen

Verwalten von Sicherheitsrechten [Seite 759]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

23.13.2 Lokal ausgeführte Instanzen

Lokal ausgeführte Instanzen sind Instanzen eines Berichts, die von Berichten auf der Zielwebsite verarbeitet wurden. Mithilfe von Föderation können Sie die abgeschlossenen Instanzen von der Zielwebsite auf die ursprüngliche Website replizieren.

Damit in einem Replikationsauftrag sowohl abgeschlossene als auch fehlgeschlagene Instanzen von der Zielwebsite auf die ursprüngliche Website repliziert werden können, klicken Sie auf **Eigenschaften des Replikationsauftrags** > **Replikationsfilter** > **Lokal ausgeführte abgeschlossene Instanzen replizieren**.

In einigen Fällen können von einem Replikationsauftrag ausschließlich die lokal ausgeführten Instanzen repliziert werden. Aktivieren Sie dazu “Lokal ausgeführte abgeschlossene Instanzen replizieren”.

Hinweis

Wenn "Lokal ausgeführte Instanzen" für einen Replikationsauftrag aktiviert ist, werden sowohl abgeschlossene als auch fehlgeschlagene Instanzen auf die ursprüngliche Website repliziert. Dies bedeutet, dass sowohl auf der ursprünglichen als auch auf der Zielwebsite Kopien vorhanden sind.

Ausstehende Instanzen werden niemals repliziert.

Wenn der Eigentümer einer lokal ausgeführten Instanz auf der ursprünglichen Website nicht vorhanden ist, entspricht der Eigentümer dem für die Verbindung verwendeten Benutzerkonto im Remoteverbindungsobjekt.

23.13.3 Instanzenfreigabe

Wenn Sie in einem Replikationsauftrag "Remote-Zeitsteuerung" und "Lokal ausgeführte Instanzen" aktivieren, können Instanzen gemeinsam verwendet werden, wenn eine ursprüngliche Website mit mehreren Zielwebsites verwendet wird, die denselben Bericht replizieren.

Beispiel

Bericht A stammt von der ursprünglichen Website, obwohl er von den Zielwebsites A und B repliziert wird. Die Instanzenfreigabe findet auf beiden Zielwebsites statt:

- Replikationsaufträge wurden mit “Remotezeitpläne replizieren” und/oder “Lokal ausgeführte abgeschlossene Instanzen replizieren” aktiviert. Replizieren Sie Bericht A mit dem gleichen Replikationsauftrag wie oben.
- Bericht A auf der Zielwebsite wurde mit “Auf ursprünglicher Website ausführen” und/oder für die lokale Ausführung geplant.

Wenn sowohl Zielwebsite A als auch Zielwebsite B Bericht A replizieren und deren entsprechende Replikationsaufträge Remotezeitpläne und/oder lokal ausgeführte Instanzen replizieren, werden alle Instanzen, die auf Zielwebsite A und/oder auf der ursprünglichen Website im Namen von Zielwebsite A verarbeitet werden, mit Zielwebsite B gemeinsam verwendet.

Entsprechend werden alle Instanzen, die auf Zielwebsite B und/oder auf der ursprünglichen Website verarbeitet wurden, gemeinsam mit Zielwebsite A verwendet. Schließlich verfügen die ursprüngliche Website und Zielwebsite A und B über eine identische Gruppe von Instanzen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Die Instanzenfreigabe ist in vielen Fällen die ideale Vorgehensweise. Beispielsweise, wenn Benutzer von anderen Websites auf Informationen aus verwandten Implementierungen zugreifen müssen. Damit Instanzen in diesem Fall nicht von Benutzern auf der lokalen Website angezeigt werden, stellen Sie sicher, dass die richtigen Sicherheitsrechte festgelegt sind. Wenden Sie in einem Berichtsobjekt beispielsweise die Rechte an, damit Benutzer nur die Instanzen in ihrem Besitz einsehen können.

> **Hinweis**
>
> Alle Objekte unterliegen den Sicherheitsregeln der BI-Plattform. Um sicherzustellen, dass Benutzer und Gruppen nur anwendbare Instanzen anzeigen lassen können, wird empfohlen, Rechte festzulegen, durch die Benutzer nur Instanzen anzeigen lassen können, die sie besitzen. Wenden Sie in einem Berichtsobjekt beispielsweise die Rechte an, damit Benutzer nur die Instanzen in ihrem Besitz einsehen können.

Weitere Informationen

Verwalten von Sicherheitsrechten [Seite 759]

23.14 Importieren und Höherstufen replizierter Inhalte

In einigen Fällen können Sie replizierten Inhalt von einem Business-Intelligence-System auf ein anderes importieren oder hochstufen. In diesem Abschnitt werden diese Features in Federation erörtert.

> **Hinweis**
>
> Objektmigrationen werden am besten von Mitgliedern der Administratorengruppe, insbesondere dem Administratorbenutzerkonto durchgeführt. Um ein Objekt zu migrieren, müssen verschiedene zugehörige Objekte u.U. ebenfalls migriert werden. Der Erwerb der erforderlichen Sicherheitsberechtigungen für sämtliche Objekte ist für ein delegiertes Administratorkonto eventuell nicht möglich.

23.14.1 Importieren replizierter Inhalte

Wenn Sie mit dem LifeCycle Manager Inhalte aus einer BI-Plattform-Implementierung in eine andere Implementierung migrieren, importiert der LifeCycle Manager keine replikationsspezifischen Informationen im Zusammenhang mit den importierten replizierten Objekten. Das bedeutet, dass das Objekt nach dem Import genauso funktioniert, als wäre es nie repliziert worden. Dies ist spezifisch für replizierte Objekte auf einer Zielwebsite und wird im folgenden Szenario beschrieben.

> **Beispiel**
>
> BI-Plattform A ist eine Zielwebsite in einem Föderationsprozess. Bericht A, ein replizierter Bericht auf System A, wird mit dem LifeCycle Manager von System A in BI-Plattform B importiert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ergebnis: Wenn Bericht A in BI-Plattform B kopiert wird, enthält er keine replizierten Informationen. Bericht A ist nicht mehr mit einem Replikationssymbol gekennzeichnet. Wenn das Objekt auf BI-Plattform A einen Konflikt verursacht hat, tritt dieser Konflikt auf System B nicht auf. Im Prinzip wird es als ein Objekt behandelt, das seinen Ursprung in System B hat.

Hinweis

Die CUID kann identisch sein, je nachdem, welche Importoptionen Sie im LifeCycle Manager auswählen.

23.14.2 Importieren replizierter Inhalte und Fortsetzen der Replikation

Nachdem Sie replizierten Inhalt importiert haben, können Sie die importierten Objekt in einen Föderation-Prozess übernehmen. Es gibt zwei Szenarios: Behandeln des Systems, in dem sich die importierten Objekte befinden, als ursprüngliche Website oder Behandeln des Systems als Zielwebsite. Um dieses System als ursprüngliche Website zu behandeln, fahren Sie normal mit Föderation fort.

Um das System als Zielwebsite zu behandeln und die importierten Objekte von der ursprünglichen Website zu replizieren, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass die CUID der Objekte beibehalten wird, wenn Sie den LifeCycle Manager verwenden.
- Stellen Sie sicher, dass die Konfliktauflösung für den ersten Replikationsauftrag auf “Ursprüngliche Website hat Vorrang” oder “Zielwebsite hat Vorrang” festgelegt ist.

Tipp

Anstatt das Objekt mit dem LifeCycle Manager von einer Zielwebsite auf eine andere zu importieren, ist es effizienter und absolut empfehlenswert, das Objekt nur mit Föderation zu replizieren.

Beispiel

Bericht A wurde auf Business-Intelligence-System A erstellt. System X hat Bericht A mit Föderation aus System A auf System X repliziert. Anschließend hat der LifeCycle Manager Bericht A aus System X auf System Y importiert.

Plan: System Y möchte Föderation für System A einrichten und Bericht A als Teil der Replikation beibehalten. System Y ist die Zielwebsite und System A die ursprüngliche Website.

Aktion: Beim Importieren von Bericht A aus System X auf System Y muss die CUID von Bericht A beibehalten werden. Wenn der erste Replikationsauftrag ausgeführt wird, wird außerdem versucht, Bericht A zu replizieren. Da das Objekt in System Y bereits vorhanden ist, verursacht die Replikation einen Konflikt. Um die zu verwendende Version anzugeben, muss der Konfliktauflösungsmodus entweder auf “Ursprüngliche Website hat Vorrang” oder “Zielwebsite hat Vorrang” festgelegt werden.

Hinweis

In diesem Beispiel wird empfohlen, das Objekt nur mit Föderation zu replizieren, anstatt es mit dem LifeCycle Manager von einer Zielwebsite auf eine andere zu importieren. Bericht A wird von System A auf

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

System Y repliziert, und es ist nicht erforderlich, den LifeCycle Manager für den Import von System X auf System Y auszuführen.

23.14.3 Höherstufen von Inhalten aus einer Testumgebung

In Unternehmen werden häufig Testverfahren ausgeführt, bevor Komponenten in die Produktionsumgebung übernommen werden. Bevor Föderation auf Produktionsrechnern eingerichtet wird, sollte sie zwischen BI-Systemen in einer Entwicklungs- oder Testumgebung getestet werden. Nachdem Sie die ursprüngliche Website und die Zielwebsite einschließlich Inhalt in einer Testumgebung erstellt haben, können Sie diese Konfiguration mithilfe der folgenden Schritte auf Produktionsrechner übernehmen:

1. Verwenden Sie LifeCycle Manager, um Inhalte von der ursprünglichen Website in der Testumgebung auf den Rechner in der Produktionsumgebung umzulagern, der als ursprüngliche Website fungiert.

   Hinweis

   Das Replikationslistenobjekt kann bei Verwendung von LifeCycle Manager nicht ausgewählt werden.

2. Erstellen Sie die Replikationsliste auf der ursprünglichen Website in der Produktionsumgebung, und nehmen Sie den gewünschten Inhalt auf.
3. Wählen Sie eine der beiden folgenden Optionen aus:
   - A) Erstellen Sie ein Remoteverbindungsobjekt und die entsprechenden Replikationsaufträge auf den Produktionsrechnern der Produktionsumgebung, die als Zielwebsite fungiert.
   - B) Verwenden Sie LifeCycle Manager, um die Remoteverbindung und Replikationsaufträge von den Zielwebsites der Entwicklungs-/Qualitätssicherungsumgebung auf die Produktionsrechner zu importieren, die als Zielwebsite(s) fungieren. Bearbeiten Sie dann die importierten Remoteverbindungen, um auf den Rechner in der Produktionsumgebung zu verweisen, der als ursprüngliche Website fungiert.

23.14.4 Neuverweisen auf eine Zielwebsite

Wenn ein Objekt von einer Ursprungswebsite repliziert wurde, muss dieses derzeit immer von dieser Ursprungswebsite repliziert werden, nicht von einem anderen BI-System. Wenn das Remoteverbindungsobjekt so bearbeitet wurde, dass es auf ein neues System verweist, schlägt jeder Replikationsversuch für Objekte fehlt, die von einem anderen BI-System repliziert wurden als das Remoteverbindungsobjekt. Um ein Objekt von einer anderen ursprünglichen Website zu replizieren, muss es erst aus der Zielwebsite gelöscht werden.

Hinweis

Nachdem Sie ein repliziertes Objekt kopiert haben, wird die CUID der Kopie geändert, und die Kopie enthält keine Replikationsinformationen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

23.15 Optimale Vorgehensweisen

Mithilfe von Federation können Sie die Leistung eines Replikationsauftrags optimieren.

Wenn ein einzelner Replikationsauftrag eine große Anzahl an Objekten enthält, können Sie zusätzliche Schritte durchführen, um die erfolgreiche Ausführung sicherzustellen. Normalerweise sollte es möglich sein, bis zu 32.000 Objekte in einem Replikationsauftrag zu replizieren. In einigen Implementierungen können jedoch Konfigurationen mit geringeren oder höheren Replikationsmengen erforderlich sein.

1) Erwerben Sie einen dedizierten Webdienst-Provider

In Föderation werden replizierte Inhalte über Webdienste gesendet. In einer Standardinstallation der BI-Plattform nutzen alle Webdienste denselben Webdienst-Provider. Daher können umfangreichere Replikationsaufträge dazu führen, dass der Webdienst-Provider länger beansprucht wird und dessen Reaktion gegenüber anderen Webdienstanforderungen und -anwendungen, die von ihm bedient werden, verlangsamt werden.

Falls Sie beabsichtigen, zahlreiche Objekte gleichzeitig zu replizieren oder mehrere Replikationsaufträge in Folge auszuführen, sollten Sie die Implementierung von Föderation Web Services auf einem eigenen Java-Anwendungsserver unter Verwendung eines eigenen Webdienst-Providers in Betracht ziehen.

Verwenden Sie zu diesem Zweck das BI-Plattform-Installationsprogramm, um die Webdienste zu installieren. Es muss bereits ein Java-Anwendungsserver ausgeführt werden. Installieren Sie andernfalls die gesamten Webschichtkomponenten, durch die Webdienste und Tomcat installiert werden.

> **Hinweis**
>
> Es müssen Informationen zu einem vorhandenen CMS angegeben werden (beispielsweise Hostname, Port und Administratorkennwort).

> **Hinweis**
>
> Die URI dieses neuen Webdienst-Providers muss im Feld "URI" der Remoteverbindung verwendet werden.

2) Erweitern Sie den verfügbaren Arbeitsspeicher auf dem Java-Anwendungsserver

Der für den Java-Anwendungsserver verfügbare Arbeitsspeicher sollte erweitert werden, wenn in einem einzelnen Replikationsauftrag zahlreiche Objekte repliziert werden bzw. wenn der Anwendungsserver von anderen Anwendungen genutzt wird.

Wenn Sie die BI-Plattform und Tomcat implementiert haben, steht standardmäßig 1 GB Arbeitsspeicher zur Verfügung. So erweitern Sie den verfügbaren Arbeitsspeicher für Tomcat:

In Windows:

1. Klicken Sie auf **Start** > **Programme** > **Tomcat** > **Tomcat-Konfiguration**.
2. Wählen Sie **Java**.
3. Suchen Sie im Feld **Java-Optionen** den Eintrag `-Xmx1024M`.
4. Erhöhen Sie den Parameter `-Xmx1024M` auf die gewünschte Größe.

> **Beispiel**
>
> Um den Arbeitsspeicher auf 2 GB zu erhöhen, geben Sie `-Xmx2048M` ein.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

In Unix:

1. Öffnen Sie in `<BOE_INSTALLVERZ>/setup/` die Datei `env.sh` mit Ihrem bevorzugten Texteditor. Erhöhen Sie den Parameter `-Xmx1024m` auf die gewünschte Größe.
2. Suchen Sie die folgenden Zeilen:

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
 # set the JAVA_OPTS for Tomcat
 JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"

 if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" =
"SunOS" -o "$SOFTWARE" = "Linux" ];
then
 JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
 fi
 export JAVA_OPTS
 # fi
```

3. Erhöhen Sie den Parameter `-Xmx1024m` auf die gewünschte Größe.

Beispiel

Um den Arbeitsspeicher auf 2 GB zu erhöhen, geben Sie `-Xmx2048m` ein.

Tipp

Bei anderen Java-Anwendungsservern finden Sie in der jeweiligen Dokumentation Informationen über die Speichererweiterung.

3) Verringern Sie die Größe der erstellten BIAR-Dateien

Föderation verwendet Webdienste zum Replizieren von Inhalten zwischen der ursprünglichen Website und der Zielwebsite. Objekte werden für einen effizienteren Transport gruppiert und in BIAR-Dateien komprimiert.

Wenn eine große Anzahl von Objekten repliziert wird, sollte der Java-Anwendungsserver so konfiguriert werden, dass kleinere BIAR-Dateien erstellt werden. Da die Objekte von Federation in ein Paket komprimiert werden, das auf mehrere kleinere BIAR-Dateien verteilt wird, besteht in Bezug auf die Anzahl der zu replizierenden Objekte keine Begrenzung.

Um die Größe der erstellten BIAR-Dateien zu verringern, fügen Sie dem Java-Anwendungsserver folgende Java-Parameter hinzu:

```
Dbobj.biar.suggestSplit
and
Dbobj.biar.forceSplit
```

Durch `bobj.biar.suggestSplit` wird eine angemessene BIAR-Dateigröße vorgeschlagen, die möglichst eingehalten wird. Der empfohlene neue Wert ist 90 MB.

Durch `bobj.biar.forceSplit` wird erzwungen, dass die Größe einer BIAR-Datei nicht über einen bestimmten Wert hinausgeht. Der empfohlene neue Wert ist 100 MB.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Die Standardeinstellungen für die Größe der BIAR-Datei müssen nur geändert werden, wenn dem Anwendungsserver nicht genügend Arbeitsspeicher zur Verfügung steht und dessen maximale Heap-Größe nicht mehr erweitert werden kann.

Für Tomcat in Windows:

1. Um das **Tomcat-Konfigurations**-Tool zu öffnen, klicken Sie auf **Start** > **Programme** > **Tomcat** > **Tomcat-Konfiguration**.
2. Wählen Sie **Java**.
3. Fügen Sie im Feld **Java-Optionen** die folgenden Zeilen am Ende hinzu:

```
-Dbobj.biar.suggestSplit=90
-Dbobj.biar.forceSplit=100
```

Für Tomcat in Unix/Linux:

1. Öffnen Sie "env.sh" mit Ihrem bevorzugten Texteditor. Die Datei befindet sich unter `<BOE_INSTALLVERZ>/setup/`.
2. Suchen Sie die folgenden Zeilen:

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for tomcat
JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120 -Djava.awt.headless=true"

if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" = "SunOS" -o "$SOFTWARE" = "Linux" ]; then
JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
 fi
export JAVA_OPTS
 # fi
```

Fügen Sie die gewünschten Parameter für die Größe der BIAR-Datei hinzu.

Beispiel: `JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m` **-Dbobj.biar.suggestSplit=90 -Dbobj.biar.forceSplit=100"**

Informieren Sie sich bei anderen Java-Anwendungsservern in Ihrer Dokumentation über das Hinzufügen von Java-Systemeigenschaften.

4) Erhöhen Sie den Wert für das Socket-Timeout

Der Adaptive Job Server ist für die Ausführung des Replikationsauftrags zuständig. Während der Ausführung des Replikationsauftrags stellt der Adaptive Job Server eine Verbindung zur ursprünglichen Website her. Wenn große Datenmengen von der ursprünglichen Website empfangen werden, ist es wichtig, dass der Socket, den der Adaptive Job Server für den Empfang von Informationen verwendet, keine Zeitüberschreitung verursacht.

Der Standardwert ist 90 Minuten. Sie können das Socket-Timeout bei Bedarf erhöhen.

So erhöhen Sie das Socket-Timeout auf dem Adaptive Job Server:

1. Öffnen Sie die Central Management Console (CMC).
2. Navigieren Sie zum Bereich **Server**, und wählen Sie **Adaptive Job Server**.
3. Klicken Sie auf **Eigenschaften**.
4. Fügen Sie am Ende folgender Zeilen “Befehlszeilenparameter” hinzu:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- **Windows:** `-javaArgs Xmx1000m,Xincgc,server,Dbobj.federation.WSTimeout=<Zeitüberschreitungswert in Minuten>`
- **Unix:** `-javaArgs Xmx512m,Dbobj.federation.WSTimeout=<Zeitüberschreitungswert in Minuten>`

Weitere Informationen

Behandeln von Fehlermeldungen [Seite 800]
Verwenden von Web Services in Föderation [Seite 788]
Einschränkungen der aktuellen Version [Seite 799]

23.15.1 Einschränkungen der aktuellen Version

Föderation ist ein sehr flexibles Tool, das in einer Produktionsumgebung jedoch einigen Einschränkungen unterliegen kann. In diesem Abschnitt werden Bereiche herausgestellt, die bearbeitet werden können, um Vorgänge in Föderation zu optimieren.

- Maximale Anzahl von Objekten

  Bei jedem Replikationsauftrag werden Objekte zwischen BI-Plattform-Implementierungen repliziert. Es wird empfohlen, die maximale Anzahl von 100.000 replizierten Objekten in einem einzelnen Replikationsauftrag nicht zu überschreiten. Obwohl ein Replikationsauftrag u.U. auch mit mehr als 100.000 Objekten ausgeführt werden kann, unterstützt Föderation nur die Replikation von maximal 100.000 Objekten.
- Rechte

  In Föderation werden Rechte nur von der ursprünglichen Website auf die Zielwebsite repliziert. Es wird empfohlen, Benutzerrechte, die in beiden Implementierungen verwendet werden, auf der ursprünglichen Website festzulegen und mithilfe der beidseitigen Replikation auf die Zielwebsites zu replizieren. Benutzerrechte auf einer bestimmten Website werden in einer BI-Plattform-Implementierung wie gewohnt auf der Website verwaltet, der der Benutzer zugeordnet ist.
- Business Views und assoziierte Objekte

  In BI-Plattform können Business Views, Business Elements, Datengrundlagen, Datenverbindungen und Wertelisten gespeichert werden. Diese Objekte werden verwendet, um die Funktionalität von Crystal Reports-Berichten zu erweitern.
  Wenn diese Objekte zuerst auf der Zielwebsite erstellt und dann unter Verwendung der beidseitigen Replikation auf die ursprüngliche Website repliziert werden, funktionieren sie u.U. nicht ordnungsgemäß und ihre Daten werden dann in Crystal Reports-Berichten nicht angezeigt.
  Es wird empfohlen, die Business Views, Business Elements, Datengrundlagen, Datenverbindungen und Wertelisten auf der ursprünglichen Website zu erstellen und dann auf die Zielwebsite zu replizieren. Wenn Sie Aktualisierungen an den Objekten auf der Zielwebsite oder der ursprünglichen Website (sofern berechtigt) vornehmen, werden die Änderungen ordnungsgemäß zwischen den Websites repliziert.
- Universumszugriffsbeschränkungen

  Die BI-Plattform kann Universumszugriffsbeschränkungen speichern. Wenn auf der Zielwebsite Universumszugriffsbeschränkungen erstellt und dann unter Verwendung der beidseitigen Replikation auf die ursprüngliche Website repliziert werden, funktionieren sie u.U. nicht ordnungsgemäß.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Um dieses Problem zu beheben, erstellen Sie zuerst die Universumszugriffsbeschränkungen auf der ursprünglichen Website und replizieren diese auf die Zielwebsite. Im zweiten Schritt legen Sie Sicherheitseinstellungen für die Universumszugriffsbeschränkungen auf der ursprünglichen Website fest und replizieren diese auf die Zielwebsite.

- Objektbereinigung

  Bei der Objektbereinigung werden Objekte gelöscht, die von der anderen Website entfernt wurden. Die Objektbereinigung wird derzeit nur von der ursprünglichen Website aus auf der Zielwebsite ausgeführt.
- Föderation-Protokolldateien

  Föderation-Protokolldateien werden in XML-Dateien geschrieben, die XML 1.1-Standards entsprechen. Um die Protokolldateien in einem Browser anzeigen zu lassen, muss dieser XML 1.1 unterstützen.

Weitere Informationen

Verwalten der Objektbereinigung [Seite 780]

23.15.2 Behandeln von Fehlermeldungen

Dieser Abschnitt enthält Fehlermeldungen, die bei Verwendung von Föderation in seltenen Fällen auftreten können. Diese Meldungen werden in den Protokollen für Replikationsaufträge oder im Funktionsbereich eines Berichts angezeigt.

1) Ungültige GUID

Fehlerbeispiel: `FEHLER 2008-01-10T00:31:08.234Z Die GUID ASXOOFyvy0FJnRcD0dZNTZg (aus Eigenschaft SI_PARENT_CUID in Objektnummer 1285) ist keine gültige GUID.`

Dieser Fehler bedeutet, dass Sie ein Objekt replizieren, dessen übergeordnetes Element nicht mitrepliziert wird und das auch auf der Zielwebsite noch nicht vorhanden ist. Beispiel: Ein Objekt wird ohne den Ordner repliziert, in dem es enthalten ist. Das übergeordnete Objekt wird u.U. nicht repliziert, da das Konto, unter dem die Objekte repliziert werden, nicht über ausreichende Rechte für das übergeordnete Objekt verfügt.

2) Crystal Reports-Berichte, in denen auf der ursprünglichen Website keine Daten angezeigt werden

Dieser Fehler kann auftreten, wenn der Crystal Reports-Bericht eine Business View, ein Business Element, eine Datengrundlage, eine Datenverbindung oder Werteliste verwendet, das bzw. die ursprünglich auf der Zielwebsite erstellt und dann auf die ursprüngliche Website repliziert wurde.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

3) Universumszugriffsbeschränkungen werden nicht richtig angewendet.

Dieser Fehler kann auftreten, wenn der Bericht ein Universum verwendet, das eine Universumszugriffsbeschränkung enthält, die auf der Zielwebsite erstellt und dann auf die ursprüngliche Website repliziert wurde.

4) Nicht genügend Arbeitsspeicher für Java

Fehlerbeispiel: `java.lang.OutOfMemoryError`.

Dieser Fehler kann auftreten, wenn der Java-Anwendungsserver beim Verarbeiten eines Replikationsauftrags über zu wenig Arbeitsspeicher verfügt. Der Replikationsauftrag ist entweder zu groß, oder der Java-Anwendungsserver verfügt nicht über genügend Arbeitsspeicher.

Erweitern Sie entweder den verfügbaren Arbeitsspeicher auf dem Java-Anwendungsserver, indem Sie Föderation Web Services auf einen dedizierten Rechner verschieben, oder verringern Sie die Anzahl der in einem Replikationsauftrag replizierten Objekte.

5) Socket-Timeout

Fehlerbeispiel: `Fehler bei der Kommunikation mit ursprünglicher Website. Zeitüberschreitung beim Lesen`.

Die von der ursprünglichen Website an den Adaptive Job Server auf der Zielwebsite gesendeten Informationen sind umfangreicher, als das zugewiesene Zeitlimit zulässt. Erhöhen Sie das Socket-Timeout auf dem Adaptive Job Server, oder verringern Sie die Anzahl der zu replizierenden Objekte im Replikationsauftrag.

6) Abfrageeinschränkung

Fehlerbeispiel: `SDK-Fehler auf Zielwebsite. Keine gültige Abfrage. (FWB 00025) ...Abfragezeichenfolge überschreitet die maximale Abfragelänge.`

Dieser Fehler kann auftreten, wenn Sie zu viele Objekte gleichzeitig replizieren und Föderation eine Abfrage sendet, die aufgrund der Größe vom CMS nicht verarbeitet werden kann. Objekte von der ursprünglichen Website werden an die Zielwebsite übergeben. Änderungen, die an die ursprüngliche Website übergeben werden müssen, werden jedoch nicht gesendet. Konflikte werden wie angegeben aufgelöst, für das Objekt werden jedoch keine Kennzeichen für die manuelle Auflösung von Konflikten festgelegt. An die Zielwebsite übergebene Objekte funktionieren weiterhin ordnungsgemäß.

Um dieses Problem zu lösen, reduzieren Sie die Anzahl der Objekte, die Sie in einem Replikationsauftrag replizieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

7) Zeitüberschreitung bei Replikationsauftrag

Fehlerbeispiel: `Objekt konnte nicht innerhalb des festgelegten Zeitintervalls zeitgesteuert verarbeitet werden.`

Sie erhalten diese Fehlermeldung u.U., wenn eine Zeitüberschreitung für den Replikationsauftrag aufgetreten ist, während auf die Beendigung eines anderen Replikationsauftrags gewartet wurde. Dieser Fehler kann auftreten, wenn Sie über mehrere Replikationsaufträge verfügen, die gleichzeitig mit derselben ursprünglichen Website verbunden werden. Es wird versucht, den fehlgeschlagenen Replikationsauftrag zum nächsten geplanten Zeitpunkt auszuführen.

Um dieses Problem zu lösen, lassen Sie den fehlgeschlagenen Replikationsauftrag zu einer Zeit verarbeiten, die nicht mit anderen Replikationsaufträgen in Konflikt steht, die mit derselben ursprünglichen Website verbunden sind.

8) Replikationseinschränkung

Fehlerbeispiel: `SDK-Fehler auf Zielwebsite. Datenbank-Zugriffsfehler. …. Interner Abfrageprozessor-Fehler: Bei der Abfrageoptimierung ist nicht genügend Stapelplatz für den Abfrageprozessor vorhanden. Fehler beim Ausführen der Abfrage in ExecWithDeadlockHandling.`

Diese Meldung kann angezeigt werden, wenn Sie die Anzahl der unterstützten Objekte überschreiten, die gleichzeitig repliziert werden können. Um dieses Problem zu lösen, verringern Sie die Anzahl der zu replizierenden Objekte im Replikationsauftrag und führen den Auftrag erneut aus.

9) Objekt gelöscht

Fehlerbeispiel: `Fehler beim Überprüfen von Sicherheitsrechten` oder `Beim Packen des Objekts wurde ein Fehler erkannt.`

Diese Meldung kann angezeigt werden, wenn ein Objekt im Replikationspaket fehlt. Dies ist beispielsweise der Fall, wenn Föderation vor der Überprüfung von Rechten und vor dem Packen des Objekts ein Objekt abfragt, das repliziert werden muss.

10) Adaptive Processing Server

Fehlerbeispiel: `Fehler bei Job Processing Server.`

Dieser Fehler kann auftreten, wenn zu viele Klassen von Föderation geladen werden und nicht genügend Arbeitsspeicher zum Verarbeiten des Replikationsauftrags verfügbar ist.

Um dieses Problem zu lösen, führen Sie die beiden folgenden Schritte aus:

1. Fügen Sie in den Befehlszeilenargumenten des Adaptive Processing Servers folgende Zeile hinzu: `-javaArgs "XX:MaxPermSize=256m"`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Fügen Sie dem Java-Anwendungsserver, zu dem Sie für Föderation eine Verbindung herstellen, folgende Parameter hinzu, um die Größe der verwendeten BIAR-Dateien zu verringern:
   - `-Dbobj.biar.suggestSplit=100m`
   - `-Dbobj.biar.forceSplit=100m`

11) Objekt-Manager-Speicherplatz

Fehlerbeispiel: `Push-Paket konnte nicht erstellt werden. Eingabe-/Ausgabeausnahmefehler: "Kein Speicherplatz auf dem Gerät."`

Dieser Fehler tritt auf, wenn das temporäre von Föderation verwendete Verzeichnis nicht genügend Speicherplatz aufweist. Um dieses Problem zu lösen, geben Sie entweder zusätzlichen Speicher im temporären Verzeichnis frei, oder verwenden Sie einen anderen Speicherort für das temporäre Verzeichnis.

Um einen anderen Speicherort für das temporäre Verzeichnis auf der ursprünglichen Website anzugeben, fügen Sie den Konfigurationsdateien des Java-Anwendungsservers folgende Zeile hinzu: `-Dbobj.tmp.dir=<<TempVerz>>`.

Um einen anderen Speicherort für das temporäre Verzeichnis auf der Zielwebsite anzugeben, fügen Sie den Befehlszeilenargumenten des Adaptive Processing Servers folgende Zeile hinzu: `-javaArgs "-Dbobj.tmp.dir=<TempVerz>"`.

In den vorangehenden Beispielen entspricht `<TempVerz>` dem Speicherort des gewünschten temporären Verzeichnisses.

12) Universumsfehler

Fehlerbeispiel: `Interner Fehler beim Aufrufen der` *processDPCommands*`-API.`

Dieser Fehler tritt auf, wenn ein repliziertes Universum über eine ungültige oder überhaupt keine "Universum-zu-Universumsverbindung"-Beziehung verfügt. Um dieses Problem zu lösen, führen Sie den Replikationsauftrag mit aktivierter Option **Von ursprünglicher Website aus regenerieren** aus und überprüfen, ob die Universumsverbindung repliziert wird.

Alternativ können Sie das Universum in Universe Designer öffnen, die Universumsverbindung bearbeiten und das Universum erneut übergeben.

Weitere Informationen

Optimale Vorgehensweisen [Seite 796]
Einschränkungen der aktuellen Version [Seite 799]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24 Ergänzende Konfigurationen für ERP-Umgebungen

24.1 Konfigurationen für die SAP NetWeaver-Integration

24.1.1 Integrieren in SAP NetWeaver Business Warehouse (BW)

24.1.1.1 Übersicht

In diesem Abschnitt erfahren Sie, wie Sie BW für die Aktivierung und Verwaltung der Berichtsveröffentlichung aus SAP Netweaver Business Warehouse in der BI-Plattform konfigurieren.

Bevor Sie mit diesem Abschnitt beginnen, stellen Sie sicher, dass Sie die Konfiguration des SAP-Authentifizierungs-Plugins in der CMC durchgeführt haben.

Weitere Informationen

Konfigurieren der SAP-Authentifizierung [Seite 299]

24.1.1.1.1 Festlegen von Ordnern und Sicherheitseinstellungen in der BI-Plattform

Beim Festlegen eines Berechtigungssystems in der BI-Plattform erstellt das System eine logische Ordnerstruktur, die dem SAP-System entspricht. Wenn Sie Rollen importieren und Inhalte in der BI-Plattform veröffentlichen, werden entsprechende Ordner erstellt. Als Administrator brauchen Sie diese Ordner nicht zu erstellen. Die Ordner werden automatisch nach der Definition eines Berechtigungssystems erstellt, wenn Sie das SAP-Authentifizierungs-Plugin konfigurieren, Rollen in die CMC importieren und Inhalte in der BI-Plattform veröffentlichen.

Hinweis

Der BI-Plattform-Administrator ist dafür zuständig, diesen Ordnern die richtigen Berechtigungen zuzuweisen:

- *SAP-Ordner der obersten Ebene*

  Stellen Sie sicher, dass die Gruppe "Alle" eingeschränkten Zugriff auf den SAP-Ordner der obersten Ebene hat.
- *System-ID-Ordner*

  Weisen Sie dem Prinzipal "Publisher" folgende Rechte in der CMC zu:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Hinweis

Der Prinzipal "Publisher" ist erst verfügbar, wenn der Inhalt veröffentlicht ist.

- Objekte zum Ordner hinzufügen
- Objekte anzeigen
- Objekte bearbeiten
- Rechte von Benutzern für Objekte ändern
- Objekte löschen

Tipp

Um die Verwaltung von Rechten zu vereinfachen, können Sie eine angepasste Zugriffsberechtigung "Publisher" mit diesen Rechten erstellen und anschließend dem Prinzipal "Publisher" diese Zugriffsberechtigung für die relevanten System-ID-Ordner zuweisen.

Weitere Informationen

Arbeiten mit Zugriffsberechtigungen [Seite 139]
Funktionsweise von Rechten in der BI-Plattform [Seite 124]

24.1.1.1.2 Verstehen der standardmäßigen Ordnersicherheitsmuster

Wenn Sie Inhalte aus SAP auf der BI-Plattform veröffentlichen, erstellt die Plattform automatisch die übrige Hierarchie aus Rollen, Ordnern und Berichten. Das System organisiert die Berichte in Ordnern, deren Namen aus der System-ID, der Clientnummer und dem Rollennamen zusammengesetzt sind.

- Wenn Sie ein Berechtigungssystem definieren, erstellt das System Ordner der obersten Ebene: SAP-, 2.0- und den Systemordner (`<SID>`).
- Wenn eine Rolle von BW aus veröffentlicht wird, erstellt das System nach Bedarf Rollenordner (die als Gruppen in die BI-Plattform importiert werden).
- Das System erstellt einen Inhaltsordner für jede Rolle, unter der Inhalte veröffentlicht werden.
- Jedes Berichtsobjekt ist mit Sicherheitseinstellungen versehen, so dass die Benutzer nur die Berichte anzeigen können, die zu ihren Rollen gehören.

Der Administrator ist dafür zuständig, den Mitgliedern der verschiedenen Rollen Rechte zuzuweisen. Mit der Workbench zur Content-Verwaltung können Sie Berichtsveröffentlichungsfunktionen innerhalb von SAP BW verwalten. Sie können im SAP-BW-System Rollen für bestimmte BI-Plattform-Systeme bestimmen, Berichte veröffentlichen sowie Berichte zwischen SAP BW und einer BI-Plattform-Implementierung synchronisieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Inhaltsordner

Die BI-Plattform importiert eine Gruppe für jede Rolle, die dem Berechtigungssystem wie in der CMC definiert hinzugefügt wird.

Um sicherzustellen, dass allen Mitgliedern einer inhaltsführenden Rolle die geeigneten Standardrechte zugewiesen werden, legen Sie in der Workbench zur Content-Verwaltung die erforderlichen Rechte für jedes Berechtigungssystem fest, das in der BI-Plattform definiert ist. Um die Workbench zur Content-Verwaltung zu starten, führen Sie die Transaktion /CRYSTAL/RPTADMIN aus:

1. Klappen Sie in der Workbench zur Content-Verwaltung **Enterprise-System** und dann **Verfügbare Systeme** auf.
2. Doppelklicken Sie auf das gewünschte System.
3. Klicken Sie auf die Registerkarte **Layout**.
4. Legen Sie **Standardsicherheitsrichtlinie für Reports** auf **Sicht** fest.
5. Legen Sie **Standardsicherheitsrichtlinie für Rollenordner** auf **Sicht auf Abruf** fest.
6. Klicken Sie auf **OK**.

Diese Einstellungen werden in der BI-Plattform für alle Inhaltsrollen übernommen. Darunter versteht man die Rollen, unter denen Inhalte veröffentlicht werden. Mitglieder dieser Rollen sind jetzt in der Lage, zeitgesteuerte Instanzen von Berichten anzuzeigen, die unter anderen Rollen veröffentlicht wurden. Außerdem können sie Berichte regenerieren, die unter Rollen veröffentlicht wurden, denen Sie als Mitglied angehören.

> **Hinweis**
>
> Es wird dringend empfohlen, die Aktivitäten der einzelnen Rollen getrennt zu halten. Obwohl es möglich ist, von einer Administratorrolle aus zu veröffentlichen, sollten Sie nur von Publisher-Rollen aus veröffentlichen. Bei Publisher-Rollen wird lediglich definiert, welche Anwender zum Veröffentlichen von Inhalten berechtigt sind. Diese Rollen sollten daher keine Inhalte enthalten. Publisher sollten in inhaltsführenden Rollen veröffentlichen, die normalen Rollenmitgliedern zugänglich sind.

24.1.1.2 Konfigurieren des BW Publishers

Der BW Publisher ermöglicht es Ihnen, Crystal-Reports-Berichte (RPT-Dateien) einzeln oder stapelweise von BW aus in der BI-Plattform zu veröffentlichen.

Unter Windows können Sie den BW Publisher auf eine der folgenden zwei Weisen konfigurieren:

- Starten von BW Publisher über einen Dienst auf einem Rechner, auf dem die BI-Plattform gehostet wird. Der BW Publisher-Dienst startet bei Bedarf Instanzen von BW Publisher.
- Starten von BW Publisher über ein lokales SAP-Gateway zum Erstellen von BW Publisher-Instanzen.

Sie müssen die Konfigurationsmethode abhängig von den jeweiligen Standortanforderungen auswählen, nachdem Sie die Vor- und Nachteile der einzelnen Konfigurationen sorgfältig abgewogen haben. Nachdem Sie BW Publisher in der BI-Plattform konfiguriert haben, müssen Sie die Veröffentlichungsfunktion in der Workbench zur Content-Verwaltung konfigurieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.3 Konfigurieren von BW Publisher als Dienst

In diesem Abschnitt wird erläutert, wie Sie die Veröffentlichung von Berichten aus BW in der BI-Plattform mithilfe von BW Publisher als Dienst ermöglichen.

24.1.1.3.1 Verteilen der BW Publisher-Installation

In diesem Abschnitt wird die Verteilung vom BW Publisher-Dienst erläutert und wie Sie BW Publisher von anderen BusinessObjects Business-Intelligence-Komponenten trennen.

Sie erzielen bei der Berichtsveröffentlichung über BW eine Lastenverteilung, indem Sie BW-Publisher-Dienste im selben BI-Plattform-System auf zwei getrennten Rechnern installieren.

Wenn Sie den BW Publisher auf den Rechnern installieren, die die BI-Plattform hosten, konfigurieren Sie diese mit identischen Programm-IDs, SAP-Gateway-Hosts und -Gateway-Services. Nachdem Sie eine RFC-Destination mit der betreffenden Programm-ID erstellt haben, wird die Berichtsveröffentlichung von BW gleichmäßig auf die Rechner verteilt, die die BI-Plattform hosten. Zudem nutzt BW den verbleibenden BW Publisher, wenn ein BW Publisher nicht mehr verfügbar ist.

Sie können die verbesserte Systemredundanz auf jede Konfiguration ausdehnen, die mehrere BW-Anwendungsserver umfasst. Konfigurieren Sie jeden BW-Anwendungsserver für die Ausführung eines SAP-Gateways. Installieren Sie dafür jeweils einen separaten BW-Publisher-Dienst auf einem Rechner, der die BI-Plattform hostet. Konfigurieren Sie jeden BW Publisher-Dienst für die Verwendung des Gateway-Hosts und Gateway-Diensts eines separaten BW-Anwendungsservers. In dieser Konfiguration kann die Veröffentlichung aus BW fortgesetzt werden, wenn BW Publisher oder ein Anwendungsserver ausfällt.

Wenn BW Publisher getrennt von anderen BI-Plattform-Komponenten ausgeführt werden soll, installieren Sie BW unter Verwendung eines eigenständigen SAP-Gateways.

In diesem Fall müssen Sie auf demselben Computer, auf dem BW Publisher vorhanden ist, ein lokales SAP-Gateway installieren. Außerdem muss BW Publisher auf das BI-Plattform-SDK und das Crystal-Reports-Druckmodul zugreifen können. Daher muss auch der SIA-Server installiert werden, wenn Sie BW Publisher und den lokalen SAP Gateway auf einem dedizierten Rechner installieren.

24.1.1.3.2 Starten von BW Publisher: UNIX

Führen Sie das BW Publisher-Skript aus, um eine oder mehrere Publisher-Instanzen zur Verarbeitung von Veröffentlichungsanforderungen zu erstellen. Es wird empfohlen, eine Publisher-Instanz zu starten.

Nach dem Starten von BW Publisher wird eine Verbindung mit dem SAP-Gateway-Dienst hergestellt, den Sie bei Ausführung des BI-Plattform-Installationsprogramms angegeben haben.

24.1.1.3.3 Starten von BW Publisher: Windows

Unter Windows verwenden Sie den Central Configuration Manager™ (CCM), um den BW Publisher-Dienst zu starten. Beim Starten des BW Publisher-Dienstes wird eine Publisher-Instanz erstellt, um

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Veröffentlichungsanforderungen des BW-Systems zu bedienen. Wenn die Anzahl der Veröffentlichungsanforderungen zunimmt, erstellt BW Publisher automatisch weitere Publisher, um dem Bedarf gerecht zu werden.

24.1.1.3.4 Konfigurieren eines Zieles für den BW Publisher-Dienst

Um BW Publisher verwenden zu können, müssen Sie eine RFC-Destination auf dem BW-Server konfigurieren, damit eine Kommunikation mit dem BW Publisher-Dienst möglich ist. Wenn Sie über einen BW-Cluster verfügen, konfigurieren Sie die RFC-Destination auf jedem Server, wobei Sie jeweils die zentrale Instanz von BW als Gateway Host verwenden.

Wenn Sie Berichte aus BW in mehreren BI-Plattform-Systemen veröffentlichen möchten, erstellen Sie eine separate RFC-Destination für den BW Publisher-Dienst der einzelnen BI-Plattform-Implementierungen. Für jedes Ziel müssen eindeutige Programm-IDs verwendet werden. Gateway-Host und Gateway-Service sind dagegen identisch.

24.1.1.3.5 Konfigurieren von BW Publisher mit einem lokalen SAP-Gateway

> **Hinweis**
>
> Verwenden Sie diese Konfiguration nicht, wenn die BI-Plattform unter UNIX installiert ist. Die Verwendung dieser Methode unter UNIX könnte ein unerwartetes Systemverhalten verursachen.

Um die Veröffentlichung von Berichten aus BW in der BI-Plattform mithilfe eines lokalen SAP-Gateways zu ermöglichen, gehen Sie wie folgt vor:

- *Installieren eines lokalen SAP-Gateways* [Seite 808].
- *Konfigurieren eines Zieles für BW Publisher* [Seite 809].

24.1.1.3.6 Installieren eines lokalen SAP-Gateways

Auf dem Computer, auf dem Sie BW Publisher installiert haben, müssen Sie auch ein lokales SAP-Gateway installieren. Es empfiehlt sich, dass ein SAP BASIS-Administrator die Installation eines dieser SAP-Gateways vornimmt.

Die aktuellste Anleitung zur Installation eines lokalen SAP-Gateways finden Sie in den Anweisungen zur SAP-Installation auf der SAP Presentation-CD.

Eine ausführliche Liste der getesteten Umgebungen finden Sie in der Product Availability Matrix (PAM) unter *http://service.sap.com/pam*. Die PAM umfasst bestimmte Versions- und Service Pack-Anforderungen für Anwendungsserver, Betriebssysteme, SAP-Komponenten usw.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Nachdem Sie das SAP-Gateway installiert haben, überprüfen Sie die Registrierungseinträge `TMP` und `TEMP` unter dem Unterschlüssel `HKEY_CURRENT_USER\Environment` mithilfe von `regedit`. Beide Registrierungseinträge sollten denselben Wert aufweisen. Dabei muss es sich um einen gültigen absoluten Verzeichnispfad handeln. Sollte einer der Einträge die Variable `%USERPROFILE%` enthalten, ersetzen Sie diese durch den absoluten Verzeichnispfad. In der Regel sind beide Registrierungseinträge auf `C:\WINDOWS\TEMP` gesetzt.

24.1.1.4 Konfigurieren eines Zieles für BW Publisher

Damit BW Publisher verwendet werden kann, müssen Sie eine RFC-Destination konfigurieren, um BW die Adresse des Computers mitzuteilen, auf dem das lokale SAP-Gateway und BW Publisher installiert wurden.

24.1.1.5 Konfigurieren von Veröffentlichungsfunktionen in der Workbench zur Content-Verwaltung

Mit der Workbench zur Content-Verwaltung können Sie Berichtsveröffentlichungsfunktionen innerhalb von SAP BW verwalten. Sie können im SAP-BW-System Rollen für bestimmte BI-Plattform-Systeme bestimmen, Berichte veröffentlichen sowie Berichte zwischen SAP BW und einer BI-Plattform-Implementierung synchronisieren. Nachdem Sie die SAP-Authentifizierung eingerichtet und BW Publisher konfiguriert haben, führen Sie die in diesem Abschnitt angegebenen Funktionen aus, um die Veröffentlichung zu ermöglichen. Diese Hinweise decken folgende Bereiche ab:

- Festlegen entsprechender Autorisierungen für unterschiedliche Benutzer der Workbench zur Content-Verwaltung
- Einrichten von Verbindungen mit der BI-Plattform, in der Inhalte veröffentlicht werden.
- Festlegen, welche Rollen in welcher BI-Plattform veröffentlichen können.
- Veröffentlichen von Inhalten von der BW- auf der BI-Plattform.

24.1.1.6 Benutzer mit Zugriff auf die Workbench zur Content-Verwaltung

Es gibt drei Benutzertypen, die auf die Workbench zur Content-Verwaltung zugreifen können:

- Nutzer von Inhalten, die inhaltsführenden Rollen angehören und die Berichte anzeigen können. Sie sind lediglich dazu berechtigt, Berichte anzuzeigen.
- BI-Plattform-Content Publisher, die Berichte in BW anzeigen, veröffentlichen, ändern und (optional) löschen können.
- BI-Plattform-Administratoren, die alle Aufgaben innerhalb der Workbench zur Content-Verwaltung ausführen können. Diese Aufgaben umfassen das Definieren von BI-Plattform-Systemen, die Veröffentlichung von Berichten und die Durchführung der Berichtsverwaltung.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.7 Erstellen von Rollen in BW für Content Publisher

Wenn Sie BW für die Integration in der BI-Plattform konfigurieren, sollten Sie herausfinden, ob Ihre aktuelle Rollenstruktur es unterstützt, bestimmte BW-Benutzer schnell als Content Publisher oder Systemadministratoren für die BI-Plattform-Systeme zu bestimmen.

Es wird empfohlen, allen neuen Rollen einen beschreibenden Namen zu geben. Beispiele von beschreibenden Rollennamen sind: `BOE_CONTENT_PUBLISHERS` und `SBOP_SYSTEM_ADMINISTRATORS`.

> **Tipp**
>
> Sie können einem Administrator entweder volle Systemverwaltungsrechte oder einen Teil dieser Rechte gewähren.

Um die Rechte dieser neuen (oder einer vorhandenen) Rolle in der BI-Plattform zu ändern, müssen Sie zunächst die SAP-Authentifizierung einrichten und anschließend die Rollen importieren. Danach können Sie die Rechte jeder importierten Rolle über die Central Management Console ändern.

Einzelheiten zur Erstellung von Rollen finden Sie in Ihrer SAP-Dokumentation. Weitere Informationen zur Verwendung von Rollen für die Inhaltsverwaltung finden Sie in den folgenden Abschnitten:

- *Importieren von SAP-Rollen* [Seite 307].
- *Festlegen von Ordnern und Sicherheitseinstellungen in der BI-Plattform* [Seite 804].
- *Verstehen der standardmäßigen Ordnersicherheitsmuster* [Seite 805].

24.1.1.8 Konfigurieren des Zugriffs auf die Workbench zur Content-Verwaltung

Für jeden Benutzertyp, der Zugriff auf die Workbench zur Content-Verwaltung hat, müssen Sie innerhalb von BW die gewünschten Autorisierungen festlegen. Die Autorisierungen sind in den folgenden Tabellen aufgeführt:

Tabelle 22: Autorisierungen für Administratoren

Berechtigungsobjekt	Feld	Werte
S_RFC S_TCODE	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	Ausführen (16)
	TCD	/CRYSTAL/RPTADMIN, RSCR_MAINT_PUBLISH
S_TABU_CLI	CLIIDMAINT	X
S_TABU_DIS	ACTVT	Ändern, Anzeigen (02, 03)

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Berechtigungsobjekt	Feld	Werte
	DICBERCLS	&NC&
	JOBACTION	DELE, RELE
	JOBGROUP	' '
S_RS_ADMWB	ACTVT	Ausführen (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Neu erstellen, Ändern, Anzeigen, Löschen (01, 02, 03, 06)
ZCNTADMJOB	ACTVT	Neu erstellen, Löschen (01, 06)
ZCNTADMRPT	ACTVT	Anzeigen, Löschen, Aktivieren, Verwalten, Überprüfen (03, 06, 07, 23, 39)

Tabelle 23: Autorisierungen für Content Publisher

Berechtigungsobjekt	Feld	Werte
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	Ausführen (16)
	TCD	/CRYSTAL/RPTADMIN
S_BTCH_JOB	JOBACTION	DELE, RELE
	JOBGROUP	' '
	ACTVT	Ausführen (16)
	RSADMWBOBJ	WORKBENCH
ZCNTADMCES	ACTVT	Anzeigen (03)
ZCNTADMJOB	ACTVT	(Neu, Löschen) 01, 06
ZCNTADMRPT	ACTVT	Anzeigen, Aktivieren, Verwalten, Überprüfen (03, 07, 23, 39) Löschen (optional) (06) Bearbeiten (optional) (02)

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Optional kann Content Publishern das Recht zum Löschen von Berichten in der BW-Workbench zur Content-Verwaltung gewährt werden. Dabei sollten Sie jedoch beachten, dass durch das Löschen eines Berichts in BW der Bericht auch in der BI-Plattform gelöscht wird. Wenn Veröffentlicher nicht über die erforderlichen Rechte zum Löschen von Berichten in der BI-Plattform verfügen, tritt ein Fehler auf.

Autorisierungen für Nutzer von Inhalten

Berechtigungsobjekt	Feld	Werte	
S_RFC	RFC_TYPE	FUGR	
	RFC_NAME	SH3A, SUNI	
	ACTVT	Ausführen (16)	
		TCD	/CRYSTAL/RPTADMIN
S_RS_ADMWB	ACTVT	Ausführen (16)	
	RSADMWBOBJ	WORKBENCH	
		ACTVT	Anzeigen (03)

24.1.1.9 Definieren eines BI-Plattform-Systems

Sie müssen innerhalb der Workbench für Inhaltsverwaltung eine Systemdefinition für jedes BI-Plattform-System erstellen, in dem Berichte veröffentlicht werden sollen.

24.1.1.9.1 Hinzufügen eines BI-Plattform-Systems

1. Führen Sie die Transaktion `/crystal/rptadmin` aus, um zur Workbench für Inhaltsverwaltung zu gelangen.
2. Wählen Sie im Fenster **Operationen** die Option **Enterprise-System**.
3. Doppelklicken Sie auf **Neues System hinzufügen**.
4. Auf der Registerkarte **System**:
   - Geben Sie einen beschreibenden Namen in das Feld **Alias** ein. Vermeiden Sie Leer- oder Sonderzeichen, da diese Zeichen eine spezielle Behandlung erfordern, wenn der Aliasname bei der Konfiguration von Enterprise Portals verwendet wird.
   - Geben Sie den Namen des Rechners ein, auf dem Ihr CMS ausgeführt wird. Wenn Sie Ihrem CMS eine von der Standardeinstellung abweichende Portnummer zugewiesen haben, geben Sie **CMSNAME : PORT** ein.
   - Wählen Sie **Standardsystem** aus, wenn in diesem System Berichte aus jeder Rolle veröffentlicht werden sollen, die einem BI-Plattform-System nicht ausdrücklich zugewiesen wurde. Es kann nur ein BI-Plattform-System als Standardsystem angegeben werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

In der Liste aller verfügbaren Systeme ist das Standardsystem durch ein grünes Häkchen gekennzeichnet.

5. Klicken Sie auf **Speichern**.
6. Fügen Sie auf der Registerkarte **RFC-Destination** jede RFC-Destination hinzu, die diesem System zugeordnet ist.

   Um ein Ziel hinzuzufügen, klicken Sie auf die Schaltfläche **Zeile einfügen**. Doppelklicken Sie in der angezeigten Liste auf den Namen der RFC-Destination.

   > **Hinweis**
   >
   > Ein BI-Plattform-System kann mehrere Destinations aufweisen, wodurch Systemredundanz hinzugefügt wird. Weitere Informationen finden Sie unter "Verteilen der BW-Publisher-Installation".

7. Aktivieren Sie das Kontrollkästchen neben dem hinzugefügten Zielnamen, und klicken Sie auf **BOE-Definition verifizieren**.

   Mit diesem Test wird überprüft, ob BW eine Verbindung mit dem angegebenen BW Publisher herstellen und sich über das Benutzerkonto mit Crystal-Berechtigung bei diesem System anmelden kann.
8. Auf der Registerkarte **HTTP**:
   - Geben Sie in das Feld **Protokoll** `http` oder `https` ein, wenn der mit der BI-Plattform verbundene Webserver für HTTPS konfiguriert ist.
   - Geben Sie in das Feld für den **Webserver-Host und -Port** den vollständig qualifizierten Domänennamen oder die IP-Adresse des Webservers ein, auf dem BI-Launchpad gehostet wird. Geben Sie bei einer Installation, die einen Java-Anwendungsserver verwendet, die Portnummer an. Geben Sie zum Beispiel `boserver01.businessobjects.com:8080` ein.
   - Geben Sie im Feld **Pfad** den Eintrag `SAP` ein

     Bei diesem Pfad handelt es sich im Grunde um den virtuellen Pfad, den der Webserver beim Verweis auf den Unterordner `sap` des BI-Plattform-Webinhalts verwendet. Geben Sie nur einen anderen Wert ein, wenn Sie Ihre Webumgebung und den Speicherort der Dateien, die die Plattform-Webinhalte enthalten, individuell angepasst haben.
     Fügen Sie keinen Schrägstrich am Anfang oder Ende dieses Eintrags ein.
   - Geben Sie in das Feld für die **Viewer-Anwendung** den Namen Ihrer Viewer-Anwendung ein.

     Geben Sie `openDocument.jsp` ein, um den Standard-Viewer für die BI-Plattform zu verwenden, bei dem die Java-Version von BI-Launchpad verwendet wird.

     Wenn die BI-Plattform mit der `ASP.NET`-Standardkonfiguration unter Windows installiert wurde, geben Sie `report/report_view.aspx` ein, um den Standardbrowser zu verwenden.
9. Wählen Sie auf der Registerkarte **Sprachen** die Sprachen von Berichten aus, die in diesem System veröffentlicht werden.
10. Fügen Sie auf der Registerkarte **Rollen** die inhaltsführenden Rollen hinzu, die diesem BI-Plattform-System zugeordnet werden sollen.

    Siehe "Importieren von SAP-Rollen"
11. Klicken Sie auf die Schaltfläche **Zeile einfügen**.

    Es wird eine Liste von Rollen angezeigt, die diesem System hinzugefügt werden können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Jede Rolle kann nur in einem BI-Plattform-System veröffentlichen. Wenn die Rollen, die Sie diesem BI-Plattform-System hinzufügen möchten, nicht in der Liste angezeigt werden, klicken Sie auf **Abbrechen**, um zur Registerkarte **Rollen** zurückzukehren, und klicken auf die Option **Rollen neu zuordnen**.

12. Wählen Sie die Rollen aus, die in diesem System veröffentlicht werden sollen, und klicken Sie auf **OK**.
13. Wählen Sie auf der Registerkarte **Layout** die Standardsicherheitseinstellungen von Berichten und Rollenordnern aus, die in diesem BI-Plattform-System veröffentlicht werden.

> **Hinweis**
>
> Für jede in diesem System veröffentlichte Rolle wird automatisch ein Ordner in der BI-Plattform erstellt. Der Ordner enthält Verknüpfungen zu den unter dieser Rolle veröffentlichten Berichten.

> **Hinweis**
>
> Nachdem Sie ein BI-Plattform-System konfiguriert haben, wirken sich Änderungen an den Standardsicherheitsebenen nicht mehr auf die Sicherheitsebenen veröffentlichter Rollenorder oder Berichte aus. Um die Standardsicherheitsebenen für alle Rollen und Inhalte zu ändern, die auf der Plattform veröffentlicht werden, löschen Sie die Rollenordner und Verknüpfungen im System. (Die eigentlichen Berichte werden dadurch nicht gelöscht.) Anschließend ändern Sie die Sicherheitseinstellungen und veröffentlichen die Rollen und Berichte erneut.

14. Klicken Sie im unteren Bereich auf **OK**, um die Einstellungen zu speichern und das BI-Plattform-System in der Workbench für Inhaltsverwaltung zu erstellen.

Jetzt können Sie Berichte aus BW in der BI-Plattform veröffentlichen.

Weitere Informationen

Verteilen der BW Publisher-Installation [Seite 807]
Importieren von SAP-Rollen [Seite 307]

24.1.1.10 Veröffentlichen von Berichten mit der Workbench zur Content-Verwaltung

Nachdem ein Bericht in BW gespeichert wurde, können Sie diesen mithilfe der Workbench zur Content-Verwaltung veröffentlichen. Sie können die Workbench zur Content-Verwaltung verwenden, um einzelne Berichte zu veröffentlichen, oder Sie können alle in einer bestimmten Rolle gespeicherten Berichte veröffentlichen. Die Workbench zur Content-Verwaltung kann nur von Benutzern verwendet werden, die über die Autorisierungen eines Crystal-Content-Publishers verfügen (siehe*Erstellen und Übertragen von Autorisierungen* [Seite 831]).

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.11 Veröffentlichen von Rollen oder Berichten

1. Führen Sie die Transaktion `/crystal/rptadmin` aus, um zur Workbench zur Content-Verwaltung zu gelangen.
2. Wählen Sie im Fenster **Operationen** die Option **Berichte veröffentlichen**.
3. Um nach Inhalten zu suchen, die im BW-System gespeichert sind, doppelklicken Sie auf **Wählen Sie zu veröffentlichende Berichte und Rollen aus**.

   Es wird ein Dialogfeld angezeigt, mit dessen Hilfe Sie die verfügbaren Rollen und Berichte filtern können.
4. Wählen Sie aus der Liste das System bzw. die Systeme mit den anzuzeigenden Inhalten aus.

   > **Hinweis**
   >
   > Die Liste umfasst alle verfügbaren Systeme, die im BW-System definiert sind.
5. Als Nächstes filtern Sie die Ergebnisse, um die Anzahl der angezeigten Berichte und Rollen einzuschränken. Verwenden Sie die folgenden Optionen:
   - **Objektversion**

     Bei Auswahl von "A: aktiv" werden alle Berichte angezeigt, die veröffentlicht werden können. Bei Auswahl der leeren Option werden alle Berichte angezeigt. (Die übrigen Optionen sind für SAP reserviert.)
   - **Objektstatus**

     Wählen Sie "ACT aktiv, ausführbar" aus, um nur veröffentlichte Berichte anzuzeigen. Wählen Sie "INA inaktiv, nicht ausführbar" aus, um nur nicht veröffentlichte Berichte anzuzeigen. Lassen Sie das Feld leer, um alle Berichte anzuzeigen. (Die übrigen Optionen sind für SAP reserviert.)
   - **Rollenfilter**

     Wenn Sie Text in dieses Feld eingeben, werden nur die Rollen angezeigt, die dieser Eingabe entsprechen. Verwenden Sie * als Platzhalterzeichen. Um beispielsweise alle Rollen anzuzeigen, die mit dem Buchstaben "d" beginnen, geben Sie "d*" ein.
   - **Berichtsbeschreibung**

     Wenn Sie Text in dieses Feld eingeben, werden nur die Berichte angezeigt, deren Beschreibungen dieser Eingabe entsprechen. Verwenden Sie * als Platzhalterzeichen für eine beliebige Anzahl von Zeichen. Verwenden Sie + als Platzhalterzeichen für 0 oder 1 Zeichen. Um beispielsweise alle Berichte anzuzeigen, deren Beschreibung das Wort "Ertrag" enthält, geben Sie "*ertrag*" ein.
6. Klicken Sie auf **OK**.

   Die Liste der Berichte, die den Kriterien entsprechen, wird im rechten Fenster angezeigt.
   Die Berichte werden hierarchisch angeordnet: BI-Plattform-System > Rollen in diesem System > Berichte, die für die Rollen gespeichert sind.
   Jedes Element in der Hierarchie ist mit einem roten, gelben oder grünen Punkt gekennzeichnet. Elemente, die sich auf einer höheren Hierarchieebene befinden, geben den Status der enthaltenen Elemente wieder, wobei die ungünstigste Bedingung oben in der Hierarchie aufgeführt ist. Wenn ein Bericht in einer Rolle beispielsweise gelb (aktiv) ist, während alle anderen Berichte grün (veröffentlicht) sind, weist die Rolle einen gelben Punkt (aktiv) auf.
   - Grün: Das Element ist vollständig veröffentlicht. Wenn es sich bei dem Element um ein BI-Plattform-System oder eine Rolle handelt, sind alle Berichte in diesem Element veröffentlicht.
   - Gelb: Das Element ist aktiv, aber nicht veröffentlicht. Wenn es sich bei dem Element um einen Bericht handelt, ist es für die Veröffentlichung verfügbar. Handelt es sich bei dem Element um eine Rolle

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

oder ein BI-Plattform-System, ist der gesamte Inhalt aktiv und mindestens ein Element, das in der Rolle oder im System enthalten ist, nicht veröffentlicht.

- Rot: Das Element entspricht einem SAP-Inhalt und kann nicht mithilfe der Workbench zur Content-Verwaltung veröffentlicht werden. Die Inhalte können erst veröffentlicht werden, nachdem sie über die BW-Workbench zur Content-Verwaltung aktiviert wurden.

7. Wählen Sie die Berichte aus, die Sie veröffentlichen möchten.

   Um alle Berichte in einer Rolle zu veröffentlichen, wählen Sie die Rolle aus. Um alle Rollen in einem BI-Plattform-System zu veröffentlichen, wählen Sie das System aus.

   > **Hinweis**
   >
   > Wenn Sie eine Rolle (oder ein System) auswählen, werden alle in dieser Rolle (bzw. in diesem System) enthaltenen Berichte ausgewählt. Um diese Auswahl aufzuheben, deaktivieren Sie das Kontrollkästchen für die Rolle (oder das System) und klicken anschließend auf "Regenerieren".

8. Klicken Sie auf **Veröffentlichen**.

   > **Hinweis**
   >
   > Im Hintergrund veröffentlichte Berichte werden verarbeitet, sobald Systemressourcen verfügbar sind. Um diese Option zu verwenden, klicken Sie anstatt auf **Veröffentlichen** auf **Im Hintergrund**.

9. Klicken Sie auf **Regenerieren**, um die Anzeige des Status von BI-Plattform-Systemen, -Rollen und -Berichten in der Workbench zur Content-Verwaltung zu aktualisieren.

   > **Tipp**
   >
   > Um einen Bericht anzuzeigen, klicken Sie mit der rechten Maustaste auf den Bericht und wählen **Ansicht**. Um festzustellen, welche Querys vom Bericht verwendet werden, klicken Sie mit der rechten Maustaste auf den Bericht und wählen **Verwendete Querys**.

   > **Hinweis**
   >
   > Wenn Sie nach dem Veröffentlichen eines Berichts in der BI-Plattform den veröffentlichten Bericht überschreiben möchten, klicken Sie auf **Überschreiben**.

Weitere Informationen

Zeitgesteuertes Verarbeiten der Veröffentlichung im Hintergrund [Seite 817]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.12 Zeitgesteuertes Verarbeiten der Veröffentlichung im Hintergrund

Die Veröffentlichung von Berichten im Hintergrund zur sofortigen oder für einen späteren Zeitpunkt festgelegten Ausführung schont die Systemressourcen. Es wird empfohlen, Berichte im Hintergrund zu veröffentlichen, um die Reaktionsfähigkeit des Systems zu verbessern.

Beim regelmäßigen Veröffentlichen von Berichten in Form zeitgesteuerter Aufträge werden die Berichtsinformationen zwischen BW und der BI-Plattform-Implementierung synchronisiert. Es wird empfohlen, alle Berichte (bzw. Rollen, in denen diese Berichte enthalten sind) zeitgesteuert zu verarbeiten. Sie können Rollen und Berichte mithilfe der Option "Aktualisierungsstatus" im Rahmen der Operation "Berichtsverwaltung" auch manuell synchronisieren. Ausführliche Informationen finden Sie unter *Aktualisieren des Berichtstatus* [Seite 817].

24.1.1.13 Aktualisieren von Systeminformationen für veröffentlichte Berichte

BW Publisher verwendet die hier eingegebenen SAP-Systeminformationen zur Aktualisierung der Datenquelle veröffentlichter Berichte. Sie können auswählen, ob der lokale BW-Anwendungsserver verwendet werden soll oder die zentrale BW-Instanz, sofern Sie eine Konfiguration mit Lastenverteilung bevorzugen.

24.1.1.14 Verwalten von Berichten

Berichtsverwaltungsaufgaben umfassen die Synchronisierung von Informationen zu Berichten zwischen der BI-Plattform und BW (Aktualisierungsstatus), das Löschen unerwünschter Berichte (Berichte löschen) sowie die Aktualisierung von Berichten, die aus früheren Versionen der Plattform migriert wurden (Post-Migration).

24.1.1.14.1 Aktualisieren des Berichtstatus

Wenn Sie in einem BI-Plattform-System Änderungen für einen veröffentlichten Bericht vornehmen (beispielsweise die Rolle ändern, in der ein Bericht veröffentlicht wird), wird diese Änderung erst bei der Synchronisierung zwischen der BI-Plattform und BW in BW übernommen. Sie können die zeitgesteuerte Verarbeitung eines Veröffentlichungsauftrags für eine regelmäßige Synchronisierung zwischen der BI-Plattform und BW einrichten (siehe *Zeitgesteuertes Verarbeiten der Veröffentlichung im Hintergrund* [Seite 817]), oder den Berichtstatus manuell mithilfe des Tools "Berichtsverwaltung" aktualisieren.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.14.2 Löschen von Berichten

Beim Löschen eines veröffentlichten Berichts aus BW mithilfe der Workbench zur Content-Verwaltung wird der Bericht auch aus der BI-Plattform gelöscht. Nur Benutzer, die über die erforderlichen Autorisierungen zum Löschen von Berichten sowohl in BW als auch im BI-Plattform-System verfügen, können Berichte entfernen.

> **Hinweis**
>
> Wenn ein Benutzer über Rechte zum Löschen eines Berichts in BW verfügt, jedoch nicht über Rechte zum Löschen in dem BI-Plattform-System, in dem dieser Bericht veröffentlicht wurde, kann ein Fehler auftreten.

24.1.1.15 Konfigurieren des SAP HTTP-Anforderungshandlers

Um die Anzeige von Berichten in BW zu ermöglichen, müssen Sie BW für die Verwendung des HTTP-Anforderungshandlers konfigurieren, der in der Workbench zur Content-Verwaltung enthalten ist. Wenn ein Benutzer dann über das SAPGUI einen Crystal-Reports-Bericht öffnet, kann BW die Anzeigeanforderung über das Web an die richtige Stelle weiterleiten.

Verwenden Sie die Transaktion "SICF", um auf die Liste der virtuellen Hosts und Dienste zuzugreifen, die im BW-System aktiv sind. Erstellen Sie unter BW in der Hierarchie `default_host` einen neuen Knoten mit dem Namen `ce_url`, und fügen Sie der Handlerliste `/CRYSTAL/CL_BW_HTTP_HANDLER` hinzu. Nach der Erstellung müssen Sie diesen Dienst möglicherweise manuell aktivieren.

24.1.1.16 Konfigurationen für die Verarbeitung von SAP-Daten

24.1.1.16.1 Verarbeiten zeitgesteuerter Berichte im SAP-Batchmodus

Bei Windows-Installationen können für die zeitgesteuerte Verarbeitung vorgesehene Berichte in der BI-Plattform im SAP-Batchmodus ausgeführt werden. Die InfoSet- und Open SQL-Treiber können Berichte im SAP-Batch- oder Hintergrundmodus ausführen, sofern bestimmte Umgebungsvariablen auf 1 gesetzt sind. Die relevanten Umgebungsvariablen lauten:

- `CRYSTAL_INFOSET_FORCE_BATCH_MODE` (für den InfoSet-Treiber)
- `CRYSTAL_OPENSQL_FORCE_BATCH_MODE` (für den Open SQL-Treiber)

Die Verwendung dieser Funktion wird jedoch nur in verteilten BI-Plattform-Installationen empfohlen. Wenn diese Umgebungsvariablen auf 1 gesetzt sind, führen die Treiber Berichte im SAP-Batchmodus aus – unabhängig von der Berichtskomponente, die den Bericht tatsächlich ausführt. Wenn Sie daher diese Umgebungsvariablen als Systemumgebungsvariablen eines Rechners erstellen, auf dem eine Kombination aus BI-Plattform-Servern verwendet wird, so führen die Treiber sämtliche Berichte im Batchmodus aus (einschließlich Berichtsanforderungen auf Abruf vom Crystal Reports Processing Server und vom Report Application Server).

Um sicherzustellen, dass die Treiber nur Ihre zeitgesteuerten Berichte im Batchmodus ausführen (Berichte, die vom Adaptive Job Server ausgeführt werden), sollten Sie keine Systemumgebungsvariablen auf Rechnern mit

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

einer Kombination aus BI-Plattform-Servern festlegen. Passen Sie anhand dieser Schritte stattdessen die Umgebungsvariablen für die einzelnen Adaptive Job Server an.

> **Hinweis**
>
> SAP-Benutzer, die die zeitgesteuerte Verarbeitung von Berichten in der BI-Plattform einrichten, benötigen möglicherweise zusätzliche Berechtigungen in SAP.

Weitere Informationen

Zeitgesteuertes Verarbeiten eines Berichts im Batchmodus anhand einer Open SQL-Query [Seite 846]

24.1.1.16.2 So führen Sie die zeitgesteuerte Verarbeitung von Berichten im SAP-Batchmodus aus

1. Erstellen Sie ein Batchskript (`.bat`-Datei) in einem Texteditor, beispielsweise dem Editor, mit folgendem Inhalt:

   ```
   @echo off
   set CRYSTAL_INFOSET_FORCE_BATCH_MODE=1
   set CRYSTAL_OPENSQL_FORCE_BATCH_MODE=1
   %*
   ```

   Durch dieses Skript werden die Umgebungsvariablen auf 1 gesetzt und anschließend alle Parameter ausgeführt, die von der Befehlszeile aus an das Skript übergeben werden.
2. Speichern Sie die Datei unter dem Namen `jobserver_batchmode.bat` in einem Ordner auf jedem Adaptive-Job-Server-Rechner.
3. Melden Sie sich bei der Central Management Console (CMC) an.
4. Wählen Sie **Server** aus.
5. Klappen Sie den Knoten **Dienstkategorien** auf, und wählen Sie **Analysis-Dienste** aus.
6. Wählen Sie **Adaptive Processing Server** und dann **Eigenschaften** im Kontextmenü aus.
   Die Seite *Eigenschaften* wird geöffnet.
7. Suchen Sie auf der Seite *Eigenschaften* nach dem Feld **Befehlszeilenparameter**.

   Dies ist der Startbefehl für den Adaptive Job Server. Beispiel:

   ```
   "\\SERVER01\C$\Programme\SAO Business Objects\SAP BusinessObjects Enterprise
   \win32_x86\JobServer.exe" -service -name SERVER01.report -ns SERVER01 -objectType
   BusinessObjects Enterprise.Report -lib procReport -restart
   ```
8. Stellen Sie dem Standardbefehl den vollständigen Pfad zur Datei `jobserver_batchmode.bat` voran, die Sie auf dem Rechner mit dem Adaptive Job Server gespeichert haben.

   In diesem Beispiel wurde die Batchdatei auf dem Rechner "SERVER01" in folgendem Pfad gespeichert:

   ```
   C:\Crystal Scripts\jobserver_batchmode.bat
   ```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Der neue Startbefehl für den Adaptive Job Server lautet folgendermaßen:

```
"\\SERVER01\C$\Crystal Scripts\jobserver_batchmode.bat" "\\SERVER01\C$\Program
Files\SAP Business Objects\SAP
BusinessObjects Enterprise 12.0\win32_x86\JobServer.exe" -service -name
SERVER01.report  -ns SERVER01
-objectType BusinessObjects Enterprise.Report -lib procReport  -restart
```

Dieser neue Startbefehl startet zunächst die Batchdatei. Die Batchdatei wiederum stellt die erforderlichen Umgebungsvariablen ein, bevor der ursprüngliche Startbefehl für den Adaptive Job Server ausgeführt wird. Auf diese Weise wird sichergestellt, dass die Umgebungsvariablen, die dem Adaptive Job Server zur Verfügung stehen, sich von den Umgebungsvariablen unterscheiden, die Servern zur Berichterstellung auf Abruf (dem Crystal Reports Processing Server und dem Report Application Server) bereitgestellt werden.

9. Klicken Sie auf **Speichern und schließen**.
10. Klicken Sie mit der rechten Maustaste auf den Adaptive Job Server, und wählen Sie **Starten** im Kontextmenü aus.

> **Hinweis**
>
> Wenn der Adaptive Job Server nicht gestartet werden kann, überprüfen Sie den neuen Startbefehl.

24.1.1.17 Konfigurationen für SAP-Transporte

24.1.1.17.1 Übersicht

Die BI-Plattform umfasst folgende Transporte:

- Open SQL Connectivity-Transport
- InfoSet Connectivity-Transport
- Transport zur Sicherheitsdefinition auf Zeilenebene
- Transportdatei für die Clusterdefinition
- Transportdatei für die Workbench zur Content-Verwaltung
- Transportdatei für die Personalisierung von BW-Query-Parametern
- MDX-Transport
- ODS-Transport

Es gibt zwei verschiedene Arten von Transportdateien: Unicode-kompatible und ANSI-Transportdateien. Wenn Sie ein BASIS-System der Version 6.20 oder höher einsetzen, verwenden Sie die Unicode-kompatiblen Transportdateien. Für ein BASIS-System einer früheren Version als 6.20 verwenden Sie die ANSI-Transportdateien. Alle installierten Transportdateien befinden sich in folgendem Verzeichnis auf dem Produktdistributionsmedium: `\Collaterals\Add-Ons\SAP\Transports\`.

> **Hinweis**
>
> Stellen Sie bei der Überprüfung auf mögliche Installationskonflikte sicher, dass keiner der Objektnamen bereits in Ihrem SAP-System enthalten ist. Objekte verwenden standardmäßig einen **`/crystal/`**-Namespace. Daher ist es nicht erforderlich, diesen Namespace selbst zu erstellen. Wenn Sie den **`/crystal/`**-Namespace manuell erstellen, werden Sie zur Eingabe von Lizenzreparaturschlüssel aufgefordert, auf die Sie nicht zugreifen können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.17.2 Konfigurieren von Transportdateien

Zum Einrichten der Datenzugriffs- oder BW-Publisher-Komponenten der BI-Plattform müssen Sie die entsprechenden Transportdateien in das SAP-System importieren. Diese Komponenten verwenden die Inhalte dieser Transportdateien bei der Kommunikation mit dem SAP-System.

Die für das SAP-System erforderlichen Installations- und Konfigurationsverfahren müssen von einem BASIS-Experten durchgeführt werden, der mit dem Change and Transport System vertraut ist und im SAP-System über Administratorrechte verfügt. Die genaue Vorgehensweise für den Import von Transportdateien ist abhängig von der ausgeführten BASIS-Version. Einzelheiten zu bestimmten Vorgehensweisen finden Sie in Ihrer SAP-Dokumentation.

Beim ersten Einsatz der Datenzugriffskomponente können alle Benutzer standardmäßig auf sämtliche SAP-Tabellen zugreifen. Zum Sichern der SAP-Daten, auf die Benutzer zugreifen können, verwenden Sie den Editor für Sicherheitsdefinitionen.

Nach dem Import der Transportdateien müssen Sie die geeigneten Benutzerzugriffsberechtigungen konfigurieren. Erstellen Sie die erforderlichen Autorisierungen, und übertragen Sie sie mithilfe von Profilen oder Rollen an SAP-Benutzer, die Crystal-Reports-Berichte entwerfen, ausführen oder zeitgesteuert verarbeiten sollen.

Weitere Informationen

Erstellen und Übertragen von Autorisierungen [Seite 831]

24.1.1.17.2.1 Arten von Transportdateien

Es gibt zwei verschiedene Arten von Transportdateien: Unicode-kompatible und ANSI-Transportdateien. Wenn Sie ein BASIS-System der Version 6.20 oder höher einsetzen, verwenden Sie die Unicode-kompatiblen Transportdateien. Für ein BASIS-System einer früheren Version als 6.20 verwenden Sie die ANSI-Transportdateien. Alle installierten Transportdateien befinden sich in folgendem Verzeichnis auf der Produktverteilung: `\Collaterals\Add-Ons\SAP\Transports\`. In der Datei `transports.txt` werden die Unicode-kompatiblen Transportdateien und ANSI-Transportdateien aufgelistet.

Transporttypen sind nachfolgend beschrieben:

- Open SQL Connectivity-Transport

  Der Open SQL Connectivity-Transport ermöglicht den Open SQL-Treibern das Herstellen einer Verbindung mit und die Berichterstellung aus dem SAP-System.
- Transport zur Sicherheitsdefinition auf Zeilenebene

  Diese Transportdatei stellt den Editor für Sicherheitsdefinitionen bereit. Hierbei handelt es sich um ein Tool, das als grafische Oberfläche für die /crystal/auth-Tabellen in der Open SQL Connectivity-Transportdatei dient.
- Transportdatei für die Clusterdefinition

  Dieser Transport stellt das Clusterdefinitions-Tool bereit. Mithilfe dieses Tools können Sie einen Metadaten-Repository für ABAP-Datenclusterdefinitionen aufbauen. Diese Definitionen versorgen den Open SQL-Treiber mit den Informationen, die er zum Erstellen von Berichten aus diesen Datenclustern benötigt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> ABAP-Datencluster sind nicht dasselbe wie Clustertabellen. Clustertabellen sind im DDIC bereits definiert.

- InfoSet Connectivity-Transport

  Die InfoSet Connectivity-Transportdatei ermöglicht dem InfoSet-Treiber den Zugriff auf InfoSets und SAP-Querys.
- Transportdatei für die Workbench zur Content-Verwaltung

  Diese Transportdatei stattet BW-Systeme mit Funktionen für die Inhaltsverwaltung aus. Sie ist ausschließlich als Unicode-kompatible Transportdatei verfügbar.
- Transportdatei für die Personalisierung von BW-Query-Parametern

  Diese Transportdatei bietet Unterstützung für personalisierte und Standardparameterwerte in Berichten, die auf BW-Querys basieren.
- BW MDX Connectivity-Transportdatei

  Diese Transportdatei ermöglicht dem MDX-Query-Treiber den Zugriff auf BW-Cubes und BW-Querys. Die Transportdatei ist mit BW 3.0B Patch 27 oder höher sowie mit BW 3.1C Patch 21 oder höher kompatibel.
- ODS Connectivity-Transportdatei

  Diese Transportdatei ermöglicht dem ODS Query-Treiber den Zugriff auf ODS-Daten. Die Transportdatei ist mit BW 3.0B Patch 27 oder höher sowie mit BW 3.1C Patch 21 oder höher kompatibel.

24.1.1.17.2.2 Prüfen auf Konflikte

Der Inhalt der Transportdateien wird automatisch unter dem SAP-BusinessObjects-Namespace registriert, wenn Sie die Dateien importieren. Der SAP-BusinessObjects-Namespace ist in neuen Versionen von R/3 und MYSAP ERP für diesen Zweck reserviert. Die Objektnamen einiger Objekte, z.B. Berechtigungsobjekte, Berechtigungsklassen und ältere Objekte, enthalten jedoch möglicherweise nicht die erforderlichen Präfixe. Es empfiehlt sich daher, diese Objekttypen vor dem Import der Transportdateien auf Konflikte zu prüfen.

Wenn die Funktionsgruppe, eines der Funktionsmodule oder eines der weiteren Objekte bereits im SAP-System vorliegen, muss der Namespace vor dem Importieren der SAP-BusinessObjects-Transportdateien aufgelöst werden. Die für Ihre SAP-Version geeigneten Verfahren finden Sie in der SAP-NetWeaver-Dokumentation.

24.1.1.17.2.3 Importieren der Transportdateien

Lesen Sie die Datei `transports_German.txt`, die sich im folgenden Verzeichnis Ihrer Produktverteilungsmedien befindet: `\Collaterals\Add-Ons\SAP\Transports\`. In dieser Datei sind die genauen Namen der Dateien aufgelistet, aus denen sich die einzelnen Transporte zusammensetzen. (Die Verzeichnisse `cofiles` und `data` unterhalb des Verzeichnisses `transports` entsprechen den Verzeichnissen .../`trans/cofiles` und .../`trans/data` auf Ihrem SAP-Server.)

Die Open SQL Connectivity-Transportdatei muss vor der Transportdatei zur Sicherheitsdefinition auf Zeilenebene oder Clusterdefinition importiert werden. Die übrigen Transportdateien können in beliebiger Reihenfolge importiert werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Nachdem Sie die Dateien von der CD auf den Server kopiert haben, stellen Sie sicher, dass alle Dateien beschreibbar sind, bevor Sie die Transportdateien importieren. Wenn die Importdateien schreibgeschützt sind, schlägt der Import fehl.

> **Hinweis**
>
> Da es sich bei diesen Transportdateien um binäre Dateien handelt, müssen Sie die Dateien in UNIX-Installationen im binären Modus über FTP hinzufügen (um eine Verfälschung der Daten zu vermeiden). Außerdem müssen Sie über eine Schreibberechtigung für den UNIX-Server verfügen.

24.1.1.17.2.4 Transportdateien

24.1.1.17.2.4.1 Open SQL Connectivity-Transport

Der Open SQL Connectivity-Transport ermöglicht den Treibern das Herstellen einer Verbindung mit und die Berichterstellung aus dem SAP-System.

Objekt	Typ	Beschreibung
/CRYSTAL/BC	Paket	Entwicklungsklasse
/CRYSTAL/OPENSQL	Funktionsgruppe	Open SQL-Funktionen
/CRYSTAL/OSQL_AUTH_FORMS	Programm	Helferprogramm
/CRYSTAL/OSQL_EXECUTE	Programm	Helferprogramm
/CRYSTAL/OSQL_TYPEPOOL-PROG	Programm	Helferprogramm
/CRYSTAL/OSQL_TYPEPOOLS	Programm	Helferprogramm
/CRYSTAL/OSQL_UTILS	Programm	Helferprogramm
ZSSI	Berechtigungsobjektklasse	Berechtigungsobjekte zur Berich-terstellung
ZSEGREPORT	Berechtigungsobjekt	Berechtigungsobjekt zur Berichter-stellung
/CRYSTAL/ OSQL_CLU_ACTKEY_ENTRY	Tabelle	Clustermetadaten
/CRYSTAL/OSQL_FCN_PARAM	Tabelle	Funktionsmetadaten

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Objekt	Typ	Beschreibung
/CRYSTAL/ OSQL_FCN_PARAM_FIELD	Tabelle	Funktionsmetadaten
/CRYSTAL/OSQL_FIELD_ENTRY	Tabelle	Tabellenmetadaten
/CRYSTAL/OSQL_OBJECT_ENTRY	Tabelle	Tabellenmetadaten
/CRYSTAL/ OSQL_RLS_CHK_ENTRY	Tabelle	RLS-Metadaten
/CRYSTAL/ OSQL_RLS_FCN_ENTRY	Tabelle	RLS-Metadaten
/CRYSTAL/ OSQL_RLS_VAL_ENTRY	Tabelle	RLS-Metadaten
ZCLUSTDATA	Tabelle	Clustermetadaten
ZCLUSTID	Tabelle	Clustermetadaten
ZCLUSTKEY	Tabelle	Clustermetadaten
ZCLUSTKEY2	Tabelle	Clustermetadaten
/CRYSTAL/AUTHCHK	Tabelle	RLS-Metadaten
/CRYSTAL/AUTHFCN	Tabelle	RLS-Metadaten
/CRYSTAL/AUTHKEY	Tabelle	RLS-Metadaten
/CRYSTAL/AUTHOBJ	Tabelle	RLS-Metadaten
/CRYSTAL/AUTHREF	Tabelle	RLS-Metadaten
ZSSAUTHCHK	Tabelle	Alte RLS-Metadaten
ZSSAUTHOBJ	Tabelle	Alte RLS-Metadaten
ZSSAUTHKEY	Tabelle	Alte RLS-Metadaten
ZSSAUTHREF	Tabelle	Alte RLS-Metadaten
ZSSAUTH FCN	Tabelle	Alte RLS-Metadaten

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.17.2.4.2 InfoSet Connectivity-Transport

Der InfoSet Connectivity-Transport ermöglicht dem InfoSet-Treiber den Zugriff auf InfoSets. Diese Transportdatei ist mit R/3 4.6c (oder höher) kompatibel. Importieren Sie diesen Transport nicht, wenn Sie SAP R/3 4.6a (oder früher) ausführen.

Objekt	Typ	Beschreibung
/CRYSTAL/BC	Paket	Entwicklungsklasse
/CRYSTAL/FLAT	Funktionsgruppe	InfoSet-Wrapper-Funktionen
/CRYSTAL/QUERY_BATCH	Programm	Ausführung im Batchmodus
/CRYSTAL/ QUERY_BATCH_STREAM	Programm	Ausführung im Streaming-Batch-modus

24.1.1.17.2.4.3 Transport zur Sicherheitsdefinition auf Zeilenebene

Dieser Transport stellt den Editor für Sicherheitsdefinitionen bereit. Hierbei handelt es sich um ein Tool, das als grafische Benutzeroberfläche für die /CRYSTAL/AUTH-Tabellen im Open SQL Connectivity-Transport dient.

Objekt	Typ	Beschreibung
/CRYSTAL/BC	Paket	Entwicklungsklasse
/CRYSTAL/TABMNT	Funktionsgruppe	Funktionsgruppe für Tabellenver-waltungsansicht für Funktionsein-schränkungen
/CRYSTAL/RLSDEF	Programm	Hauptprogramm
/CRYSTAL/RLS_INCLUDE1	Programm	Include-Programm mit den Modul-definitionen
/CRYSTAL/RLS_INCLUDE2	Programm	Include-Programm mit den Unter-routinendefinitionen
TDDAT [/CRYSTAL/AUTHFCN]	Tabelleninhalt	Tabellenverwaltungsdefinition
TVDIR [/CRYSTAL/AUTHFCN]	Tabelleninhalt	Tabellenverwaltungsdefinition
/CRYSTAL/AUTHFCNS	Definition von Transport- und Ver-waltungsobjekt	Tabellenverwaltungsdefinition
/CRYSTAL/RLS	Transaktion	Hauptprogrammtransaktion

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Objekt	Typ	Beschreibung
/CRYSTAL/RLSFCN	Transaktion	Intern vom Hauptprogramm aufgerufene Helfertransaktion

24.1.1.17.2.4.4 Transportdatei für die Clusterdefinition

Dieser Transport stellt das Clusterdefinitions-Tool bereit. Mithilfe dieses Tools können Sie einen Metadaten-Repository für ABAP-Datenclusterdefinitionen aufbauen. Diese Definitionen versorgen den Open SQL-Treiber mit den Informationen, die er zum Erstellen von Berichten aus diesen Datenclustern benötigt.

> **Hinweis**
>
> ABAP-Datencluster sind nicht dasselbe wie Clustertabellen. Clustertabellen sind im DDIC bereits definiert.

Objekt	Typ	Beschreibung
ZCIMPRBG	Programm	Hauptprogramm
ZCRBGTOP	Programm	Include-Programm
ZCDD	Transaktion	Hauptprogrammtransaktion

24.1.1.17.2.4.5 Transportdatei für die Workbench zur Content-Verwaltung

Diese Transportdatei stattet BW-Systeme mit Funktionen für die Inhaltsverwaltung aus. Sie ist nur als Unicode-kompatible Transportdatei verfügbar.

Objekt	Typ	Beschreibung
/CRYSTAL/BC	Paket	Entwicklungsklasse
/CRYSTAL/CL_BW_HTTP_HANDLER	Klasse	HTTP-Anforderungshandler für mehrere CE-Installationen
/CRYSTAL/OBJECT_STATUS_DOM	Domäne	Berichtsaktivität
/CRYSTAL/OBJ_POLICY_DOM	Domäne	CE-Objektsicherheit
/CRYSTAL/OBJECT_STATUS	Datenelement	Berichtsaktivität
/CRYSTAL/OBJ_POLICY	Datenelement	CE-Objektsicherheit

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Objekt	Typ	Beschreibung
/CRYSTAL/CE_SYNCH	Funktionsgruppe	Publisher-Stubs
/CRYSTAL/CA_MSG	Meldungsklasse	Statusmeldungen
/CRYSTAL/CE_SYNCH_FORMS	Programm	Programmkomponente
/CRYSTAL/CONTENT_ADMIN	Programm	Programmkomponente
/CRYSTAL/ CONTENT_ADMIN_CLASS_D	Programm	Programmkomponente
/CRYSTAL/ CONTENT_ADMIN_CLASS_I	Programm	Programmkomponente
/CRYSTAL/ CONTENT_ADMIN_CTREE	Programm	Programmkomponente
/CRYSTAL/ CONTENT_ADMIN_FORMS	Programm	Programmkomponente
/CRYSTAL/ CONTENT_ADMIN_MODULES	Programm	Programmkomponente
/CRYSTAL/ CONTENT_ADMIN_PAIS	Programm	Programmkomponente
/CRYSTAL/ CONTENT_ADMIN_PBOS	Programm	Programmkomponente
/CRYSTAL/ CONTENT_ADMIN_TAB_FRM	Programm	Programmkomponente
/CRYSTAL/ CONTENT_ADMIN_TOP	Programm	Programmkomponente
/CRYSTAL/PUBLISH_WORKER	Programm	Programmkomponente
/CRYSTAL/ PUBLISH_WORKER_DISP	Programm	Programmkomponente
/CRYSTAL/ PUBLISH_WORKER_DISP_I	Programm	Programmkomponente
/CRYSTAL/ PUBLISH_WORKER_FORMS	Programm	Programmkomponente
/CRYSTAL/ PUBLISH_WORKER_PROC	Programm	Programmkomponente

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Objekt	Typ	Beschreibung
/CRYSTAL/ PUBLISH_WORKER_PROC_I	Programm	Programmkomponente
/CRYSTAL/ PUBLISH_WORKER_SCREEN	Programm	Programmkomponente
/CRYSTAL/CA_DEST	Tabelle	Anwendungsstatus
/CRYSTAL/CA_JOB	Tabelle	Anwendungsstatus
/CRYSTAL/CA_JOB2	Tabelle	Anwendungsstatus
/CRYSTAL/CA_LANG	Tabelle	Anwendungsstatus
/CRYSTAL/CA_PARM	Tabelle	Anwendungsstatus
/CRYSTAL/CA_ROLE	Tabelle	Anwendungsstatus
/CRYSTAL/CA_SYST	Tabelle	Anwendungsstatus
/CRYSTAL/MENU_TREE_ITEMS	Struktur	Anwendungsstatus
/CRYSTAL/REPORT_ID	Tabelle	Anwendungsstatus
/CRYSTAL/RPTADMIN	Transaktion	Hauptprogrammtransaktion
/CRYSTAL/EDIT_REPORT	Programm	Wrapper für die Berichtsbearbeitung
/CRYSTAL/EDIT_REPORT	Funktionsgruppe	Funktionen für die Berichtsbearbeitung
ZSSI	Berechtigungsobjektklasse	Crystal-Berechtigungen
ZCNTADMCES	Berechtigungsobjekt	CE-Operationen
ZCNTADMRPT	Berechtigungsobjekt	Berichtsoperationen
ZCNTADMJOB	Berechtigungsobjekt	Hintergrundaufträge

24.1.1.17.2.4.6 ODS Connectivity-Transportdatei

Diese Transportdatei ermöglicht dem ODS Query-Treiber den Zugriff auf ODS-Daten. Die Transportdatei ist mit BW 3.0B Patch 27 oder höher sowie mit BW 3.1C Patch 21 oder höher kompatibel.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Objekt	Typ	Beschreibung
/CRYSTAL/BC	Paket	Entwicklungsklasse
/CRYSTAL/ODS_REPORT	Funktionsgruppe	ODS-Funktionen

24.1.1.17.2.4.7 Transportdatei für die Personalisierung von BW-Query-Parametern

Diese Transportdatei bietet Unterstützung für personalisierte und Standardparameterwerte in Berichten, die auf BW-Querys basieren.

Objekt	Typ	Beschreibung
/CRYSTAL/BC	Paket	Entwicklungsklasse
/CRYSTAL/PERS_VAR	Struktur	Variablendefinition
/CRYSTAL/PERS_VALUE	Struktur	Wertdefinition
/CRYSTAL/PERS	Funktionsgruppe	Personalisierungsfunktionen

24.1.1.17.2.4.8 BW MDX Connectivity-Transportdatei

Diese Transportdatei ermöglicht dem MDX-Query-Treiber den Zugriff auf BW-Cubes und BW-Querys. Die Transportdatei ist mit BW 3.0B Patch 27 oder höher sowie mit BW 3.1C Patch 21 oder höher kompatibel.

Objekt	Typ	Beschreibung
/CRYSTAL/BC	Paket	Entwicklungsklasse
/CRYSTAL/MDX	Funktionsgruppe	MDX-Funktionen
/CRYSTAL/ MDX_STREAM_LAYOUT	Tabellendefinition	Dataset-Struktur
/CRYSTAL/CX_BAPI_ERROR	Klasse	Ausnahme
/CRYSTAL/CX_META-DATA_ERROR	Klasse	Ausnahme
/CRYSTAL/CX_MISSING_STREA-MINFO	Klasse	Ausnahme
/CRYSTAL/CX_NO_MORE_CELLS	Klasse	Ausnahme

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Objekt	Typ	Beschreibung
/CRYSTAL/ CX_NO_MORE_MEMBERS	Klasse	Ausnahme
/CRYSTAL/ CX_NO_MORE_PROPERTIES	Klasse	Ausnahme
/CRYSTAL/ CX_SAVE_SESSION_STATE	Klasse	Ausnahme
/CRYSTAL/MDX_APPEND_DATA	Klasse	Dataset-Prozessor
/CRYSTAL/MDX_READER_BASE	Klasse	Dataset-Prozessor
/CRYSTAL/MDX_READ_DIMENSI-ONS	Klasse	Dataset-Prozessor
/CRYSTAL/MDX_READ_MEASU-RES	Klasse	Dataset-Prozessor
/CRYSTAL/MDX_READ_PROPER-TIES	Klasse	Dataset-Prozessor
/CRYSTAL/MDX_AXIS_LEVELS	Tabellentyp	Metadatenstruktur
/CRYSTAL/MDX_PROPERTY_KEYS	Tabellentyp	Metadatenstruktur
/CRYSTAL/ MDX_PROPERTY_VALUES	Tabellentyp	Metadatenstrukturr
/CRYSTAL/ MDX_STREAM_LAYOUT_TAB	Tabellentyp	Metadatenstruktur

24.1.1.18 Überblick über Berechtigungen

Dieser Bereich enthält eine Liste von SAP-Berechtigungen, die gemäß unserer Erfahrung und Testumgebung für die Durchführung gängiger Aufträge der BI-Plattform in einer integrierten SAP-Umgebung erforderlich sind. Möglicherweise werden in einzelnen Implementierungen zusätzliche Berechtigungsobjekte oder -felder benötigt.

Sie müssen mithilfe jedes Berechtigungsobjekt eine Autorisierung erstellen und die entsprechenden Feldwerte festlegen. Anschließend übertragen Sie die entsprechenden Autorisierungen auf die Profile (oder Rollen) der SAP-Anwender. Die folgenden Abschnitte enthalten eine Beschreibung der erforderlichen Autorisierungen sowie die benötigten Feldwerte. Einzelheiten zur jeweils erforderlichen Vorgehensweise bei den bestimmten SAP-Versionen finden Sie in Ihrer SAP-Dokumentation.

> **Hinweis**
>
> Die in diesem Abschnitt enthaltenen Informationen sind lediglich als empfohlene Richtlinien zu verstehen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Das Berechtigungsobjekt ZSEGREPORT gehört zur Objektklasse ZSSI, die beim Import der SAP-Integration-Transportdateien zur Unterstützung von Open-SQL-Querys installiert wird.

24.1.1.18.1 Erstellen und Übertragen von Autorisierungen

Sie müssen die Autorisierungen erstellen und anwenden, die von den einzelnen Benutzern für den Informationszugriff über die Desktop Intelligence Integration für SAP benötigt werden. Die genaue Vorgehensweise bei der Erstellung, Konfiguration und Übertragung von Autorisierungen hängt von der installierten SAP-Version ab. Dieser Bereich enthält eine Liste von SAP-Autorisierungen, die gemäß unserer Erfahrung und Testumgebung für die Durchführung gängiger Aufgaben erforderlich sind, wenn ein in einer SAP-NetWeaver-ABAP-Umgebung integriertes BI-Plattform-System verwendet wird. Möglicherweise werden in einzelnen Implementierungen zusätzliche Berechtigungsobjekte oder -felder benötigt.

Weitere Informationen

Konfigurieren von Veröffentlichungsfunktionen in der Workbench zur Content-Verwaltung [Seite 809]

24.1.1.19 Aktionen in BW

Dieser Abschnitt beschreibt verschiedene Aktionen in BW.

24.1.1.19.1 Aktionen innerhalb von Crystal Reports

24.1.1.19.1.1 Erstellen eines neuen Berichts aus einer Query in einer BW-Rolle

Berechtigungsobjekt	Feld	Werte
S_USER_AGR	ACT_GROUP	<ANWENDERROLLE>
	ACTVT	01, 02, 06
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	RS_PERS_BOD

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Berechtigungsobjekt	Feld	Werte
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	**<INFOAREA>****
	RSINFOCUBE	**<INFOCUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMPUTER_ID>****
S_RS_COMP1	RSZCOMPID	**<COMPUTER_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERYEIGENTÜMER>***
	ACTVT	16

* **<BENUTZERROLLE>** steht für den Namen der jeweiligen Rolle, die der Benutzer übernimmt. In diesem Feld können mehrere Werte angegeben werden.

* **<QUERYEIGENTÜMER>** steht für den Namen des Eigentümers der Query. Wenn Sie einen Namen angeben, können Sie Berichte nur aus den Querys dieses Eigentümers erstellen. Geben Sie * ein, um Querys beliebiger Eigentümer für die Berichterstellung zu verwenden.

** Bei**< INFOAREA>**, **<INFOCUBE>** oder **<COMPUTER_ID>** geben Sie * ein, um einen beliebigen Wert anzuzeigen. Wenn Sie einen bestimmten Wert angeben, können Berichte nur aus den Querys erstellt werden, in denen diese InfoAreas, Cubes und Computer-IDs enthalten sind.

24.1.1.19.1.2 Öffnen eines vorhandenen Berichts von einer BW-Rolle aus

Berechtigungsobjekt	Feld	Werte
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SUSO, SUNI. RSCR, SH3A, RFC1, RZX0, RZX2, RS_PERS_BOD, /CRYSTAL/PERS, RSOB
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFOAREA>****

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Berechtigungsobjekt	Feld	Werte
	RSINFOCUBE	<INFOCUBE>**
	RSZCOMPTP	REP
	RSZCOMPID	<COMPUTER_ID>**
S_RS_COMP1	RSZCOMPID	<COMPUTER_ID>**
	RSZCOMPTP	REP
	RSZOWNER	<QUERYEIGENTÜMER>*
	ACTVT	16

<QUERYEIGENTÜMER> steht für den Namen des Eigentümers der Query, aus der Sie den Bericht erstellen. Wenn Sie den Namen des Queryeigentümers eingeben, können Sie den Bericht nur aus Querys dieses Eigentümers erstellen. Geben Sie * ein, um Querys beliebiger Eigentümer zu verwenden.

** Bei< INFOAREA>, <INFOCUBE> oder <COMPUTER_ID> geben Sie * ein, um einen beliebigen Wert anzuzeigen. Wenn Sie einen bestimmten Wert angeben, können Berichte nur aus den Querys erstellt werden, in denen diese InfoAreas, Cubes und Computer-IDs enthalten sind.

24.1.1.19.1.3 Anzeigen einer Vorschau oder Aktualisieren eines Berichts

Berechtigungsobjekt	Feld	Werte
S_RS_COMP	RSINFOAREA	<INFOAREA>**
	RSINFOCUBE	<INFOCUBE>**
	RSZCOMPTP	REP
	RSZCOMPID	<COMPUTER_ID>**
S_RS_COMP1	RSZCOMPID	<COMPUTER_ID>**
	RSZCOMPTP	REP
	RSZOWNER	<QUERYEIGENTÜMER>*
	ACTVT	16

<QUERYEIGENTÜMER> steht für den Namen des Eigentümers der Query, aus der Sie den Bericht erstellen. Wenn Sie den Namen des Queryeigentümers eingeben, können Sie den Bericht nur aus Querys dieses Eigentümers erstellen. Geben Sie * ein, um Querys beliebiger Eigentümer zu verwenden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

** Bei< INFOAREA>, <INFOCUBE> oder <COMPUTER_ID> geben Sie * ein, um einen beliebigen Wert anzuzeigen. Wenn Sie einen bestimmten Wert angeben, können Berichte nur aus den Querys erstellt werden, in denen diese InfoAreas, Cubes und Computer-IDs enthalten sind.

24.1.1.19.1.4 Überprüfen der Datenbank (Aktualisieren von Tabellendefinitionen in einem Bericht)

Berechtigungsobjekt	Feld	Werte
S_RS_COMP	RSINFOAREA	<INFOAREA>**
	RSINFOCUBE	<INFOCUBE>**
	RSZCOMPTP	REP
	RSZCOMPID	<COMPUTER_ID>**
S_RS_COMP1	RSZCOMPID	<COMPUTER_ID>**
	RSZCOMPTP	REP
	RSZOWNER	<QUERYEIGENTÜMER>*
	ACTVT	16

<QUERYEIGENTÜMER> steht für den Namen des Eigentümers der Query, aus der Sie den Bericht erstellen. Wenn Sie den Namen des Queryeigentümers eingeben, können Sie den Bericht nur aus Querys dieses Eigentümers erstellen. Geben Sie * ein, um Querys beliebiger Eigentümer zu verwenden.

** Bei< INFOAREA>, <INFOCUBE> oder <COMPUTER_ID> geben Sie * ein, um einen beliebigen Wert anzuzeigen. Wenn Sie einen bestimmten Wert angeben, können Berichte nur aus den Querys erstellt werden, in denen diese InfoAreas, Cubes und Computer-IDs enthalten sind.

24.1.1.19.1.5 Festlegen des Speicherorts der Datenquelle

Berechtigungsobjekt	Feld	Werte
S_RS_COMP	RSINFOAREA	<INFOAREA>**
	RSINFOCUBE	<INFOCUBE>**
	RSZCOMPTP	REP
	RSZCOMPID	<COMPUTER_ID>**

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Berechtigungsobjekt	Feld	Werte
S_RS_COMP1	RSZCOMPID	<COMPUTER_ID>**
	RSZCOMPTP	REP
	RSZOWNER	<QUERYEIGENTÜMER>*
	ACTVT	16

<QUERYEIGENTÜMER> steht für den Namen des Eigentümers der Query, aus der Sie den Bericht erstellen. Wenn Sie den Namen des Queryeigentümers eingeben, können Sie den Bericht nur aus Querys dieses Eigentümers erstellen. Geben Sie * ein, um Querys beliebiger Eigentümer zu verwenden.

** Bei< INFOAREA>, <INFOCUBE> oder <COMPUTER_ID> geben Sie * ein, um einen beliebigen Wert anzuzeigen. Wenn Sie einen bestimmten Wert angeben, können Berichte nur aus den Querys erstellt werden, in denen diese InfoAreas, Cubes und Computer-IDs enthalten sind.

24.1.1.19.1.6 Speichern eines Berichts in einer BW-Rolle

Berechtigungsobjekt	Feld	Werte
S_USER_AGR	ACT_GROUP	<BENUTZERROLLE> *
	ACTVT	01, 02, 06
S_CTS_ADMI	CTS_ADMFCT	TABL

* <BENUTZERROLLE> steht für den Namen der jeweiligen Rolle, die der Benutzer übernimmt. In diesem Feld können mehrere Werte angegeben werden.

24.1.1.19.1.7 Vorbereiten eines Berichts für die Übersetzung bei der Speicherung in BW

Berechtigungsobjekt	Feld	Werte
S_USER_AGR	ACT_GROUP	<ANWENDERROLLE>
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL

<BENUTZERROLLE> steht für den Namen der jeweiligen Rolle, die der Benutzer übernimmt. In diesem Feld können mehrere Werte angegeben werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.19.1.8 Speichern und gleichzeitiges Veröffentlichen eines Berichts auf der BI-Plattform

Berechtigungsobjekt	Feld	Werte
S_USER_AGR	ACT_GROUP	<ANWENDERROLLE>
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	<INFOAREA> ***
	RSINFOCUBE	<INFOCUBE> ***
	RSZCOMPTP	REP
	RSZCOMPID	<COMPUTER_ID> ***
S_RS_COMP1	RSZCOMPID	<COMPUTER_ID> ***
	RSZCOMPTP	REP
	RSZOWNER	<QUERYEIGENTÜMER> **
	ACTVT	16

<BENUTZERROLLE> steht für den Namen der jeweiligen Rolle, die der Benutzer übernimmt. In diesem Feld können mehrere Werte angegeben werden.

** <QUERYEIGENTÜMER> steht für den Namen des Eigentümers der Query, aus der Sie den Bericht erstellen. Wenn Sie den Namen des Queryeigentümers eingeben, können Sie den Bericht nur aus Querys dieses Eigentümers erstellen. Geben Sie * ein, um Querys beliebiger Eigentümer zu verwenden.

*** Bei < INFOAREA> , <INFOCUBE> oder <COMPUTER_ID> geben Sie * ein, um einen beliebigen Wert anzuzeigen. Wenn Sie einen bestimmten Wert angeben, können Berichte nur aus den Querys erstellt werden, in denen diese InfoAreas, Cubes und Computer-IDs enthalten sind.

24.1.1.19.1.9 Starten des BEx Query Designer™

Berechtigungsobjekt	Feld	Werte
S_RS_COMP	RSINFOAREA	<INFOAREA>**
	RSINFOCUBE	<INFOCUBE>**
	RSZCOMPTP	REP

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Berechtigungsobjekt	Feld	Werte
	RSZCOMPID	**<COMPUTER_ID>****
S_RS_COMP1	RSZCOMPID	**<COMPUTER_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERYEIGENTÜMER>***
	ACTVT	16
S_CTS_ADMI	CST_ADMFCT	TABL

* **<QUERYEIGENTÜMER>** steht für den Namen des Eigentümers der Query, aus der Sie den Bericht erstellen. Wenn Sie den Namen des Queryeigentümers eingeben, können Sie den Bericht nur aus Querys dieses Eigentümers erstellen. Geben Sie * ein, um Querys beliebiger Eigentümer zu verwenden.

** Bei **<INFOAREA>**, **<INFOCUBE>** oder **<COMPUTER_ID>** geben Sie * ein, um einen beliebigen Wert anzuzeigen. Wenn Sie einen bestimmten Wert angeben, können Berichte nur aus den Querys erstellt werden, in denen diese InfoAreas, Cubes und Computer-IDs enthalten sind.

24.1.1.19.2 Aktionen innerhalb von BI-Launchpad

24.1.1.19.2.1 Anmelden an der BI-Plattform mit SAP-Anmeldedaten

Berechtigungsobjekt	Feld	Werte
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

24.1.1.19.2.2 Anzeigen eines SAP BW-Berichts auf Abruf

Berechtigungsobjekt	Feld	Werte
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFOAREA>****

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Berechtigungsobjekt	Feld	Werte
	RSINFOCUBE	<INFOCUBE>**
	RSZCOMPTP	REP
	RSZCOMPID	<COMPUTER_ID>**
S_RS_COMP1	RSZCOMPID	<COMPUTER_ID>**
	RSZCOMPTP	REP
	RSZOWNER	<QUERYEIGENTÜMER>*
	ACTVT	16
S_RS_ODSO	RSINFOAREA	<INFOAREA>**
	RSODSOBJ	0CRM_OLVM
	RSODSPART	Daten
	ACTVT	03

<QUERYEIGENTÜMER> steht für den Namen des Eigentümers der Query, aus der Sie den Bericht erstellen. Wenn Sie den Namen des Queryeigentümers eingeben, können Sie den Bericht nur aus Querys dieses Eigentümers erstellen. Geben Sie * ein, um Querys beliebiger Eigentümer zu verwenden.

** Bei< INFOAREA>, <INFOCUBE> oder <COMPUTER_ID> geben Sie * ein, um einen beliebigen Wert anzuzeigen. Wenn Sie einen bestimmten Wert angeben, können Berichte nur aus den Querys erstellt werden, in denen diese InfoAreas, Cubes und Computer-IDs enthalten sind.

24.1.1.19.2.3 Aktualisieren eines Berichts vom Viewer aus

Berechtigungsobjekt	Feld	Werte
S_RS_COMP	RSINFOAREA	<INFOAREA>**
	RSINFOCUBE	<INFOCUBE>**
	RSZCOMPTP	REP
	RSZCOMPID	<COMPUTER_ID>**
S_RS_COMP1	RSZCOMPID	<COMPUTER_ID>**
	RSZCOMPTP	REP

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Berechtigungsobjekt	Feld	Werte
	RSZOWNER	**<QUERYEIGENTÜMER>***
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFOAREA>****
	RSODSOBJ	0CRM_OLVM
	RSODSPART	Daten
	ACTVT	03

* **<QUERYEIGENTÜMER>** steht für den Namen des Eigentümers der Query, aus der Sie den Bericht erstellen. Wenn Sie den Namen des Queryeigentümers eingeben, können Sie den Bericht nur aus Querys dieses Eigentümers erstellen. Geben Sie * ein, um Querys beliebiger Eigentümer zu verwenden.

** Bei **<INFOAREA>**, **<INFOCUBE>** oder **<COMPUTER_ID>** geben Sie * ein, um einen beliebigen Wert anzuzeigen. Wenn Sie einen bestimmten Wert angeben, können Berichte nur aus den Querys erstellt werden, in denen diese InfoAreas, Cubes und Computer-IDs enthalten sind.

24.1.1.19.2.4 Zeitgesteuertes Verarbeiten eines Berichts

Berechtigungsobjekt	Feld	Werte
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFOAREA>****
	RSINFOCUBE	**<INFOCUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMPUTER_ID>****
S_RS_COMP1	RSZCOMPID	**<COMPUTER_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERYEIGENTÜMER>***
	ACTVT	16

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Berechtigungsobjekt	Feld	Werte
S_RS_ODSO	RSINFOAREA	<INFOAREA>**
	RSODSOBJ	0CRM_OLVM
	RSODSPART	Daten
	ACTVT	03

<QUERYEIGENTÜMER> steht für den Namen des Eigentümers der Query, aus der Sie den Bericht erstellen. Wenn Sie den Namen des Queryeigentümers eingeben, können Sie den Bericht nur aus Querys dieses Eigentümers erstellen. Geben Sie * ein, um Querys beliebiger Eigentümer zu verwenden.

** Bei< INFOAREA>, <INFOCUBE> oder <COMPUTER_ID> geben Sie * ein, um einen beliebigen Wert anzuzeigen. Wenn Sie einen bestimmten Wert angeben, können Berichte nur aus den Querys erstellt werden, in denen diese InfoAreas, Cubes und Computer-IDs enthalten sind.

24.1.1.19.2.5 Lesen dynamischer Auswahllisten in Berichtsparametern

Berechtigungsobjekt	Feld	Werte
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB
	ACTVT	16

24.1.1.19.3 Aktionen innerhalb von SAP NetWeaver (ABAP)

24.1.1.19.3.1 Innerhalb von Crystal Reports unter Verwendung des Open SQL-Treibers

Dieser Abschnitt beschreibt verschiedene Aktionen in SAP NetWeaver (ABAP) innerhalb von Crystal Reports unter Verwendung des Open-SQL-Treibers.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.19.3.2 Anmelden bei SAP-Servern

Berechtigungsobjekt	Feld	Werte
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16

24.1.1.19.3.3 Einfügen von neuen Berichten

Berechtigungsobjekt	Feld	Werte
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	01

24.1.1.19.3.4 Öffnen oder Anzeigen der Vorschau eines vorhandenen Berichts

Berechtigungsobjekt	Feld	Werte
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.19.3.5 Überprüfen der Datenbank (Aktualisieren von Tabellendefinitionen in einem Bericht)

Berechtigungsobjekt	Feld	Werte
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

24.1.1.19.3.6 Festlegen des Speicherorts der Datenquelle

Berechtigungsobjekt	Feld	Werte
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

24.1.1.19.4 Aktionen innerhalb von Crystal Reports unter Verwendung des InfoSet-Treibers bei Berichterstellung auf der Basis von InfoSet

24.1.1.19.4.1 Anmelden bei SAP-Servern

Berechtigungsobjekt	Feld	Werte
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.19.4.2 Erstellen neuer Berichte aus einem InfoSet in SAP NetWeaver (ABAP)

Berechtigungsobjekt	Feld	Werte
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/FLAT, SKBW, AQRC
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL

> **Hinweis**
>
> Fügen Sie außerdem ausreichende Berechtigungen zum Anzeigen von Datenzeilen hinzu. Beispiel: P_ORIG oder P_APAP.

Weitere Informationen

Festlegen des Speicherorts der Datenquelle [Seite 843]

24.1.1.19.4.3 Überprüfen der Datenbank (Aktualisieren von Tabellendefinitionen in einem Bericht)

Berechtigungsobjekt	Feld	Werte
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

24.1.1.19.4.4 Festlegen des Speicherorts der Datenquelle

Berechtigungsobjekt	Feld	Werte	
P_ABAP	REPID	AQTGSYSTGENERATESY, SAPDBPNP	
		COARS	2

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.19.5 Aktionen innerhalb von Crystal Reports unter Verwendung des InfoSet-Treibers bei der Berichterstellung aus einer ABAP-Query

24.1.1.19.5.1 Anmelden bei SAP-Servern

Berechtigungsobjekt	Feld	Werte
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

24.1.1.19.5.2 Erstellen neuer Berichte aus einer ABAP-Query in SAP NetWeaver

Berechtigungsobjekt	Feld	Werte
P_ABAP	REPID	AQTG02==========P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
S_TABU_DIS	ACTVT	03
	GROUP	Name der Tabellengruppe

24.1.1.19.5.3 Überprüfen der Datenbank

Berechtigungsobjekt	Feld	Werte
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.19.5.4 Festlegen des Speicherorts der Datenquelle

Berechtigungsobjekt	Feld	Werte
P_ABAP	REPID	AQTG02==========P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16
S_TABU_DIS	ACTVT	03
	GROUP	Name der Tabellengruppe

24.1.1.19.6 Aktionen innerhalb der BI-Plattform

24.1.1.19.6.1 Zeitgesteuertes Verarbeiten eines Berichts im Dialogmodus (mit einer Open SQL-Query)

Berechtigungsobjekt	Feld	Werte
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

Hinweis

Der Wert für CLASS lautet BLANK.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.1.1.19.6.2 Zeitgesteuertes Verarbeiten eines Berichts im Batchmodus anhand einer Open SQL-Query

Berechtigungsobjekt	Feld	Werte
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL, SH3A
	ACTVT	16
S_BTCH_JOB	JOBGROUP	' '
	JOBACTION	RELE
ZSEGREPORT	ACTVT	02
S_BTCH_ADM	BTCADMIN	Y

Hinweis

Der Wert für CLASS lautet BLANK.

24.1.1.19.6.3 Crystal-Berechtigungssystem

Berechtigungsobjekt	Feld	Wert
Berechtigung für den Datenzugriff (S_DATASET)	Aktivität (ACTVT)	Lese-, Schreibzugriff (33, 34)
	Physischer Dateiname (FILENAME)	* (steht für Alle)
	Name des ABAP-Programms (PROGRAM)	*
Berechtigungsprüfung für RFC-Zugriff (S_RFC)	Aktivität (ACTVT)	16
	Name des zu schützenden RFC (RFC_NAME)	BDCH, STPA, SUSO, SUUS, SU_USER, SYST, SUNI, PRGN_J2EE, /CRYSTAL/SECURITY

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Berechtigungsobjekt	Feld	Wert
	Typ des zu schützenden RFC-Objektes (RFC_TYPE)	Funktionsgruppe (FUGR)
Anwenderstammpflege: Anwendergruppen (S_USER_GRP)	Aktivität (ACTVT)	Erstellen/Generieren und Anzeigen (03)
	Anwendergruppe in Anwenderstammpflege (CLASS)	* **Hinweis** Um mehr Sicherheit zu gewährleisten, können Sie die Benutzergruppen, deren Mitglieder Zugriff auf die BI-Plattform benötigen, auch ausdrücklich aufführen.

24.1.1.19.6.4 Ausführen und Erstellen von BW BEx Querys

Wenn beim Erstellen eines Berichts aus einem Universum basierend auf einer BW BEx Query eine Datumsdimension einbezogen wird, muss der Systemadministrator sowohl dem Benutzer, der das Universum erstellt, als auch dem Benutzer, der den Bericht ausführt, eine `S_RS_IOBJ`-Berechtigung erteilen.

Berechtigungsobjekt	Feld	Werte
S_RS_IOBJ	ACTVT	03
	RSIOBJ	
	RSIOBJ_CAT	
	RSIOBJ_PART	

24.2 Konfigurieren für die JD Edwards-Integration

24.2.1 Konfigurieren der Einzelanmeldung für SAP Crystal Reports

Die BI-Plattform ist standardmäßig so konfiguriert, dass Benutzer von SAP Crystal Reports mit der Einzelanmeldung auf JD Edwards EnterpriseOne-Daten zugreifen können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.2.1.1 Deaktivieren der Einzelanmeldung für JD Edwards und SAP Crystal Reports

1. Klicken Sie in der Central Management Console (CMC) auf **Anwendungen**.
2. Doppelklicken Sie auf **Crystal-Reports-Konfiguration**.
3. Klicken Sie auf **Einzelanmeldungsoptionen**.
4. Wählen Sie **crdb_pseone** aus.
5. Klicken Sie auf **Entfernen**.
6. Klicken Sie auf **Speichern und schließen**.
7. Wählen Sie auf der Seite **Server** in der CMC **Crystal-Reports-Dienste**, und klicken Sie auf **Server neu starten**.

24.2.1.2 Aktivieren der Einzelanmeldung für JD Edwards und SAP Crystal Reports

Gehen Sie wie folgt vor, falls Sie die Einzelanmeldung für JD Edwards und SAP Crystal Reports deaktiviert haben und diese erneut aktivieren möchten.

1. Klicken Sie in der Central Management Console (CMC) auf **Anwendungen**.
2. Doppelklicken Sie auf **Crystal-Reports-Konfiguration**.
3. Klicken Sie auf **Einzelanmeldungsoptionen**.
4. Geben Sie unter *SSO-Kontext für Datenbankanmeldung mit folgenden Treibern verwenden* den Eintrag **crdb_pseone** ein.
5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Speichern und schließen**.
7. Wählen Sie auf der Seite **Server** in der CMC **Crystal-Reports-Dienste**, und klicken Sie auf **Server neu starten**.

24.2.2 Konfigurieren der SSL (Secure Sockets Layer) für JD-Edwards-Integrationen

Sie können das SSL-Protokoll (Secure Sockets Layer) für die gesamte Netzwerkkommunikation zwischen Clients und Servern in der BI-Plattform- und JD-Edwards-EnterpriseOne-Implementierung verwenden.

Für die Verwendung von JD-Edwards-EnterpriseOne-Daten mit der BI-Plattform sind einige Änderungen an der SSL-Konfiguration erforderlich. Speichern Sie wie bei der SSL-Konfiguration für andere BI-Plattform-Server und -Clients folgende KEY- und Zertifikatdateien an einem geschützten Ort (im gleichen Verzeichnis), auf das die Computer Ihrer BI-Plattform-Implementierung Zugriff haben.

- Die vertrauenswürdige Zertifikatdatei (cacert.der).
- Die generierte Serverzertifikatdatei (servercert.der).
- Die Serverschlüsseldatei (server.key).
- Die Kennsatzdatei (passphrase.txt).

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.2.2.1 So aktivieren Sie die JD Edwards EnterpriseOne-Datenkonnektivität mit SSL

> **Hinweis**
>
> Bei allen im nachfolgenden Verfahren beschriebenen Werten wird zwischen Groß- und Kleinschreibung unterschieden.

1. Kopieren Sie Ihre SSL-Zertifikate nach `C:\SSLCert`.
2. Starten Sie den Central Configuration Manager (CCM).
3. Halten Sie den Server Intelligence Agent (SIA) an.
4. Doppelklicken Sie auf den SIA, um das Dialogfeld *Eigenschaften* zu öffnen.
5. Klicken Sie auf die Registerkarte **Protokoll**.
6. Wählen Sie **SSL aktivieren**.
7. Wählen Sie für den *SSL-Zertifikatordner* das Verzeichnis aus, das die SSL-Zertifikate enthält: `C:\SSLCert`.
8. Wählen Sie unter *Server-SSL-Zertifikatdatei* die Datei `servercert.der`.
9. Wählen Sie unter *Dateien für vertrauenswürdige SSL-Zertifikate* die Datei `cacert.der`.
10. Wählen Sie unter *Datei für den privaten SSL-Schlüssel* die Datei `server.key`.
11. Wählen Sie unter *Kennphrasendatei für den privaten SSL-Schlüssel* die Datei `passphrase.key`.
12. Klicken Sie auf **Anwenden**.
13. Starten Sie den Server Intelligence Agent.

Der BI-Plattform-Reporting-Server (z.B. Adaptive Job Server) muss neu gestartet werden, damit die Änderungen übernommen werden.

24.2.2.2 Datei mit der SSL-Konfigurationseigenschaft

Die Eigenschaftendatei `sslconf.properties` enthält alle Informationen für die von der BI-Plattform verwendeten erforderlichen Zertifikate und Schlüssel. Beispiel:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Die Datei `sslconf.properties` sollte in dem Ordner abgelegt werden, in dem die `BI-Plattform` installiert ist. Dies ist standardmäßig C:\Programme\Business Objects\BusinessObjects 13.0.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.3 Konfigurieren für die PeopleSoft Enterprise-Integration

24.3.1 Konfigurieren der Einzelanmeldung (SSO) für SAP Crystal Reports und PeopleSoft Enterprise

Die BI-Plattform ist standardmäßig so konfiguriert, dass Benutzer von SAP Crystal Reports mit der Einzelanmeldung auf PeopleSoft Enterprise-Daten zugreifen können.

24.3.1.1 Deaktivieren der Einzelanmeldung für PeopleSoft Enterprise und SAP Crystal Reports

1. Klicken Sie in der Central Management Console (CMC) auf **Anwendungen**.
2. Doppelklicken Sie auf **Crystal-Reports-Konfiguration**.
3. Klicken Sie auf **Einzelanmeldungsoptionen**.
4. Wählen Sie **crdb_psenterprise**.
5. Klicken Sie auf **Entfernen**.
6. Klicken Sie auf **Speichern und schließen**.
7. Wählen Sie auf der Seite **Server** in der CMC **Crystal-Reports-Dienste**, und klicken Sie auf **Server neu starten**.

24.3.1.2 Aktivieren der Einzelanmeldung für PeopleSoft Enterprise und SAP Crystal Reports

Wenn Sie die Einzelanmeldung für PeopleSoft Enterprise und SAP Crystal Reports deaktiviert haben und wieder aktivieren möchten.

1. Klicken Sie in der Central Management Console (CMC) auf **Anwendungen**.
2. Doppelklicken Sie auf **Crystal-Reports-Konfiguration**.
3. Klicken Sie auf **Einzelanmeldungsoptionen**.
4. Geben Sie unter *SSO-Kontext für Datenbankanmeldung mit folgenden Treibern verwenden* den Eintrag **crdb_psenterprise** ein.
5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Speichern und schließen**.
7. Wählen Sie auf der Seite **Server** in der CMC **Crystal-Reports-Dienste**, und klicken Sie auf **Server neu starten**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.3.2 Konfigurieren der SSL-Kommunikation

Sie können das SSL-Protokoll (Secure Sockets Layer) für die gesamte Netzwerkkommunikation zwischen Clients und Servern in der BI-Plattform-Implementierung verwenden.

Speichern Sie wie bei der SSL-Konfiguration für andere BI-Plattform-Server und -Clients folgende KEY- und Zertifikatdateien an einem geschützten Ort (im gleichen Verzeichnis), auf das die Rechner Ihrer BI-Plattform-Implementierung Zugriff haben.

- Die vertrauenswürdige Zertifikatdatei (cacert.der).
- Die generierte Serverzertifikatdatei (servercert.der).
- Die Serverschlüsseldatei (server.key).
- Die Kennsatzdatei (passphrase.txt).

24.3.2.1 Datei mit der SSL-Konfigurationseigenschaft

Die Eigenschaftendatei `sslconf.properties` enthält alle Informationen für die von BI-Plattform-Komponenten verwendeten erforderlichen Zertifikate und Schlüssel. Beispiel:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Die Datei `sslconf.properties` sollte im Installationsordner der BI-Plattform abgelegt werden. Standardmäßig ist dies `C:\Programme\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\`.

24.3.2.2 Aktivieren von SSL für den PeopleSoft-Abfrageserver

> **Hinweis**
>
> Bei allen im nachfolgenden Verfahren beschriebenen Werten wird zwischen Groß- und Kleinschreibung unterschieden.

1. Kopieren Sie Ihre SSL-Zertifikate nach `C:\SSLCert`.
2. Starten Sie den Central Configuration Manager (CCM).
3. Halten Sie den Server Intelligence Agent (SIA) an.
4. Doppelklicken Sie auf den SIA, um das Dialogfeld *Eigenschaften* zu öffnen.
5. Klicken Sie auf die Registerkarte **Protokoll**.
6. Wählen Sie **SSL aktivieren**.
7. Wählen Sie für den *SSL-Zertifikatordner* das Verzeichnis aus, das die SSL-Zertifikate enthält: `C:\SSLCert`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

8. Wählen Sie unter *Server-SSL-Zertifikatdatei* die Datei `servercert.der`.
9. Wählen Sie unter *Dateien für vertrauenswürdige SSL-Zertifikate* die Datei `cacert.der`.
10. Wählen Sie unter *Datei für den privaten SSL-Schlüssel* die Datei `server.key`.
11. Wählen Sie unter *Kennphrasendatei für den privaten SSL-Schlüssel* die Datei `passphrase.key`.
12. Klicken Sie auf **Anwenden**.
13. Starten Sie den Server Intelligence Agent.

Der BI-Plattform-Reporting-Server (z.B. Adaptive Job Server) muss neu gestartet werden, damit die Änderungen übernommen werden.

24.3.2.3 So aktivieren Sie die Sicherheitsbrücke mit SSL

> **Hinweis**
>
> Bei allen im nachfolgenden Verfahren beschriebenen Werten wird zwischen Groß- und Kleinschreibung unterschieden.

1. Kopieren Sie Ihre SSL-Zertifikate nach `C:\SSLCert`.
2. Starten Sie den Central Configuration Manager (CCM).
3. Halten Sie den Server Intelligence Agent (SIA) an.
4. Doppelklicken Sie auf den SIA, um das Dialogfeld *Eigenschaften* zu öffnen.
5. Klicken Sie auf die Registerkarte **Protokoll**.
6. Wählen Sie **SSL aktivieren**.
7. Wählen Sie für den *SSL-Zertifikatordner* das Verzeichnis aus, das die SSL-Zertifikate enthält: `C:\SSLCert`.
8. Wählen Sie unter *Server-SSL-Zertifikatdatei* die Datei `servercert.der`.
9. Wählen Sie unter *Dateien für vertrauenswürdige SSL-Zertifikate* die Datei `cacert.der`.
10. Wählen Sie unter *Datei für den privaten SSL-Schlüssel* die Datei `server.key`.
11. Wählen Sie unter *Kennphrasendatei für den privaten SSL-Schlüssel* die Datei `passphrase.key`.
12. Klicken Sie auf **Anwenden**.
13. Starten Sie den Server Intelligence Agent.

24.3.3 Leistungsoptimierung für PeopleSoft-Systeme

Um eine optimale Leistung bei der Berichterstellung auf der Grundlage von PeopleSoft-Abfragen zu gewährleisten, sind Kenntnisse darüber erforderlich, wie Abfragen von Crystal Reports und der BI-Plattform ausgeführt werden.

Bei jeder Aktualisierung oder Ausführung eines Berichts, der auf einer PeopleSoft-Abfrage basiert, wird eine Verbindung mit einem PeopleSoft-Server hergestellt:

- In Umgebungen von PeopleSoft Enterprise (PeopleTools 8.46 oder höher) wird eine Verbindung mit dem *PeopleSoft Analytic Server* hergestellt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- In Umgebungen von PeopleSoft Enterprise (PeopleTools 8.21-8.45) wird eine Verbindung mit dem *PeopleSoft-Anwendungsserver* hergestellt.

24.3.3.1 Empfehlungen

In einer optimalen Implementierung erfolgt die Einrichtung von einem oder mehreren PeopleSoft Analytic Server(n) bzw. PeopleSoft-Anwendungsserver(n) zur alleinigen Bearbeitung von Berichtsanfragen. In jedem dieser Server steuern die Einstellungen von "Min Instances" und "Max Instances" die Anzahl der Berichtsanfragen, die jederzeit bearbeitet werden können. Diese Einstellung bietet folgende Vorteile:

- Es gibt keine Konflikte zwischen Berichtsanfragen und anderen Transaktionsanfragen im PeopleSoft-Server.
- Es ist möglich, Wartungsarbeiten am Server durchzuführen, der Berichtsanfragen behandelt, ohne dafür den Server zu deaktivieren, der Transaktionsanfragen behandelt.

In einer Umgebung, in der sowohl Berichts- als auch Transaktionsanfragen vom selben PeopleSoft Analytic Server bzw. PeopleSoft-Anwendungsserver bearbeitet werden, ist die BI-Plattform so zu konfigurieren, dass nur ein Bericht auf einmal ausgeführt werden kann. Andernfalls sind Benutzer nicht in der Lage, Transaktionsanfragen zu stellen, wenn sämtliche PSANALYTICSRV- bzw. PSAPPSRV-Prozesse zum Ausführen von Berichten verwendet werden.

> **Hinweis**
>
> Informationen zur Beschränkung der Anzahl geplanter Berichtsaufträge und/oder Aufträge zur Ansicht von Berichten nach Anfrage finden Sie unter "Verwalten und Konfigurieren von Servern" im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.

> **Hinweis**
>
> Es ist nicht möglich, das System auf eine bestimmte Anzahl von Crystal-Reports-Benutzern einzuschränken, die gleichzeitig auf den Server zugreifen können.

Sollte es zu Leistungsminderungen kommen, können Sie mit dem Psadmin-Konfigurationstool herausfinden, ob sich Anfragen zu einer Warteschlange aufgestaut haben. Überwachen Sie auch die Systemressourcen auf dem PeopleSoft Analytic Server bzw. PeopleSoft-Anwendungsserver. Wenn mangels physischer Speicher virtuelle Speicher verwendet werden, kann sich auf die Verarbeitungszeit erhöhen.

24.3.3.2 PeopleSoft-Server

Bei einem PeopleSoft Analytic Server werden die Berichte durch den PSANALYTICSRV-Prozess regeneriert oder ausgeführt. Bei einem PeopleSoft-Anwendungsserver werden die Berichte durch den PSAPPSRV-Prozess regeneriert oder ausgeführt. Die Anzahl der verfügbaren PSANALYTICSRV- bzw. PSAPPSRV-Prozesse bestimmt die Anzahl der Berichte, die Sie gleichzeitig ausführen können.

Eine Konfigurationsdatei für den PeopleSoft Analytic Server oder PeopleSoft-Anwendungsserver enthält normalerweise folgende Informationen:

```
Min Instances=3
Max Instances=5
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

In diesem Beispiel sind mindestens drei PSANALYTICSRV- bzw. PSAPPSRV-Prozesse jederzeit verfügbar, und es besteht die Möglichkeit, diese bis auf fünf Prozesse zu erhöhen. Die Einstellungen bedeuten nicht unbedingt, dass fünf Berichte immer gleichzeitig ausgeführt werden können. Die Prozesse können auch zum Abarbeiten anderer Aufgaben im System verwendet werden. Wenn keine PSANALYTICSRV- bzw. PSAPPSRV-Prozesse für die Bearbeitung einer Anfrage verfügbar sind, wird die Anfrage in eine Warteschlange gestellt, bis ein Prozess verfügbar wird.

> **Hinweis**
>
> Die Konfigurationsdatei für den PeopleSoft *Anwendungsserver* enthält normalerweise auch den Parameter `Service-Zeitüberschreitung`, der angibt, wie lange Anfragen in Warteschlangen auf einen verfügbaren Prozess warten. Wenn innerhalb der für den Parameter angegebenen Zeit kein Prozess verfügbar wird, kommt es zu einer Zeitüberschreitung für die Anfrage.

24.4 Konfiguration für Siebel-Integration

24.4.1 Konfigurieren von Siebel für die Integration in die SAP-BI-Plattform

Die BI-Plattform-Integration enthält eine Verknüpfung zu Crystal Reports, über die Sie Inhalt aus der SAP-BusinessObjects-Business-Intelligence-Suite in eine Siebel-Anwendung einbetten können. Nach der Installation und Konfiguration können die Benutzer BI-Launchpad über das neue Menüelement aus der Siebel-Anwendung heraus starten.

Die erforderlichen Dateien sind standardmäßig im folgenden Ordner installiert: `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\`.

24.4.1.1 Importieren des Siebel-Integrationsprojekts der BI-Plattform

1. Starten Sie Siebel Tools
2. Klicken Sie auf **Tools** > **Import from Archive** (Aus Archiv importieren).
3. Wenn eine Eingabeaufforderung für eine Archivdatei angezeigt wird, suchen Sie den Ordner "Siebel Files" Ihrer Integration-Produktinstallation.

   Dies ist standardmäßig: `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\`.
4. Wechseln Sie zum entsprechenden Unterordner (entweder Siebel 7.7 oder Siebel 8.0), und wählen Sie die Datei `BusinessObjectsEnterprise.sif` aus.
   Der Import-Assistent wird angezeigt.
5. Klicken Sie auf **Objektdefinition der Archivdatei mit der Definition im Repository zusammenführen**.
6. Befolgen Sie die Anweisungen am Bildschirm des Assistenten, um den Import des Integration-Projekts abzuschließen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Das Integration-Projekt wird zum Repository hinzugefügt.

7. Sperren Sie das **BusinessObjects Integration**-Projekt.

24.4.2 Erstellen des Crystal-Reports-Menüelements

1. Sperren Sie das Projekt **Menu** (Menü) in Siebel Tools.
2. Wählen Sie im Object Explorer das Objekt **Menu Item** (Menüelement).

   > **Hinweis**
   >
   > Wenn das Objekt "Menu" (Menü) nicht im Object Explorer angezeigt wird, klicken Sie auf **View (Ansicht)** > **Options (Optionen)** in Siebel Tools, klicken Sie auf die Registerkarte **Object Explorer** (Objekt-Explorer), und wählen Sie das Objekt **Menu** (Menü).

3. Wählen Sie in der Liste **Menus** (Menüs) das Menü **Generic Web** (Generisches Web).
4. Klicken Sie auf die Überschrift der Liste **Menu Items** (Menüelemente).
5. Klicken Sie auf **Edit (Bearbeiten)** > **New Record (Neuer Datensatz)**.
6. Definieren Sie das neue Menüelement entsprechend. Dies sind die empfohlenen Werte:
   - Name: Ansicht – Crystal Reports
   - Command (Befehl): Crystal Reports
   - Comments (Kommentare): SAP BusinessObjects-Menü "Integrierter Bericht"
   - Inaktive (Inaktiv): False
7. Verwenden Sie eine Postionsnummer, um eine Position für das Menüelement in Ihrem Ansichtsmenü auszuwählen.

   Um eine Positionsnummer auszuwählen, ist es hilfreich, die Menüelemente nach Position zu sortieren.
8. Sie können nun Gebietsschemaeinträge hinzufügen, um die Beschriftung entsprechend zu lokalisieren.

Rekompilieren Sie nun Ihre Siebel-Anwendung. Siehe *Rekompilieren der Siebel-Anwendung* [Seite 855].

24.4.2.1 Rekompilieren der Siebel-Anwendung

Nachdem Sie die BI-Plattform installiert und den Benutzern den zugehörigen Befehl über ein Siebel-Menüelement verfügbar gemacht haben, müssen Sie die Siebel-Anwendung gemäß Ihrer üblichen Vorgehensweise rekompilieren. Einzelheiten hierzu finden Sie im Siebel Bookshelf.

Erstellen Sie nach dem Rekompilieren Ihrer Siebel-Anwendung die JavaScript-Dateien neu. In Siebel 7.7 und höher können die JavaScript-Dateien im Rahmen des Rekompilierungsprozesses automatisch neu erstellt werden.

Da die zum Kompilieren des Siebel-Repositorys erforderlichen Schritte auf Ihrem Siebel Tools-Rechner durchgeführt werden, müssen Sie die resultierenden JavaScript-Dateien vom Siebel Tools-Rechner auf Ihren Siebel-Server implementieren. Normalerweise und abhängig vom Installationsort von Siebel finden Sie die generierten JavaScript-Dateien im folgenden Verzeichnis:

```
C:\sea77\tools\PUBLIC\ENU\<srf1096416329_444>
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Der Name des Beispielordners **<srf1096416329_444>** wird von Siebel Tools generiert und entspricht eindeutig der resultierenden Repository-Datei.

Die JavaScript-Dateien werden auf dem Siebel Server in der Regel im folgenden Verzeichnis implementiert, abhängig vom Installationsort von Siebel:

```
C:\sea77\SWEApp\PUBLIC\ENU\<srf1096416329_444>
```

Der von Siebel Tools generierte Ordnername muss unbedingt beibehalten werden.

Außerdem müssen Sie Ihre Siebel-Konfigurationsdatei auf dem Siebel Server-Rechner aktualisieren, um den Dienst zu ermöglichen. Suchen Sie die entsprechende Konfigurationsdatei auf Ihrem Siebel Server-Rechner. Wenn Sie beispielsweise eine englische Version des Siebel Call Centers ausführen, verwenden Sie `uagent.cfg`. Standardmäßig befindet sich diese Datei unter `C:\sea77\siebsrvr\bin\ENU\uagent.cfg` für Siebel 7.7.

Fügen Sie anschließend folgende Zeile am Ende des SWE-Abschnitts der Konfigurationsdatei ein:

```
ClientBusinessService<NUMBER> = BusinessObjects Integration Service
```

Die `ClientBusinessService`-Nummern sind sequenziell. Wenn keine anderen ClientBusinessServices im SWE-Abschnitt vorhanden sind, setzen Sie **<NUMBER>** auf 0. Andernfalls setzen Sie **<NUMBER>** auf den nächsthöheren Wert.

Für Siebel 8 oder höher:

1. Melden Sie sich bei Siebel Tools an, und suchen Sie das Anwendungsobjekt **Siebel Universal Agent** im Object Explorer.
2. Erweitern Sie die Anwendungsobjekte, um das Objekt **Application User Prop** anzuzeigen.
3. Erstellen Sie einen neuen Eintrag für jeden zu deklarierenden Business Service und legen Sie dabei die Eigenschaften für Name und Value (Wert) wie folgt fest:
   - Name = ClientBusinessServiceX
   - Value = BusinessObjects Integration

Sie erstellen nun das Menüelement "Crystal Reports", über das der importierte Siebel-Befehl aufgerufen wird.

24.4.3 Kontextsensitivität

Kontextsensitivität ist eine Funktion, über die dem Benutzer aufgabenrelevante Berichte zur Verfügung gestellt werden. In diesem Fall würden Benutzern, die auf Crystal Reports direkt über eine Siebel-Clientanwendung zugreifen, automatisch Berichte angezeigt werden, die für die Integration von Siebel-Daten ausgelegt sind.

24.4.3.1 Konfiguration von Kontextsensitivität

Stellen Sie vor der Konfiguration der Kontextsensitivität sicher, dass Sie Folgendes durchgeführt haben:

- Sie haben BusinessObjects XI Integration für Siebel installiert
- Sie haben Siebel für die Integration in BI-Plattform konfiguriert

1. Öffnen Sie die Central Management Console (CMC).

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

2. Klicken Sie auf **Authentifizierung**.
3. Doppelklicken Sie auf **Siebel**.
   Die Siebel-Zuordnungsschnittstelle wird angezeigt.
4. Klicken Sie auf **Domänen**.
   Die Domänen-Zuordnungsschnittstelle wird angezeigt.
5. Notieren Sie den Domänennamen, der dem zu verwendenden Siebel-Server entspricht.
6. Schließen Sie die Siebel- Zuordnungsschnittstelle.
7. Öffnen Sie BI-Launchpad.
8. Erstellen Sie einen neuen Ordner unter `PublicFolders\Siebel` mit demselben Namen wie die Siebel-Domäne in der CMC.
9. Legen Sie alle Berichte, in die Siebel-Informationen integriert werden sollen, in diesem Ordner ab.

24.4.3.2 Festlegen der URL für Kontextsensitivität

1. Wechseln Sie nach Neuerstellung der JavaScript-Dateien der Anwendung in den Ordner "Siebel Files" Ihrer `BI-Plattform-Installation`, der sich standardmäßig im folgenden Verzeichnis befindet: C:\Programme \Business Objects\SAP BusinessObjects Enterprise XI\Siebel Files\.
2. Kopieren Sie die Datei `BusinessObjectsEnterpriseServer.html`. Suchen Sie anschließend den öffentlichen Ordner, in dem das Programm "genbscript" die neuen JavaScript-Dateien erstellt hat, und legen Sie eine Kopie der Datei `BusinessObjectsEnterpriseServer.html` im entsprechenden Sprachunterordner ab.

   Wenn Sie beispielsweise die JavaScript-Dateien einer Anwendung im Ordner `c:\sea752\SWEApp\PUBLIC \ENU` auf dem Siebel-Server erstellt haben, kopieren Sie die Datei `BusinessObjectsEnterpriseServer.html` in den Ordner `c:\sea752\SWEApp\PUBLIC\ENU`.
3. Öffnen Sie die Datei `BusinessObjectsEnterpriseServer.html` aus dem öffentlichen Ordner in einem Texteditor, z.B. Notepad, und suchen Sie die folgende Zeile:

```
Var userDomain = "SIEB78"

var destAddr = "http://<SAP-BusinessObjects-Server>:8080/BOE/BI/logon/
siebelStart.do"
```

> **Hinweis**
>
> Um die Variable **`<userDomain>`** oder **`<destAddr>`** zu ändern, müssen Sie die Webseiten im Cache Ihres Browsers löschen, um sicherzustellen, dass der Browser auf die richtige Zieladresse zeigt.

> **Hinweis**
>
> Für die Variable "userDomain" wird zwischen Groß- und Kleinschreibung unterschieden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.4.3.3 Verifizieren der Kontextsensitivität

1. Klicken Sie in Siebel-Tools auf **Debug (Debuggen)** > **Start**.
2. Wechseln Sie zu einem beliebigen Bildschirm und klicken Sie auf das Menü **View** (Ansicht).
   Ihr neues Crystal-Reports-Menüelement müsste in dem Menü angezeigt werden.
3. Klicken Sie auf das Menüelement **Crystal Reports**.
   Die BI-Plattform öffnet das BI-Launchpad-Fenster, in das der Benutzername und das Kennwort für die Verbindung eingegeben werden muss. Diese Angaben sind nur bei der ersten Anmeldung vor der Zeitüberschreitung der Sitzung erforderlich. Der in HTML konfigurierte Domänenname und die Siebel-Authentifizierung müssten bereits ausgefüllt sein.

> **Hinweis**
>
> Dieser Schritt dient nur zur Verifizierung der Installation bis zu diesem Punkt. Vor der Anmeldung bei der BI-Plattform über die Siebel-Authentifizierung müssen Sie der BI-Plattform Siebel-Zuständigkeiten zugeordnet haben.

24.4.3.4 Hinzufügen von Ordnern zur BI-Plattform

Die BI-Plattform Integration für Siebel erfordert, dass einige Ordner zu BI-Launchpad hinzugefügt werden, um die Kontextsensitivität vollständig zu ermöglichen.

Um die Funktionalität zu gewährleisten, sollte der Kontextordner folgende Struktur aufweisen: `Öffentliche Ordner\Siebel\<Domänenname>`. Nur Berichte, die im Unterordner `<Domänenname>` gespeichert sind und im Siebel-System so konfiguriert wurden, dass sie auf die entsprechende SAP-BusinessObjects-Geschäftskomponente verweisen, werden als Teil der Kontextsensitivitätsfunktion angezeigt. Der hier verwendete `<Domänenname>` muss mit dem Domänennamen übereinstimmen, der für Siebel in der Authentifizierungskonfiguration konfiguriert wurde, und er muss außerdem mit dem in der Datei `BusinessObjectsEnterpriseServer.html` auf Siebelseite konfigurierten Wert übereinstimmen.

> **Hinweis**
>
> Die Schritte in diesem Abschnitt müssen von Siebel Tools durchgeführt werden.

24.4.4 Konfigurieren der Einzelanmeldung für SAP Crystal Reports und Siebel

Die BI-Plattform ist standardmäßig so konfiguriert, dass Benutzer von SAP Crystal Reports mit der Einzelanmeldung auf Siebel-Daten zugreifen können.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

24.4.4.1 Deaktivieren der Einzelanmeldung für Siebel und SAP Crystal Reports

1. Klicken Sie in der Central Management Console (CMC) auf **Anwendungen**.
2. Doppelklicken Sie auf **Crystal-Reports-Konfiguration**.
3. Klicken Sie auf **Einzelanmeldungsoptionen**.
4. Wählen Sie **crdb_siebel**.
5. Klicken Sie auf **Entfernen**.
6. Klicken Sie auf **Speichern und schließen**.
7. Starten Sie SAP Crystal Reports erneut.

24.4.4.2 Aktivieren der Einzelanmeldung für Siebel und SAP Crystal Reports

Wenn Sie die Einzelanmeldung für Siebel und SAP Crystal Reports deaktiviert haben und wieder aktivieren möchten.

1. Klicken Sie in der Central Management Console (CMC) auf **Anwendungen**.
2. Doppelklicken Sie auf **Crystal-Reports-Konfiguration**.
3. Klicken Sie auf **Einzelanmeldungsoptionen**.
4. Geben Sie unter *SSO-Kontext für Datenbankanmeldung verwenden...* **crdb_siebel** ein.
5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Speichern und schließen**.
7. Starten Sie die SAP Crystal Reports-Server erneut.

24.4.5 Konfigurieren für Secure Sockets Layer-Kommunikation

Sie können das SSL-Protokoll (Secure Sockets Layer) für die gesamte Netzwerkkommunikation zwischen Clients und Servern in Ihrer Siebel- und BI-Plattform-Implementierung verwenden.

Speichern Sie wie bei der SSL-Konfiguration für andere BI-Plattform-Server und -Clients folgende KEY- und Zertifikatdateien in einem geschützten Verzeichnis, auf das die Rechner Ihrer Siebel-Implementierung Zugriff haben.

- Die vertrauenswürdige Zertifikatdatei (cacert.der).
- Die generierte Serverzertifikatdatei (servercert.der).
- Die Serverschlüsseldatei (server.key).
- Die Kennsatzdatei (passphrase.txt).

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Datei mit der SSL-Konfigurationseigenschaft

Die Eigenschaftendatei `sslconf.properties` enthält alle Informationen für die erforderlichen Zertifikate und Schlüssel, die von der Integration für Siebel-Komponenten verwendet werden. Beispiel:

```
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Die Datei `sslconf.properties` sollte im Installationsordner der BI-Plattform abgelegt werden; standardmäßig ist dies `C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`.

24.4.5.1 Einrichten der Siebel-Datenkonnektivität mit SSL

> **Hinweis**
>
> Bei allen im nachfolgenden Verfahren beschriebenen Werten wird zwischen Groß- und Kleinschreibung unterschieden.

1. Kopieren Sie Ihre SSL-Zertifikate nach `C:\SSLCert`.
2. Starten Sie den Central Configuration Manager (CCM).
3. Halten Sie den Server Intelligence Agent (SIA) an.
4. Doppelklicken Sie auf den SIA, um das Dialogfeld *Eigenschaften* zu öffnen.
5. Klicken Sie auf die Registerkarte **Protokoll**.
6. Wählen Sie **SSL aktivieren**.
7. Wählen Sie für den *SSL-Zertifikatordner* das Verzeichnis aus, das die SSL-Zertifikate enthält: `C:\SSLCert`.
8. Wählen Sie unter *Server-SSL-Zertifikatdatei* die Datei `servercert.der`.
9. Wählen Sie unter *Dateien für vertrauenswürdige SSL-Zertifikate* die Datei `cacert.der`.
10. Wählen Sie unter *Datei für den privaten SSL-Schlüssel* die Datei `server.key`.
11. Wählen Sie unter *Kennphrasendatei für den privaten SSL-Schlüssel* die Datei `passphrase.key`.
12. Klicken Sie auf **Anwenden**.
13. Starten Sie den Server Intelligence Agent.

Der BI-Plattform-Reporting-Server (z.B. Adaptive Job Server) muss neu gestartet werden, damit die Änderungen übernommen werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

25 Verwalten und Konfigurieren von Protokollen

25.1 Protokollieren der Ablaufverfolgung für Komponenten

Protokolle

Die BI-Plattform generiert Meldungen auf Systemebene und schreibt diese in Protokolldateien. Systemadministratoren können diese Protokolldateien verwenden, um die Leistung zu überwachen oder Fehler zu beheben.

Ablaufverfolgungen

Die BI-Plattform generiert außerdem Ablaufverfolgungen (Aufzeichnungen von Ereignissen, die während der Ausführung einer überwachten Komponente auftreten) und sammelt diese in Protokolldateien mit der Erweiterung `.glf`. Die verfolgten Ereignisse reichen von Statusmeldungen bis hin zu schweren Ausnahmefehlern. SAP-Support-Mitarbeiter und -Entwickler können mithilfe von Ablaufverfolgungen die Leistung von BI-Plattform-Komponenten (Server und Webanwendungen) sowie die Aktivität der überwachten Komponenten darstellen.

Durch das Festlegen der Protokollierungsebene der Ablaufverfolgung bestimmen Sie den Typ und die Ausführlichkeit der an die Protokolldatei gesendeten Informationen. Die Protokollierungsebene der Ablaufverfolgung ist ein Filter, mit dem Ablaufverfolgungen unter einem bestimmten Grenzwert unterdrückt werden. Durch die Überwachung des Ablaufverfolgungsprotokolls einer Komponente können Sie bestimmen, ob die aktuelle Instanz einer Komponente oder deren Konfiguration geändert werden muss, um unter einer erhöhten Arbeitslast ausgeführt werden zu können.

> **Hinweis**
>
> Sie können BI-Plattform-Protokolldateien mit einem beliebigen Texteditor anzeigen.

25.2 Ablaufverfolgungsprotokollierungsebenen

Folgende Ablaufverfolgungsprotokollierungsebenen stehen für BI-Plattform-Komponenten zur Verfügung:

Ebene	Beschreibung
Nicht angegeben	Die Ablaufverfolgungsprotokollierungsebene wird über einen anderen Mechanismus angegeben (normalerweise eine `.ini`-Datei).
Keine	Es erfolgt keine Ablaufverfolgung.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Ebene	Beschreibung
Niedrig	Der Filter für die Ablaufverfolgungsprotokollierung ermöglicht die Protokollierung von Fehlermeldungen, während Warn- und Statusmeldungen ignoriert werden. Wichtige Statusmeldungen werden für Meldungen für Start, Herunterfahren, Start- und Endanforderung für Komponenten protokolliert. Diese Ebene wird für Debuggingzwecke nicht empfohlen.
Mittel	Der Ablaufverfolgungsprotokollfilter ist so eingestellt, dass Fehler-, Warn- und die meisten Statusmeldungen berücksichtigt werden. Weniger wichtige oder sehr umfangreiche Statusmeldungen werden herausgefiltert. Diese Ebene ist nicht ausreichend ausführlich für das Debugging.
Hoch	Es werden keine Meldungen gefiltert. Diese Ebene wird für Debuggingzwecke empfohlen. **Achtung** Diese Ablaufverfolgungsprotokollierungsebene wirkt sich in hohem Maße auf die Systemressourcen aus, indem die Prozessorauslastung erhöht und mehr Speicherplatz belegt wird.

25.3 Konfigurieren der Serververfolgung

Eine Protokollnachricht ist eine permanente Aufzeichnung der Ereignisse und des Status eines Softwaresystems. Die Ablaufverfolgungsdaten für eine überwachte BI-Plattform-Implementierung werden in eine spezielle `.glf`-Protokolldatei geschrieben und im Protokollierungsverzeichnis gespeichert.

- Unter Windows ist das Standardverzeichnis **`<INSTALLVERZ>`**`\SAP BusinessObjects Enterprise XI 4.0\logging`
- Unter Unix ist das Standardverzeichnis **`<INSTALLVERZ>`**`/sap_bobj/logging`

Der Name der `.glf`-Protokolldatei setzt sich aus einer Kurz-ID, dem Servernamen und einer Zahlenreferenz zusammen, beispielsweise `aps_mysia.AdaptiveProcessingServer_trace.000012.glf`. Sobald sich die Größe der Protokolldatei dem 10-MB-Schwellenwert nähert, wird eine neue Ablaufverfolgungsprotokolldatei für den überwachten Server erstellt. Außerdem werden fünf Protokolldateien gleichzeitig verwaltet. Während neue Protokolldateien erstellt werden, werden alte Protokolldateien gelöscht.

Durch Festlegen von Ablaufverfolgungsprotokoll-Ebenen für einen bestimmten Server oder eine bestimmte Servergruppe können Sie den Schweregrad und die Wichtigkeitsstufe der in der Protokolldatei erfassten Ablaufverfolgungsdaten regulieren.

Hinweis

Um die Ablaufverfolgungsprotokoll-Ebenen für bestimmte Server oder Servergruppen zu ändern, verwenden Sie die Ablaufverfolgungsprotokoll-Einstellungen in der Central Management Console (CMC). Um andere

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter zu ändern, ändern Sie die Ablaufverfolgungsprotokoll-Ebene und andere Einstellungen manuell in der Datei `BO_trace.ini`

25.3.1 Festlegen der Protokollierungsebene in der CMC

Die Protokollierungsebene der Ablaufverfolgung für einen Server kann ohne Auswirkungen auf andere Verfolgungseinstellungen angepasst werden.

1. Greifen Sie im Abschnitt *Server* in der CMC auf einen Server zu.
   - Wählen Sie einen Server einer bestimmten Kategorie aus.
   - Klicken Sie im Navigationsbereich auf **Serverliste** , um die vollständige Serverliste aufzurufen, und wählen Sie einen Server aus.
2. Klicken Sie mit der rechten Maustaste auf den ausgewählten Server, und wählen Sie **Eigenschaften** aus.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
3. Wählen Sie im Bereich *Ablaufverfolgungsprotokoll-Einstellungen* eine Einstellung in der Liste **Protokollierungsebene** aus.
4. Klicken Sie auf **Speichern und schließen**.

Die neue Protokollierungsebene wird sofort wirksam.

Um ein anderes Ausgabeverzeichnis für die Protokolldateien anzugeben, geben Sie den Parameter `–loggingPath <Zielverzeichnis>` im Bereich *Befehlszeilenparameter* ein. Starten Sie den Server neu, damit die Einstellung wirksam wird.

Weitere Informationen

Ablaufverfolgungsprotokollierungsebenen [Seite 595]

25.3.2 Festlegen der Protokollierungsebene für für mehrere Server in der CMC

1. Greifen Sie im Abschnitt *Server* der CMC auf mehrere Server zu.
   - Wählen Sie Server einer bestimmten Kategorie aus.
   - Klicken Sie im Navigationsbereich auf **Serverliste** , um die vollständige Serverliste aufzurufen. Halten Sie die *STRG* -Taste gedrückt, und klicken Sie auf mehrere Server, um sie auszuwählen.
2. Klicken Sie mit der rechten Maustaste auf die ausgewählten Server und wählen **Gemeinsame Dienste bearbeiten**.
   Das Dialogfeld *Gemeinsame Dienste bearbeiten* wird angezeigt.
3. Wählen Sie im Bereich *Ablaufverfolgungsprotokoll-Einstellungen* eine Einstellung in der Liste **Protokollierungsebene** aus.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

4. Klicken Sie auf **OK**.

Die neue Protokollierungsebene wird sofort wirksam.

Um ein anderes Ausgabeverzeichnis für die Protokolldateien anzugeben, geben Sie den Parameter –`loggingPath` **`<Zielverzeichnis>`** im Bereich *Befehlszeilenparameter* ein. Starten Sie den Server neu, damit die Einstellung wirksam wird.

Weitere Informationen

Ablaufverfolgungsprotokollierungsebenen [Seite 595]

25.3.3 Konfigurieren der Serververfolgung mit der Datei "BO_trace.ini"

In der Datei `BO_trace.ini` werden standardmäßig nur Fehler und Assertionen protokolliert.

1. Öffnen Sie die Datei `BO_trace.ini`.
   - Unter Windows ist das Standardverzeichnis **`<INSTALLVERZ>`**`\SAP BusinessObjects Enterprise XI 4.0\conf\`.
   - Unter Unix ist das Standardverzeichnis **`<<INSTALLVERZ>>`**`/sap_bobj/enterprise_xi40/conf/`.
2. Entfernen Sie den Kommentar aus den Zeilen im Abschnitt “Trace Syntax and Setting”.
3. Ändern Sie die Parameter für die Serverablaufverfolgung. Die folgenden Parameter werden zum Konfigurieren der Serverablaufverfolgung verwendet:

Parameter	Mögliche Werte	Beschreibung
`sap_log_level`	**`log_information`** **`log_warning`** **`log_error`** **`log_fatal`** **`log_none`**	Legt die Wichtigkeitsstufe von Protokollnachrichten fest. Die Standardwichtigkeitsstufe für Protokollnachrichten ist **`log_error`**. Die Wichtigkeitstufe der Protokollnachrichten folgt einer Hierarchie, wobei **`log_information`** die wichtigste Stufe und **`log_none`** die am wenigsten wichtige Stufe ist. Wenn Sie eine Wichtigkeitsstufe für Protokollnachrichten festlegen, werden alle Protokollnachrichten dieser Wichtigkeitsstufe und darunter liegender Wichtigkeitsstufen angezeigt. Wenn Sie die

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Mögliche Werte	Beschreibung
		Wichtigkeitsstufe beispielsweise auf **log_warning** setzen, werden Nachrichten des Typs **log_warning**, **log_error** und **log_fatal** in die Protokolldatei geschrieben. **Hinweis** **log_information** und **log_warning** kann auf **log_info** und **log_warn** abgekürzt werden.
sap_trace_level	**trace_debug** **trace_path** **trace_information** **trace_error** **trace_none**	Legt die Wichtigkeitsstufe von Ablaufverfolgungsnachrichten fest. Die Standardwichtigkeitsstufe für Ablaufverfolgungsnachrichten ist **trace_error**. Die Wichtigkeitstufe der Ablaufverfolgungsnachrichten folgt einer Hierarchie, wobei **trace_debug** die wichtigste Stufe und **trace_none** die am wenigsten wichtige Stufe ist. Wenn Sie eine Wichtigkeitsstufe für Ablaufverfolgungsnachrichten festlegen, werden alle Ablaufverfolgungsnachrichten dieser Wichtigkeitsstufe und darunter liegender Wichtigkeitsstufen angezeigt. Wenn Sie die Wichtigkeitsstufe beispielsweise auf **trace_path** setzen, werden Nachrichten des Typs **trace_path**, **trace_information** und **trace_error** in die Protokolldatei geschrieben. **Hinweis** **trace_information** kann mit **trace_info** abgekürzt werden.

4. Speichern und schließen Sie die Datei `BO_trace.ini`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Die Datei `BO_trace.ini` wird häufig gelesen. An der Datei `BO_trace.ini` vorgenommene Änderungen werden fünf Minuten, nachdem sie gespeichert wurden, wirksam. Wenn Sie den CMS neu starten, werden an der Datei `BO_trace.ini` vorgenommene Änderungen sofort wirksam.

Beispiel

Datei `BO_trace.ini`

```
sap_log_level=log_warning;
sap_trace_level=trace_path;
```

25.3.3.1 Konfigurieren der Ablaufverfolgung für einen bestimmten Server

Die Datei `BO_trace.ini` enthält Parameter für die Ablaufverfolgung für BI-Plattform-Server. Die Einstellungen wirken sich auf alle verwalteten Server aus. Administratoren können in der Datei `BO_trace.ini` bestimmte Ablaufverfolgungsparameter für einen spezifischen Server festlegen.

Achtung

Neue Einstellungen auf der Protokollierungsebene der Ablaufverfolgung, die in der CMC für einen bestimmten Server angegeben werden, überschreiben sämtliche Einstellungen in der Datei `BO_trace.ini`.

1. Öffnen Sie die Datei `BO_trace.ini`.
   - Unter Windows ist das Standardverzeichnis **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\conf\`.
   - Unter Unix ist das Standardverzeichnis **<<INSTALLVERZ>>**`/sap_bobj/enterprise_xi40/conf/`.
2. Verwenden Sie eine `If`-Anweisung, um Ablaufverfolgungseinstellungen für einen bestimmten Server anzugeben. Beispiel:

   ```
   if (process == "aps_MySIA.ProcessingServer") {
     sap_log_level=log_warning;
     sap_trace_level=trace_path;
   }
   ```

   Tipp

   Der Prozess muss für die Ablaufverfolgungseinstellung angegeben werden, um für einen bestimmten Server zu gelten.
3. Speichern und schließen Sie die Datei `BO_trace.ini`.

Die modifizierten Einstellungen werden innerhalb von fünf Minuten implementiert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

25.4 Konfiguration der Ablaufverfolgung für Webanwendungen

Ablaufverfolgungen für eine überwachte BI-Plattform-Implementierung werden in eine spezifische `.glf`-Protokolldatei geschrieben und in einem Verzeichnis auf dem Rechner gespeichert, der den Webanwendungsordner hostet.

- Unter Windows ist das Standardverzeichnis `C:\SBOPWebapp_<ANWENDUNG>_<IP-ADRESSE>_<PORT>\`, z.B. `C:\SBOPWebapp_BIlaunchpad_192.0.2.0_8080\`
- Unter Unix ist das Standardverzeichnis `$userHome/SBOPWebapp_<ANWENDUNG>_<IP-ADRESSE>_<PORT>/`, z.B. `$userHome/SBOPWebapp_CMC_192.0.2.0_8080/`

Die Ablaufverfolgungsprotokollierungs-Ebene für Webanwendungen ist in der CMC standardmäßig auf **Nicht angegeben** gesetzt. Ablaufverfolgungsprotokolleinstellungen sind für die folgenden Anwendungen in der CMC verfügbar:

- Central Management Console
- BI-Launchpad
- Open Document
- Webdienst

> **Hinweis**
>
> Um die Ablaufverfolgungsprotokoll-Ebenen für bestimmte Server oder Servergruppen zu ändern, verwenden Sie die Ablaufverfolgungsprotokoll-Einstellungen in der Central Management Console (CMC). Um andere Parameter zu ändern, ändern Sie die Ablaufverfolgungsprotokoll-Ebene und andere Einstellungen manuell in der Datei `BO_trace.ini` Diese Datei wird zusammen mit den `BOE-war`- und `dswsbobje.war`-Dateien auf Ihrem Webanwendungsserver implementiert.

Vor der Konfiguration der Datei `BO_trace.ini` müssen die vorhandenen Webanwendungen mithilfe des WDeploy-Tools vom Webanwendungsserver deinstalliert werden. Nach der Konfiguration der Datei `BO_trace.ini` muss diese erneut mit den Webanwendungen auf dem Webanwendungsserver implementiert werden. Weitere Informationen zur Verwendung von WDeploy zur Vorbereitung, Installation und Deinstallation von Webanwendungen finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.

25.4.1 Einstellen der Ablaufverfolgungsprotokollierungsebene der Webanwendung in der CMC

Um andere Webanwendungen zu verfolgen, müssen Sie die entsprechende `BO_trace.ini`-Datei manuell konfigurieren.

1. Klicken Sie im Bereich *Anwendungen* der CMC mit der rechten Maustaste auf eine Anwendung und wählen **Ablaufverfolgungsprotokoll-Einstellungen**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Diese Anwendungen verfügen über Ablaufverfolgungsprotokoll-Einstellungen: BI-Launchpad, CMC, Open Document, Hochstufverwaltung, Versionsverwaltung, Grafischer Vergleich und Webdienst.

Das Dialogfeld *Ablaufverfolgungsprotokoll-Einstellungen* wird angezeigt.

2. Wählen Sie in der Liste **Protokollierungsebene** eine Einstellung aus.
3. Klicken Sie auf **Speichern und schließen**.

Die neue Ablaufverfolgungsprotokollierungsebene wird nach der nächsten Anmeldung an der Webanwendung wirksam.

Weitere Informationen

Ablaufverfolgungsprotokollierungsebenen [Seite 595]

25.4.2 Konfigurieren der Ablaufverfolgungseinstellungen mit der Datei `BO_trace.ini`

Die Datei `BO_trace.ini` wird zusammen mit `BOE`- und `dswsbobje-WAR`-Dateien auf dem Webanwendungsserver implementiert. Sie können die Datei `BO_trace.ini` verwenden, um Ablaufverfolgungsparameter für BI-Plattform-Webanwendungen anzugeben. Da der Zugriff auf diese Datei nicht immer möglich ist, muss die betroffene Webanwendung auf dem Webanwendungsserver deinstalliert werden.

1. Verwenden Sie WDeploy, um die Webanwendung vom Webanwendungsserver zu deinstallieren. Weitere Informationen zur Verwendung von WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.
   - Wenn Sie den im Lieferumfang der BI-Plattform enthaltenen Tomcat-Webanwendungsserver verwenden, müssen die Webanwendungen nicht deinstalliert werden. Sie können die Dateien direkt ändern.
     - Die Konfigurationsdatei der Ablaufverfolgung für die `BOE.war`-Datei ist verfügbar unter **`<INSTALLVERZ>`**`\Tomcat\webapps\BOE\WEB-INF\TraceLog`.
     - Die Konfigurationsdatei der Ablaufverfolgung für die Datei `dswsbobje.war` ist verfügbar unter **`<INSTALLVERZ>`**`\Tomcat\webapps\dswsbobje\WEB-INF\conf`.

> **Hinweis**
>
> Wenn Sie den gebündelten Tomcat-Webanwendungsserver verwenden, überspringen Sie Schritt 2.

2. Greifen Sie auf eine vorimplementierte Version der Datei `BO_trace.ini` zu:
   - Der Standardspeicherort für eine vorimplementierte Version der Konfigurationsdatei für die Datei `BOE.war` ist **`<INSTALLVERZ>`**`\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Der Standardspeicherort für eine vorimplementiert Version der Konfigurationsdatei für die Datei `dswsbobje.war` ist **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`

3. Öffnen Sie die Datei `BO_trace.ini`.
   - Unter Windows ist das Standardverzeichnis **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\conf\`.
   - Unter Unix ist das Standardverzeichnis **<<INSTALLVERZ>>**`/sap_bobj/enterprise_xi40/conf/`.
4. Ändern Sie die Parameter für die Serverablaufverfolgung. Die folgenden Parameter werden zum Konfigurieren der Serverablaufverfolgung verwendet:

Parameter	Mögliche Werte	Beschreibung
sap_log_level	**log_information** **log_warning** **log_error** **log_fatal** **log_none**	Legt die Wichtigkeitsstufe von Protokollnachrichten fest. Die Standardwichtigkeitsstufe für Protokollnachrichten ist **log_error**. Die Wichtigkeitstufe der Protokollnachrichten folgt einer Hierarchie, wobei **log_information** die wichtigste Stufe und **log_none** die am wenigsten wichtige Stufe ist. Wenn Sie eine Wichtigkeitsstufe für Protokollnachrichten festlegen, werden alle Protokollnachrichten dieser Wichtigkeitsstufe und darunter liegender Wichtigkeitsstufen angezeigt. Wenn Sie die Wichtigkeitsstufe beispielsweise auf **log_warning** setzen, werden Nachrichten des Typs **log_warning**, **log_error** und **log_fatal** in die Protokolldatei geschrieben. **Hinweis** **log_information** und **log_warning** kann auf **log_info** und **log_warn** abgekürzt werden.
sap_trace_level	**trace_debug** **trace_path** **trace_information** **trace_error** **trace_none**	Legt die Wichtigkeitsstufe von Ablaufverfolgungsnachrichten fest. Die Standardwichtigkeitsstufe für Ablaufverfolgungsnachrichten ist **trace_error**.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Mögliche Werte	Beschreibung
		Die Wichtigkeitstufe der Ablaufverfolgungsnachrichten folgt einer Hierarchie, wobei **trace_debug** die wichtigste Stufe und **trace_none** die am wenigsten wichtige Stufe ist. Wenn Sie eine Wichtigkeitsstufe für Ablaufverfolgungsnachrichten festlegen, werden alle Ablaufverfolgungsnachrichten dieser Wichtigkeitsstufe und darunter liegender Wichtigkeitsstufen angezeigt. Wenn Sie beispielsweise die Wichtigkeitsstufe der Ablaufverfolgung auf **trace_path** festlegen, werden Meldungen, die **trace_path**, **trace_info** und **trace_error** umfassen, in die Protokolldatei geschrieben. **Hinweis** **trace_information** kann mit **trace_info** abgekürzt werden.

5. Speichern und schließen Sie die Datei `BO_trace.ini`.
6. Verwenden Sie Wdeploy zum Implementieren der `.war`-Datei auf dem Rechner, der den Webanwendungsserver hostet.

Die modifizierten Ablaufverfolgungseinstellungen werden nach der nächsten Webanwendungsanmeldung wirksam.

25.4.2.1 Konfiguration der Ablaufverfolgung für eine bestimmte Webanwendung

Die Datei `BO_trace.ini` wird zusammen mit `BOE`- und `dswsbobje-WAR`-Dateien auf dem Webanwendungsserver implementiert. Sie können die Datei `BO_trace.ini` verwenden, um Ablaufverfolgungsparameter für BI-Plattform-Webanwendungen anzugeben. Da der Zugriff auf diese Datei nicht immer möglich ist, muss die betroffene Webanwendung auf dem Webanwendungsserver deinstalliert werden. Nachfolgend werden die Webanwendungen und die damit verknüpften `.war`-Dateien aufgeführt:

Webanwendung	WAR-Datei	Vorimplementierter Speicherort
Central Management Console	`BOE.war`	**<INSTALLVERZ>**\SAP BusinessObjects Enterprise

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Webanwendung	WAR-Datei	Vorimplementierter Speicherort
		XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
BI-Launchpad	BOE.war	**<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
Open Document	BOE.war	**<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
Webdienst	dswsbobje.war	**<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf

1. Verwenden Sie WDeploy, um die Webanwendung vom Webanwendungsserver zu deinstallieren. Weitere Informationen zur Verwendung von WDeploy finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.
   - Wenn Sie den im Lieferumfang der BI-Plattform enthaltenen Tomcat-Webanwendungsserver verwenden, müssen die Webanwendungen nicht deinstalliert werden. Sie können die Datei direkt ändern.
     - Die Konfigurationsdatei der Ablaufverfolgung für die BOE.war-Datei ist verfügbar unter **<INSTALLVERZ>**\Tomcat\webapps\BOE\WEB-INF\TraceLog.
     - Die Konfigurationsdatei der Ablaufverfolgung für die Datei dswsbobje.war ist verfügbar unter **<INSTALLVERZ>**\Tomcat\webapps\dswsbobje\WEB-INF\conf.

   Hinweis

   Wenn Sie den gebündelten Tomcat-Webanwendungsserver verwenden, überspringen Sie Schritt 2.

2. Greifen Sie auf eine vorimplementierte Version der Datei BO_trace.ini zu:
   - Der Standardspeicherort für eine vorimplementierte Version der Konfigurationsdatei für die Datei BOE.war ist **<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
   - Der Standardspeicherort für eine vorimplementiert Version der Konfigurationsdatei für die Datei dswsbobje.war ist **<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf
3. Öffnen Sie die Datei BO_trace.ini.
   - Unter Windows ist das Standardverzeichnis **<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\conf\.
   - Unter Unix ist das Standardverzeichnis **<<INSTALLVERZ>>**/sap_bobj/enterprise_xi40/conf/.
4. Verwenden Sie eine If-Anweisung, um Ablaufverfolgungseinstellungen für eine bestimmte Webanwendung anzugeben. Beispiel:

```
if (device_name == "Webapp_opendocument_trace") {
  sap_log_level=log_warning;
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

```
  sap_trace_level=trace_path;
}
```

Der Prozess muss für die Ablaufverfolgungseinstellung angegeben werden, um für einen bestimmten Webanwendungsserver zu gelten. Folgende Webanwendungen sind nach der ersten Installation verfügbar:

Webanwendung	Gerätename
BI-Launchpad	**WebApp_BIlaunchpad**
Central Management Server	**WebApp_CMC**
OpenDocument	**WebApp_OpenDocument**

Folgende Parameter werden zur Konfiguration der Webanwendungsserver-Ablaufverfolgung verwendet:

Parameter	Mögliche Werte	Beschreibung
sap_log_level	**log_information** **log_warning** **log_error** **log_fatal** **log_none**	Legt die Wichtigkeitsstufe von Protokollnachrichten fest. Die Standardwichtigkeitsstufe für Protokollnachrichten ist **log_error**. Die Wichtigkeitstufe der Protokollnachrichten folgt einer Hierarchie, wobei **log_information** die wichtigste Stufe und **log_none** die am wenigsten wichtige Stufe ist. Wenn Sie eine Wichtigkeitsstufe für Protokollnachrichten festlegen, werden alle Protokollnachrichten dieser Wichtigkeitsstufe und darunter liegender Wichtigkeitsstufen angezeigt. Wenn Sie die Wichtigkeitsstufe beispielsweise auf **log_warning** setzen, werden Nachrichten des Typs **log_warning**, **log_error** und **log_fatal** in die Protokolldatei geschrieben. **Hinweis** **log_information** und **log_warning** kann auf **log_info** und **log_warn** abgekürzt werden.
sap_trace_level	**trace_debug** **trace_path** **trace_information** **trace_error** **trace_none**	Legt die Wichtigkeitsstufe von Ablaufverfolgungsnachrichten fest. Die Standardwichtigkeitsstufe für

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Mögliche Werte	Beschreibung
		Ablaufverfolgungsnachrichten ist **trace_error**. Die Wichtigkeitstufe der Ablaufverfolgungsnachrichten folgt einer Hierarchie, wobei **trace_debug** die wichtigste Stufe und **trace_none** die am wenigsten wichtige Stufe ist. Wenn Sie eine Wichtigkeitsstufe für Ablaufverfolgungsnachrichten festlegen, werden alle Ablaufverfolgungsnachrichten dieser Wichtigkeitsstufe und darunter liegender Wichtigkeitsstufen angezeigt. Wenn Sie beispielsweise die Wichtigkeitsstufe der Ablaufverfolgung auf **trace_path** festlegen, werden Meldungen, die **trace_path**, **trace_info** und **trace_error** umfassen, in die Protokolldatei geschrieben. **Hinweis** **trace_information** kann mit **trace_info** abgekürzt werden.

5. Speichern und schließen Sie die Datei `BO_trace.ini`.
6. Verwenden Sie Wdeploy zum Implementieren der `.war`-Datei auf dem Rechner, der den Webanwendungsserver hostet.

25.5 Konfiguration der Ablaufverfolgung für das Upgrade-Management-Tool

Sie können mit der CMC keine Konfiguration der Ablaufverfolgung für das Upgrade-Management-Tool durchführen. Die Ablaufverfolgung für das Upgrade-Management-Tool muss über die Datei `BO_trace.ini` erfolgen.

- Unter Windows ist das Standardverzeichnis **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\conf\`.
- Unter Unix ist das Standardverzeichnis **<<INSTALLVERZ>>**`/sap_bobj/enterprise_xi40/conf/`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

25.5.1 Konfiguration der Ablaufverfolgung für das Upgrade-Management-Tool

1. Öffnen Sie die Datei `BO_trace.ini`.
   - Unter Windows ist das Standardverzeichnis **`<INSTALLVERZ>`**`\SAP BusinessObjects Enterprise XI 4.0\conf\`.
   - Unter Unix ist das Standardverzeichnis **`<<INSTALLVERZ>>`**`/sap_bobj/enterprise_xi40/conf/`.
2. Entfernen Sie den Kommentar aus den erforderlichen Zeilen im Abschnitt *Trace Syntax and Setting*.
3. Verwenden Sie eine `If`-Anweisung, um die Einstellungen für die Ablaufverfolgung anzugeben. Beispiel:

```
if (process == "upgrademanagementtool") {
  sap_log_level=log_warning;
  sap_trace_level=trace_path;
}
```

> **Tipp**
>
> Der Prozess muss in den Einstellungen der Ablaufverfolgung als `upgrademanagementtool` angegeben werden, um auf das Upgrade-Management-Tool angewendet werden zu können.

4. Speichern und schließen Sie die Datei `BO_trace.ini`.

Die modifizierten Einstellungen werden innerhalb von fünf Minuten implementiert.

25.6 Konfigurieren der Verfolgung für BI-Plattform-Client-Anwendungen

Verfolgung kann auf den folgenden Clients aktiviert werden:

- Universe-Design-Tool
- Information-Design-Tool
- Web-Intelligence-Rich-Client

Sie können die Verfolgung für diese Komponenten konfigurieren, indem Sie die .ini-Dateien für jeden Client-Typ bearbeiten. Diese .ini-Dateien funktionieren genauso wie die BO_trace.ini-Datei, die an anderer Stelle in diesem Kapitel beschrieben ist. Einzelheiten zum Ändern der .ini-Datei finden Sie unter *Konfigurieren der Serververfolgung mit der Datei "BO_trace.ini"* [Seite 864].

Die Dateien müssen sich in den für diese Anwendungen konfigurierten Arbeitsverzeichnissen befinden (standardmäßig `<INSTALLVERZ>\SAP BusinessObjects`). Falls sie noch nicht vorhanden sind, müssen Sie sie erstellen. Die Dateien haben folgende Namen:

- Universe-Design-Tool: `designer_trace.ini`.
- Information-Design-Tool: `BO_Trace.ini`
- Web-Intelligence-Rich-Client: `WebIRichClient_trace.ini`

Weitere Informationen zu diesen Produkten erhalten Sie in der Dokumentation.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

26 Integration in SAP Solution Manager

26.1 Übersicht über die Integration

Um die Integration in SAP Solution Manager zu ermöglichen, wurde die BI-Plattform um Unterstützungsfunktionen erweitert. Die folgenden SAP Solution Manager™-Komponenten können verwendet werden, um die BI-Plattform-Implementierung zu unterstützen:

- Solution Landscape Directory
- Solution Manager Diagnostics
- Introscope von CA Wily
- SAP Passport

> **Hinweis**
>
> Das SAP-Supportportal für SAP BusinessObjects finden Sie unter:*https://websmp205.sap-ag.de/bosap-support*

26.2 Checkliste für die SAP Solution Manager-Integration

Der folgenden Tabelle können Sie entnehmen, welche Komponenten erforderlich sind, damit SAP Solution Manager Unterstützung für die BI-Plattform bereitstellen kann.

SAP Solution Manager-Unterstützung	Für die BI-Plattform erforderlich
SLD-Registrierung	• SAPHOSTAGENT muss installiert sein, um die Registrierung von BI-Plattform-Servern zu aktivieren. **Hinweis** Wenn SAPHOSTAGENT bereits installiert ist, registriert das BI-Plattform-Installationsprogramm die Server automatisch. • Für den Data Supplier, der Berichte für die Backend-Server erstellt, muss die Datei connect.key erstellt werden. • (Optional) Für die SLD-Registrierung bei WebSphere 6.1 oder 7 muss das SLDREG-Registrierungstool auf jedem WebSphere-Webanwendungsserver installiert werden. Weitere Informationen finden Sie im SAP-Hinweis 1482727. • (Optional) Für die SLD-Registrierung bei SAP NetWeaver 7.2 ist SLDREG auf jedem NetWeaver-Host zu installieren. Weitere Informationen finden Sie im SAP-Hinweis 1018839.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

SAP Solution Manager-Unterstützung	Für die BI-Plattform erforderlich
	• (Optional) Für die SLD-Registrierung mit Apache Tomcat, muss SLDREG auf jedem Tomcat-Server installiert werden. Weitere Informationen finden Sie im SAP-Hinweis 1508421.
SMD-Integration	• Der SMD Agent (DIAGNOSTICS.AGENT) muss auf alle Hosts von BI-Plattform-Servern heruntergeladen und auf diesen installiert werden. • Das SMAmin-Benutzerkonto muss in der BI-Plattform aktiviert sein.
Leistungsinstrumentation	• Introscope Agent muss zum Herstellen von Verbindungen zu Enterprise Manager konfiguriert werden. Verwenden Sie zum Konfigurieren der Verbindungen das BI-Plattform-Installationsprogramm oder CMC-Knotenplatzhalter. • Der SMD Agent muss installiert werden. • Die BI-Plattform muss für die Herstellung von Verbindungen zum SMD Agent konfiguriert werden. Verwenden Sie zum Konfigurieren der Verbindungen das BI-Plattform-Installationsprogramm oder CMC-Knotenplatzhalter.
SAP Passport	• Sie müssen das SAP Passport-Clienttool herunterladen und installieren.

26.3 Verwalten der System Landscape Directory-Registrierung

26.3.1 Registrierung der BI-Plattform in der Systemlandschaft

System Landscape Directory (SLD) ist ein zentrales Repository von Systemlandschaftsinformationen, die für die Verwaltung des Softwarelebenszyklus relevant sind. SLD enthält eine Beschreibung der Systemlandschaft, d.h. der derzeit installierten Systeme und Softwarekomponenten. Die Data Suppliers des SLD registrieren die Systeme auf dem SLD-Server und halten die Informationen auf dem neuesten Stand. Verwaltungs- und Geschäftsinformationen greifen auf die im SLD gespeicherten Informationen zu, um Aufgaben in einer DV-Umgebung für die Zusammenarbeit auszuführen.

Der im System Landscape Directory (SLD) enthaltene Data Supplier (DS) ist eine Anwendung, mit der die BI-Plattform-Server im SLD-Server registriert werden. Für jede Installation der Plattform wird ein spezifischer Data Supplier bereitgestellt, um Daten zu den folgenden Komponenten abzurufen:

- BI-Plattform-Server
- Auf dem WebSphere-Webanwendungsserver gehostete Webanwendungen und -dienste.

> **Hinweis**
>
> SAP NetWeaver verfügt über einen integrierten SLD-DS-Lieferanten, der den NetWeaver-Anwendungsserver sowie gehostete Webanwendungen und -dienste registriert. Dieser SLD-DS ist für in eine SAP NetWeaver-Umgebung integrierte BI-Plattform-Implementierungen relevant.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Der SLD-DS, der über BI-Plattform-Server berichtet, setzt voraus, dass das Programm SLDREG installiert und konfiguriert wurde. Das Programm SLDREG wird als Teil der Installation des Tools SAPHOSTAGENT installiert. Weitere Informationen zum Zugriff auf und die Installation von SAPHOSTAGENT finden Sie im Abschnitt zur "Vorbereitung" im *Installationshandbuch für SAP BusinessObjects Business Intelligence*. Nach der Installation von SLDREG erstellen Sie eine Datei `connect.key` für die Herstellung einer Verbindung zum SLD-Server.

Informationen zum Konfigurieren des spezifischen Datenlieferanten für WebSphere finden Sie im *Handbuch für die Implementierung von Webanwendungen*.

Während der Installation der BI-Plattform werden für die Registrierung der BI-Plattform benötigte Informationen in einer Konfigurationsdatei gespeichert. Diese Datei enthält Informationen, mit deren Hilfe der SLD-DS eine Verbindung zu der BI-Plattform-Datenbank herstellt.

26.3.1.1 Erstellen der Datei connect.key für den Data Supplier von SDL

Vor der Erstellung der Datei `connect.key` für den SLD-Datenlieferanten müssen Sie SAPHOSTAGENT herunterladen und installieren. Weitere Einzelheiten finden Sie im Abschnitt zur "Vorbereitung" im *Business-Intelligence-Installationshandbuch*.

> **Hinweis**
>
> Die Datei `connect.key` wird für die SLD-Registrierung bei dem Data Supplier benötigt, der Daten von den BI-Plattformservern abruft.

1. Öffnen Sie eine Befehlszeilenkonsole.
2. Navigieren Sie zum SAPHOSTAGENT-Standardinstallationspfad.
   - Unter Windows: `Programme\SAP\hostctrl\exe`
   - Unter Unix: `/usr/sap/hostctrl/exe`
3. Führen Sie den folgenden Befehl aus:
   ```
   sldreg -configure connect.key
   ```
4. Geben Sie die folgenden Konfigurationsoptionen ein
   - Benutzername
   - Kennwort
   - Host
   - Portnummer
   - Geben Sie an, dass HTTP verwendet werden soll

Das Tool `sldreg` erstellt die Datei connect.key, die automatisch vom Data Supplier verwendet wird, um Informationen per Push an den SLD-Server zu übertragen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

26.3.2 Auslösungszeitpunkt der SLD-Registrierung

Der SLD-Registrierungsprozess wird in folgenden Fällen vom Data Supplier ausgelöst, der Berichte für die BI-Plattform-Backend-Server erstellt:

- Ein Serverknoten auf Ihrer BI-Plattform-Implementierung wird neu gestartet.
- Ein neuer Server oder Knoten wird der Implementierung hinzugefügt.
- Ein Server oder Knoten wird gelöscht.

> **Hinweis**
>
> Wenn ein Server oder Knoten gelöscht wird, ändert der SLD-Registrierungsprozess den Inhalt auf dem SLD-Server nicht. Um den SLD-Server zu aktualisieren, wenn ein Server oder ein Knoten entfernt wird, löschen Sie das System aus dem SLD und senden es erneut, indem Sie die BI-Plattform neu starten.

Der Data Supplier für die WebSphere-SLD-Registrierung kann manuell aufgerufen werden oder für die Ausführung in einem bestimmten Intervall festgelegt sein, beispielsweise alle 24 Stunden. Weitere Informationen zur Konfiguration dieses Data Suppliers finden Sie im SAP-Hinweis 482727.

26.3.3 Protokollieren der SLD-Konnektivität

Konfigurationsdatei des Data Suppliers

Für BI-Plattform-Implementierungen wird eine Konfigurationsdatei erstellt, die für die SLD-Registrierung verwendet wird. Die Datei, `sldparserconfig.properties`, befindet sich in folgendem Verzeichnis: `<INSTALLVERZ>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/`.

Protokollieren der SLD-Konnektivität

Die Konnektivität zwischen dem SLD-Server und dem Data Supplier in der BI-Plattform-Implementierung wird über das Tool `sldreg` und die Datei `connect.key` gesteuert.

> **Hinweis**
>
> Der Name der Protokolldatei wird als Eigenschaft in der Datei `sldparserconfig.properties` angegeben.

Die Protokolldatei für den Data Supplier von SLD, der für die BI-Plattform-Backend-Server Berichte erstellt, befindet sich standardmäßig in folgendem Verzeichnis: `<INSTALLVERZ>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/bobjsldds.log`. Die Datei wird bei jeder Ausführung des Data Suppliers überschrieben.

Die Protokolldateien für `sldreg` befindet sich standardmäßig in folgendem Verzeichnis: `<INSTALLVERZ>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/log`. Die Namen der sldreg-Protokolldateien können nicht geändert werden und weisen folgendes Format auf: `sldreg_<Zeitstempel>.log`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Jedes Mal, wenn der Data Supplier sldreg aufruft, wird eine neue Protokolldatei erstellt.

26.4 Verwalten von Solution Manager Diagnostics Agents

26.4.1 Übersicht über Solution Manager Diagnostics (SMD)

Die SMD-Komponente (Solution Manager Diagnostics) von SAP Solution Manager bietet sämtliche Funktionen, die zur zentralen Analyse und Überwachung einer kompletten Systemlandschaft erforderlich sind. Die BI-Plattform kann vom SMD-Server überwacht werden, falls ein SMD Agent installiert ist. Der SMD Agent (`DIAGNOSTICS.AGENT`) erfasst Informationen für die SMD-Komponente, mit denen Problemursachen analysiert werden können. Zu den Informationen, die erfasst und an den SMD-Server gesendet werden, gehören Backend-Serverkonfigurationen und der Speicherort von Serverprotokolldateien.

26.4.2 Arbeiten mit SMD Agents

Der SMD Agent wird nicht von der BI-Plattform installiert. Der Agent, `DIAGNOSTICS.AGENT`, kann von *http://service.sap.com/swdc* heruntergeladen werden.

Informationen zum Installieren und Konfigurieren des Agenten stehen unter *http://service.sap.com/diagnostics* zur Verfügung.

Richtlinien zur Arbeit mit dem SMD Agent

Orientieren Sie sich an den folgenden Richtlinien zur Verwendung von SMD Agents für die Überwachung der BI-Plattform.

- Die Installationsreihenfolge des überwachten Systems und des Agents spielt keine Rolle. Sie können den SMD Agent vor oder nach der Installation und Implementierung der BI-Plattform installieren.
- Notieren Sie sich bei der Installation eines SMD Agents den Hostnamen und den Überwachungsport. Diese werden für die Konfiguration der BI-Plattform als überwachtes System unbedingt benötigt. Wenn Sie den Agent vor dem überwachten System installiert haben, können Sie die Konfigurationsinformationen während des BI-Plattform-Installationssetups angeben. Diese Informationen lassen sich auch später über Platzhalter für die Knoten in der Central Management Console der Implementierung bereitstellen.
- Falls die Backend-Server in einem verteilten System bereitgestellt werden, sollten Sie einen SMD Agent auf jedem Rechner installieren, der einen Backend-Server hostet.
- Der SMD Agent ist für die Leistungsintrumentation für Nicht-Java-Server erforderlich.
- Sie müssen das SMAdmin-Benutzerkonto aktivieren, um den SMD-Serverzugriff auf den CMS zu ermöglichen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

26.4.3 SMAdmin-Benutzerkonto

Für jede BI-Plattform-Implementierung wird ein Benutzerkonto für die SMD-Integration erstellt. Mithilfe dieses schreibgeschützten Kontos meldet sich der SMD-Server beim CMS an, um Serverkonfigurationsdaten und andere Informationen über die Implementierung zu erfassen.

Das SMAdmin-Konto wird standardmäßig deaktiviert.

26.4.3.1 Aktivieren des SMAdmin-Kontos

1. Wählen Sie im Verwaltungsbereich *Benutzer und Gruppen* der CMC **Benutzerliste** aus.
   Die Liste der Benutzer wird angezeigt.
2. Suchen Sie das Benutzerkonto *SMAdmin* .
3. Klicken Sie auf **Verwalten** > **Eigenschaften** .
   Das Dialogfeld *Eigenschaften* wird angezeigt.
4. Löschen Sie das Feld **Konto ist deaktiviert**.
5. Klicken Sie auf **Speichern und schließen**.

26.5 Verwalten der Leistungsinstrumentation

26.5.1 Leistungsinstrumentation für die BI-Plattform

Sie können mit CA Wily Introscope als Teil von SAP Solution Manager die BI-Plattform-Leistungsinstrumentation messen. Während der Installation der Plattform werden die folgenden Ressourcen für die Implementierung bereitgestellt

- Introscope-Agent: Introscope-Agents sammeln Leistungsmetriken von BI-Plattform-Java-Backend-Servern. Die Agenten sammeln auch Informationen von der DV-Umgebung. Die Agenten melden diese Metriken dann dem Enterprise Manager.
- Die zur Vereinfachung des Instrumentationsprozesses bereitgestellten Dateien. Ein Satz von Dateien wird für die Instrumentation auf Nicht-Java-Servern bereitgestellt und ein anderer für die Instrumentation auf Java-Servern. SAP Solution Manager setzt die Komponente Enterprise Manager (EM) voraus. EM fungiert als zentrales Repository für alle Introscope-Leistungsdaten und -Metriken, die in einer Anwendungsumgebung erfasst wurden. EM verarbeitet Leistungsdaten und stellt sie Benutzern für die Produktionsüberwachung und -diagnose zur Verfügung.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

26.5.2 Einrichten der Leistungsinstrumentation für die BI-Plattform

Es stehen zwei Möglichkeiten zum Einrichten der Leistungsinstrumentation für Workflows zur Verfügung, die auf BI-Plattform-Backend-Servern ausgeführt werden.

1. Während des Installationssetups für die BI-Plattform. Sie benötigen den Hostnamen und den Überwachungsport für den SMD Agent. Weitere Informationen finden Sie im *Installationshandbuch für SAP BusinessObjects Business Intelligence*. Wenn Sie diese Option auswählen, wird die Instrumentation standardmäßig ausgeführt, sobald Sie die Implementierung des überwachten Systems abgeschlossen haben.
2. Nach der Installation der BI-Plattform können Sie die Konfigurationseinstellungen für den SMD Agent über Platzhalter in den Knoteneigenschaften in der Central Management Console (CMC) bereitstellen.

> **Hinweis**
>
> Für die Instrumentation von Workflows auf Nicht-Java-Servern muss der SMD Agent (`DIAGNOSTICS.AGENT`) installiert sein.

Weitere Informationen

Arbeiten mit SMD Agents [Seite 879]

26.5.2.1 Konfigurieren von Knoten für die Instrumentation

Gehen Sie anhand der folgenden Anweisungen vor, wenn Sie während des Installationssetups der BI-Plattform keine Konfigurationsinformationen für den SMD Agent und Enterprise Manager bereitgestellt haben.

1. Wechseln Sie zum Bereich *Server* der CMC.
2. Klicken Sie im Navigationsbereich auf **Knoten**.
   Alle verfügbaren Knoten werden angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Knoten, auf dem Sie die Instrumentation ausführen möchten, und wählen Sie **Platzhalter** aus.
   Das Dialogfeld "Platzhalter" wird angezeigt.
4. Ändern Sie den Wert für die folgenden Platzhalter.

Platzhalter	Beschreibung
%IntroscopeAgentEnableInstrumentation%	Aktiviert oder deaktiviert die Instrumentation auf Java-Servern. Wird auf "Aktiviert" festgelegt, wenn Sie Konfigurationsdetails für Enterprise Manager während des Installations-Setups angegeben haben. Bei Festlegung auf `true` wird die Instrumentation aktiviert.
%IntroscopeAgentEnterpriseManagerHost%	Hostname des Rechners, auf dem Enterprise Manager installiert ist

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Platzhalter	Beschreibung
%IntroscopeAgentEnterpriseManagerPort%	Der von Enterprise Manager verwendete Überwachungsport
%IntroscopeAgentEnterpriseManagerTransport%	Das von Enterprise Manager verwendete Kommunikationsprotokoll. Zu den unterstützten Protokollen gehören TCP, SSL, HTTP Tunnel und HTTPS.
%NCSInstrumentLevelThreshold%	Wird zum Festlegen der Instrumentationsebene für andere Server als Java-Server verwendet. Wird auf "0" festgelegt, wenn die Instrumentation deaktviert werden soll. Wird auf einen beliebigen Wert über "0" festgelegt, um die Instrumentation zu aktivieren.
%SMDAgentHost%	Der Hostname des Rechners, auf dem der SMD Agent (`DIAGNOSTICS.AGENT`) installiert ist
%SMDAgentPort%	Der vom SMD Agent verwendete Überwachungsport

5. Klicken Sie auf **Speichern und schließen**.
6. Starten Sie den Knoten neu.

Nach dem Neustart des Knotens werden die neu angegebenen Werte an alle verwalteten Server weitergegeben.

26.5.3 Leistungsinstrumentation für die Webschicht

Instrumentationsdaten für Webschichtkomponenten sind nicht in der BI-Plattform enthalten.

26.5.4 Protokolldateien der Instrumentation

Nach der Konfiguration der BI-Plattform-Implementierung zur Ausführung der Instrumentation werden Meldungen an bestimmten Speicherorten protokolliert. Anhand der Protokolldateien können Sie den Instrumentationsstatus überprüfen.

Für die Instrumentation auf Java-Backend-Servern wird eine Protokolldatei in folgendem Verzeichnis gespeichert: `<INSTALLVERZ>/SAP BusinessObjects Enterprise XI 4.0/java/wily/logs` . Für jeden Java-Prozess wird eine separate `.log` -Datei erstellt. Der Ordner enthält auch Dateien vom Typ `AutoProbe.log`, in denen angegeben wird, welche Methoden für die Instrumentation geladen wurden.

Für die Instrumentation auf Nicht-Java-Backend-Servern werden Protokolldateien in folgendem Verzeichnis gespeichert: `<INSTALLVERZ>/SAP BusinessObjects Enterprise XI 4.0/logging/`. Unter Unix befinden sich die Dateien im Verzeichnis `<sap_bobj>\logging\`. Instrumentationsbezogene Protokolldateien für Nicht-Java-Server werden als `.trc`-Dateien gespeichert.

Für die Instrumentation auf Webanwendungsservern wird eine Protokolldatei in folgendem Verzeichnis gespeichert: `<INSTALLVERZ>/SAP BusinessObjects Enterprise XI 4.0/java/wily/webapp/logs`. Zwei Arten von Protokolldateien sind in diesem Ordner enthalten: `Introscope.log` und `Autoprobe.log`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

26.6 Ablaufverfolgung mit SAP Passport

Neben der Ablaufverfolgung für BI-Plattform-Komponenten wie Servern und Webanwendungen kann die Ablaufverfolgung auch für bestimmte Aktionen eingesetzt werden. Bei einer End-to-End-Ablaufverfolgung wird die Leistung einer einzigen Transaktion verfolgt. Die Konsolidierung aller Ablaufverfolgungsinformationen für eine bestimmte Aktion ermöglicht es SAP-Supportmitarbeitern, alle Ablaufverfolgungsdaten einzusehen, ohne durch Ablaufverfolgungsinformationen für andere Aktionen abgelenkt zu werden.

SAP Passport

Der Mechanismus, der die End-to-End-Ablaufverfolgung für die BI-Plattform unterstützt, ist ein Tool namens SAP Passport™. Das SAP Passport-Clienttool fügt einen eindeutigen Identifikator in alle HTTP-Anforderungen eines bestimmten Workflows ein. Dieser Identifikator wird dann an alle Server weitergeleitet, die im Workflow zum Einsatz kommen. Mithilfe dieses eindeutigen Identifikators können SAP-Supportmitarbeiter eine End-to-End-Ablaufverfolgung für den Workflow zusammenstellen.

> **Hinweis**
>
> In der CMC und der Konfigurationsdatei `BO_trace.ini` angegebene Ablaufverfolgungsprotokollierungsebenen werden verwendet, wenn sie höher als die in dem SAP-Passport-Clienttool `SAPClientPlugin.exe` angegebenen Ebenen sind.

Sie finden Passport in den Protokollen für Backend-Server, Webanwendungen und in Webdienstprotokollen.

Das SAP-Passport-Clienttool wird nicht als Teil der BI-Plattform installiert. Um auf das Tool zuzugreifen und es herunterzuladen, wechseln Sie zu *http://service.sap.com/swdc*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

27 Befehlszeilenverwaltung

27.1 Unix-Skripte

Dieser Abschnitt enthält detaillierte Informationen zu den in der Unix-Distribution der BI-Plattform enthaltenen Verwaltungstools und -skripten. Dieser Abschnitt dient in erster Linie zum Nachschlagen. Ausführliche Informationen und Konfigurationsanleitungen finden Sie in den entsprechenden Abschnitten dieses Handbuchs.

Mit den Skripten der Unix-Distribution der BI-Plattform stehen Ihnen alle Konfigurationsoptionen zur Verfügung, die in der Windows-Version von Central Configuration Manager (CCM) verfügbar sind. Darüber hinaus stehen weitere Skripte zur Verfügung, die den Zugriff auf Unix-spezifische Optionen ermöglichen oder als Vorlagen für eigene Skripte verwendet werden können. Einige zusätzliche Skripte sind für die interne Verwendung durch die BI-Plattform bestimmt. Im folgenden werden die einzelnen Skripte mit den jeweiligen Befehlszeilenoptionen beschrieben.

> **Hinweis**
>
> Bei der Eingabe von Unix-Befehlszeilenparametern müssen Sie bestimmte Shell-Sonderzeichen ggf. einfach oder mehrfach maskieren. Wenn z. B. ein Ausrufezeichen (“!”) in einem Kennwort verwendet wird, müssen Sie es ggf. wie folgt maskieren: `./ccm.sh -display -username Administrator -password Abc\!defgh123 -cms cmsname`.

27.1.1 Skripte: Dienstprogramme

In diesem Abschnitt werden die Verwaltungsskripte beschrieben, die Ihnen die Arbeit mit der BI-Plattform unter UNIX erleichtern. Im verbleibenden Teil dieses Abschnitts werden die Konzepte hinter den einzelnen Aufgaben erläutert, die Sie mit diesen Skripten ausführen können. Im vorliegenden Abschnitt finden Sie Informationen zu allen wichtigen Befehlszeilenoptionen und den zugehörigen Argumenten.

27.1.1.1 ccm.sh

Das Skript `ccm.sh` ist im Verzeichnis **`<INSTALLVERZ>`**`/sap_bobj` Ihrer Installation installiert. Mit diesem Skript können Sie die Optionen des Central Configuration Managers über die Befehlszeile steuern. Dieser Abschnitt enthält eine Liste der Befehlszeilenoptionen sowie Beispiele.

> **Hinweis**
>
> Optionale Argumente stehen in eckigen Klammern [ ].

> **Hinweis**
>
> Wenn Sie den Namen eines Server Intelligence Agents nicht genau kennen, informieren Sie sich in den Befehlseigenschaften in der Datei `ccm.config` und verwenden den Wert, der auf die Option `-name` folgt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

> **Hinweis**
>
> Das Skript `ccm.sh` kann nur von dem Benutzer gestartet werden, der die BI-Plattform installiert hat.

- Die **<weiteren Authentifizierungsdaten>**, die bei einigen Argumenten anzugeben sind, werden in der zweiten Tabelle aufgeschlüsselt.

CCM-Option	Gültige Argumente	Beschreibung
`-help`	Nicht zutreffend	Mit dieser Option wird eine Zusammenfassung der Optionen und Argumente für das Skript angezeigt.
`-start`	`all` oder **<sianame>**	Startet jeden Server Intelligence Agent als Prozess. Mit der Option `all` werden alle Knoten auf dem Rechner gestartet, einschließlich Knoten, die zu anderen Clustern gehören.
`-stop`	`all` oder **<sianame>**	Stoppen Sie jeden Server Intelligence Agent über die jeweilige Prozess-ID. Die Option `all` startet alle Knoten des Rechners, einschließlich der zu verschiedenen Clustern gehörigen Knoten.
`-restart`	`all` oder **<sianame>**	Stoppt alle Server Intelligence Agents über die jeweiligen Prozess-IDs. Anschließend werden die einzelnen SIAs gestartet. Mit der Option `all` werden alle Knoten auf dem Rechner gestartet, einschließlich Knoten, die zu anderen Clustern gehören.
`-managedstart`	**<vollständig qualifizierter Servername><[weitere Authentifizierungsdaten]>**	Startet einen Server
`-managedstop`	**<vollständig qualifizierter Servername><[weitere Authentifizierungsdaten]>**	Stoppt einen Server
`-managedrestart`	**<vollständig qualifizierter Servername><[weitere Authentifizierungsdaten]>**	Stoppt einen Server und startet dann den Server

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

CCM-Option	Gültige Argumente	Beschreibung
-managedforceterminate	**<vollständig qualifizierter Servername><[weitere Authentifizierungsdaten]>**	Stoppt den Server unverzüglich, ohne aktuelle Verarbeitungsanforderungen abzuschließen
-enable	**<vollständig qualifizierter Servername><[weitere Authentifizierungsdaten]>**	Aktivieren Sie einen gestarteten Server, sodass er im System registriert wird und die Überwachung des entsprechenden Ports aufnimmt. Verwenden Sie den vollständig qualifizierten Servernamen.
-disable	**<vollständig qualifizierter Servername><[weitere Authentifizierungsdaten]>**	Deaktiviert einen Server, so dass er nicht mehr auf Anforderungen der BI-Plattform reagiert, der Serverprozess jedoch weiterläuft. Verwenden Sie den vollständig qualifizierten Servernamen.
-display	**< [weitere Authentifizierungsdaten]>**	Meldet den aktuellen Status aller Server im Cluster, darunter die Servernamen, die Hostnamen, die Prozess-IDs, die Beschreibungen sowie den Ausführungs- und Aktivierungsstatus

In der folgenden Tabelle werden die Optionen beschrieben, die in dem durch **<[weitere Authentifizierungsdaten]>** gekennzeichneten Argument enthalten sind.

> **Hinweis**
>
> Zur Erhöhung der Sicherheit müssen die Anmeldedaten eines Kontos bei der Enterprise-Authentifizierung immer angegeben werden. Andere Authentifizierungstypen werden nicht unterstützt.

Authentifizierungsoption	Gültige Argumente	Beschreibung
-cms	**<CMS-Name:Portnummer>**	Gibt den CMS an, bei dem Sie sich anmelden möchten. Wenn diese Option nicht angegeben wird, verwendet der CCM standardmäßig den lokalen Rechner und den Anschluss 6400.
-username	**<username>**	Geben Sie ein Konto an, das Administratorrechte für die BI-Plattform hat. Wenn diese Option nicht angegeben wird, wird das standardmäßige Administratorkonto verwendet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Authentifizierungsoption	Gültige Argumente	Beschreibung
-password	<password >	Gibt das Kennwort für das Konto an. Wenn diese Option nicht angegeben wird, wird bei der Anmeldung ein leeres Kennwort verwendet. **Hinweis** Bei Angabe des Arguments –password muss auch das Argument –username angegeben werden.

Der CCM liest aus der Datei ccm.config die Zeichenfolgen zum Starten und weitere Konfigurationswerte.

Weitere Informationen

ccm.config [Seite 888]

27.1.1.1.1 Beispiele

Mit den folgenden zwei Befehlen werden alle BI-Plattform-Server gestartet und aktiviert. Der Central Management Server (CMS) wird auf dem lokalen Rechner mit dem Standardport 6400 gestartet:

```
ccm.sh -start all
ccm.sh -enable all
```

Mit den folgenden zwei Befehlen werden alle BI-Plattform-Server gestartet und aktiviert. Der CCM aktiviert alle Server in dem Cluster, in dem der CMS auf dem Rechner MACHINE01 und dem Port 6701 ausgeführt wird:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701
```

Mit den folgenden zwei Befehlen werden alle BI-Plattform-Server gestartet und aktiviert. Dabei wird das angegebene Administratorkonto SysAdmin und das angegebene Kennwort verwendet:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

Mit diesem einzelnen Befehl wird eine Anmeldung unter dem angegebenen Administratorkonto durchgeführt und anschließend ein Adaptive Job Server deaktiviert, der auf einem zweiten Rechner ausgeführt wird:

```
ccm.sh -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -
password 35%bC5@5
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

27.1.1.1.2 ccm.config

In dieser Konfigurationsdatei werden die Zeichenfolgen zum Starten sowie weitere Werte definiert, die beim Ausführen von CCM-Befehlen verwendet werden. Die Datei wird vom CCM selbst sowie von anderen Skript-Dienstprogrammen der BI-Plattform verwaltet. Änderungen an dieser Datei sind normalerweise nur erforderlich, wenn die Befehlszeile eines Server Intelligence Agent angepasst werden muss. Diese Datei sollte unbedingt gesichert werden, bevor Sie sie manuell bearbeiten.

Weitere Informationen

Überblick über Befehlszeilen [Seite 895]

27.1.1.2 cmsdbsetup.sh

Das Skript `cmsdbsetup.sh` befindet sich im Installationsverzeichnis **`<sap_bobj>`**. Über die Textoberfläche dieses Skripts können Sie die folgenden Aufgaben ausführen.

- Konfigurieren einer CMS-Systemdatenbank
- Neuinitialisieren einer CMS-Systemdatenbank
- Kopieren von Daten aus einer anderen Datenquelle
- Ändern des Clusterschlüssels
- Ändern des Namens des Clusters

> **Hinweis**
>
> Sichern Sie vor Ausführung dieses Skripts die aktuelle CMS-Systemdatenbank und den Inhalt der Input und Output File Repositorys. Weitere Informationen finden Sie im Abschnitt “Sichern und Wiederherstellen Ihres Systems”. Zusätzliche Informationen zu CMS-Clustern und zum Konfigurieren der CMS-Datenbank finden Sie unter "Clustern von Central Management Servern" im Kapitel “Serverwartung” des *Administratorhandbuchs für SAP BusinessObjects Business Intelligence*.

Vom Skript wird der Name des Server Intelligence Agents (SIA) angefordert. Um den Namen des SIA zu prüfen, zeigen Sie die Befehlseigenschaften des SIA in der Datei `ccm.config` an. Der aktuelle Name des SIA wird nach der Option `-name` angezeigt. Alternativ können Sie die Option 8 mit der Datei `serverconfig.sh` verwenden.

Weitere Informationen

Clustern von Central Management Servern [Seite 378]
Übersicht über Sicherung und Wiederherstellung [Seite 487]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

27.1.1.3 serverconfig.sh

Das Skript `serverconfig.sh` befindet sich im Installationsverzeichnis **<sap_bobj>**. Das Skript verfügt über eine Textoberfläche, mit der Sie folgende Operationen durchführen können.

- einen Knoten hinzufügen
- einen Knoten entfernen
- einen Knoten ändern
- einen Knoten verschieben
- die Serverkonfiguration sichern
- die Serverkonfiguration wiederherstellen
- die Webschichtkonfiguration ändern
- alle Knoten auflisten

27.1.1.3.1 Hinzufügen, Löschen, Ändern und Auflisten von Knoten unter UNIX

1. Wechseln Sie in das Verzeichnis **<INSTALLVERZ>**`/sap_bobj` Ihrer Installation.
2. Geben Sie den folgenden Befehl ein:

   ```
   ./serverconfig.sh
   ```

   Die folgenden Optionen werden angezeigt:

   1. einen Knoten hinzufügen
   2. einen Knoten entfernen
   3. einen Knoten ändern
   4. einen Knoten verschieben
   5. die Serverkonfiguration sichern
   6. die Serverkonfiguration wiederherstellen
   7. die Webschichtkonfiguration ändern
   8. alle Knoten auflisten
3. Geben Sie die Nummer des gewünschten Befehls ein.
4. Wenn Sie einen Server hinzufügen, löschen oder ändern, werden weitere Informationen abgefragt. Geben Sie die gewünschten Informationen ein.

27.1.2 Skriptvorlagen

27.1.2.1 startservers

Das Skript `startservers` ist im Verzeichnis **<INSTALLVERZ>**`/sap_bobj` Ihrer Installation installiert. Dieses Skript kann als Vorlage für eigene Skripte verwendet werden: Es dient als Beispiel und veranschaulicht, wie Sie ein eigenes Skript einrichten können, durch das die BI-Plattform-Server gestartet werden, indem eine Reihe von

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

CCM-Befehlen ausgeführt wird. Ausführliche Informationen zum Schreiben von CCM-Befehlen für Server finden Sie unter *ccm.sh* [Seite 884].

27.1.2.2 stopservers

Das Skript `stopservers` ist im Verzeichnis **`<INSTALLVERZ>`**`/sap_bobj` Ihrer Installation installiert. Dieses Skript kann als Vorlage für eigene Skripte verwendet werden: Es dient als Beispiel und veranschaulicht, wie Sie ein eigenes Skript einrichten können, durch das die BI-Plattform-Server gestoppt werden, indem eine Reihe von CCM-Befehlen ausgeführt wird. Ausführliche Informationen zum Schreiben von CCM-Befehlen für Server finden Sie unter *ccm.sh* [Seite 884].

27.1.3 In der BI-Plattform verwendete Skripte

Diese sekundären Skripte werden häufig im Hintergrund ausgeführt, wenn Sie das BI-Plattform-Hauptskript-Dienstprogramm ausführen. Sie müssen sie nicht selbst ausführen.

bobjrestart.sh

Dieses Skript wird intern vom CCM ausgeführt, um Server-Intelligence-Agent-Knoten zu verwalten. Führen Sie dieses Skript nicht selbst aus.

env.sh

Das Skript `env.sh` befindet sich im Installationsverzeichnis **`<sap_bobj/setup>`**. Es konfiguriert die von einigen anderen Skripten benötigten Umgebungsvariablen für die BI-Plattform. BI-Plattform-Skripte führen env.sh wie gewünscht aus. Weitere Einzelheiten finden Sie im *Installationshandbuch für SAP BusinessObjects Business Intelligence*.

env-locale.sh

Das Skript `env-locale.sh` wird für das Konvertieren der Zeichenfolgen der Skriptsprache in unterschiedliche Kodierungen verwendet (z.B. UTF8, EUC oder Shift-JIS). Das Skript wird bei Bedarf durch das Skript `env.sh` ausgeführt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

initlaunch.sh

Das Skript `initlaunch.sh` führt `env.sh` aus, um die BI-Plattform-Umgebungsvariablen einzurichten. Anschließend werden alle Befehle ausgeführt, die Sie ggf. als Befehlszeilenargument für das Skript angegeben haben. Dieses Skript wurde von SAP BusinessObjects hauptsächlich als Fehlerbehebungstool entwickelt.

postinstall.sh

Das Skript `postinstall.sh` befindet sich im Installationsverzeichnis **`<SKRIPTVERZ>`**. Sie sollten dieses Skript nicht selbst ausführen.

setup.sh

Das Skript `setup.sh` befindet sich im Root-Verzeichnis Ihrer Installation. Dieses Skript stellt ein textbasiertes Programm bereit, mit dem Sie die BI-Plattform-Installation konfigurieren können. Es wird bei der Installation der BI-Plattform automatisch ausgeführt. Das Skript fragt die zum erstmaligen Konfigurieren der BI-Plattform benötigten Informationen ab.

Wie Sie genau auf die Eingabeaufforderungen des Setup-Skripts bei der Installation der BI-Plattform reagieren müssen, erfahren Sie im *Business-Intelligence-Installationshandbuch*.

setupinit.sh

Das Skript `setupinit.sh` befindet sich im Installationsverzeichnis **`</sap_bobj/init>`**. Es kopiert die Steuerungsskripte für den automatischen Start in die entsprechenden `rc#`-Verzeichnisse. Wenn die BI-Plattform-Server zusammen mit dem Rechner, auf dem sie installiert sind, gestartet und gestoppt werden sollen, führen Sie dieses Skript aus, nachdem das Skript `setup.sh` beendet wurde.

> **Hinweis**
>
> Zum Ausführen dieses Skripts sind Root-Rechte erforderlich.

27.2 Windows-Skripte

Dieser Abschnitt enthält detaillierte Informationen zu den Verwaltungstools und -skripten auf dem Windows-Datenträger der BI-Plattform. Dieser Abschnitt dient in erster Linie zum Nachschlagen. Ausführliche Informationen und Konfigurationsanleitungen finden Sie in den entsprechenden Abschnitten dieses Handbuchs.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Der Windows-Datenträger der BI-Plattform enthält die Windows-Version des Central Configuration Manager (CCM). Sie können nicht nur mit der Benutzeroberfläche interagieren, sondern auch die ausführbare CCM-Datei mit Optionen für die Serververwaltung über die Befehlszeile ausführen.

27.2.1 ccm.exe

Die ausführbare Datei `ccm.exe` befindet sich im Verzeichnis **`<INSTALLVERZ>`**`\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64` der Installation. Sie können die ausführbare Datei für bestimmte Vorgänge direkt über die Befehlszeile ausführen. Dieser Abschnitt enthält eine Liste der Befehlszeilenoptionen sowie Beispiele.

> **Hinweis**
>
> Vor Verwendung der Befehlszeilenoptionen von `ccm.exe` zur Interaktion mit einem bestimmten Server müssen der Server Intelligence Agent (SIA) und der Central Management Server (CMS) ausgeführt werden.

> **Hinweis**
>
> Optionale Argumente stehen in eckigen Klammern [ ].

> **Hinweis**
>
> Die **`<weiteren Authentifizierungsdaten>`**, die bei einigen Argumenten anzugeben sind, werden in der zweiten Tabelle aufgeschlüsselt.

CCM-Option	Gültige Argumente	Beschreibung
`-help`	Nicht zutreffend	Mit dieser Option wird eine Zusammenfassung der Optionen und Argumente für das Skript angezeigt.
`-managedstart`	`all` oder **`<vollständig qualifizierter Servername> <[andere Authentifizierungsinformationen]>`**	Startet einen Server
`-managedstop`	`all` oder **`<vollständig qualifizierter Servername> <[andere Authentifizierungsinformationen]>`**	Stoppt einen Server
`-managedrestart`	`all` oder **`<vollständig qualifizierter Servername> <[andere Authentifizierungsinformationen]>`**	Stoppt einen Server und startet dann den Server

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

CCM-Option	Gültige Argumente	Beschreibung
-managedforceterminate	all oder **<vollständig qualifizierter Servername> <[andere Authentifizierungsinformationen]>**	Stoppt den Server unverzüglich, ohne aktuelle Verarbeitungsanforderungen abzuschließen
-enable	all oder **<vollständig qualifizierter Servername> <[andere Authentifizierungsinformationen]>**	Aktiviert einen gestarteten Server, sodass er im System registriert wird und die Überwachung des zugewiesenen Ports aufnimmt
-disable	all oder **<vollständig qualifizierter Servername> <[andere Authentifizierungsinformationen]>**	Deaktiviert einen Server, so dass er nicht mehr auf Anforderungen der BI-Plattform reagiert, der Serverprozess jedoch weiterläuft.
-display	**<[weitere Authentifizierungsdaten]>**	Meldet den aktuellen Status aller Server im Cluster, darunter die Servernamen, die Hostnamen, die Prozess-IDs, die Beschreibungen sowie den Ausführungs- und Aktivierungsstatus

In der folgenden Tabelle werden **<weitere Authentifizierungsdaten>** aus der ersten Tabelle aufgeschlüsselt und erläutert.

> **Hinweis**
>
> Die Anmeldedaten eines Kontos müssen bei der Enterprise-Authentifizierung immer angegeben werden.

Authentifizierungsoption	Gültige Argumente	Beschreibung
-cms	**<CMS-Name:Portnummer>**	Gibt den CMS an, bei dem Sie sich anmelden möchten. Wenn diese Option nicht angegeben wird, verwendet der CCM standardmäßig den lokalen Rechner und den Anschluss 6400.
-username	**<Benutzername>**	Geben Sie ein Konto an, das Administratorrechte für die BI-Plattform hat. Wenn diese Option nicht angegeben wird, wird das standardmäßige Administratorkonto verwendet.
-password	**<Kennwort>**	Gibt das Kennwort für das Konto an. Wenn diese Option nicht angegeben wird, wird bei der Anmeldung ein leeres Kennwort verwendet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Authentifizierungsoption	Gültige Argumente	Beschreibung
		Hinweis Bei Angabe des Arguments `-password` muss auch das Argument `-username` angegeben werden.
`-authentication`	**`<Authentifizierungstyp>`**	Gibt den Authentifizierungstyp an. Es wird nur **`secEnterprise`** unterstützt.

Der CCM liest aus der Datei `ccm.config` die Zeichenfolgen zum Starten und weitere Konfigurationswerte.

27.2.1.1 Beispiele

Bei den folgenden Beispielen wird davon ausgegangen, dass ein Server Intelligence Agent (SIA) und ein Central Management Server (CMS) gestartet sind und ausgeführt werden. Vor Verwendung der Befehlszeilenoptionen von `ccm.exe` zur Interaktion mit einzelnen Servern können Sie mithilfe des folgenden Windows-Befehls den SIA-Dienst starten:

```
net start "Server Intelligence Agent (NODENAME)"
```

Der SIA lässt sich auch mit `net stop "Server Intelligence Agent (NODENAME)"` stoppen.

Mit diesem Befehl werden alle BI-Plattform-Server gestartet:

```
ccm.exe -managedstart all
```

Mit diesem Befehl wird ein Adaptive Job Server gestartet. Der CMS wurde mit dem Port 6701 statt des Standardports gestartet:

```
ccm.exe -managedstart MACHINE01.AdaptiveJobServer -cms MACHINE01:6701
```

Mit diesem Befehl wird ein Adaptive Job Server mit einem angegebenen Administratorkonto namens `SysAdmin` gestartet:

```
ccm.exe -enable MACHINE01.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -
password 35%bC5@5
```

Mit diesem Befehl wird eine Anmeldung unter dem angegebenen Administratorkonto durchgeführt und anschließend ein Adaptive Job Server deaktiviert, der auf einem zweiten Rechner ausgeführt wird:

```
ccm.exe -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin
-password 35%bC5@5
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

27.3 Serverbefehlszeilen

27.3.1 Überblick über Befehlszeilen

Dieser Abschnitt enthält eine Liste der Befehlszeilenoptionen für die Steuerung von BI-Plattform-Servern.

Wenn Sie einen Server über die Central Management Console (CMC) starten oder konfigurieren, wird beim Starten (oder Neustarten) des Servers eine standardmäßige Befehlszeile mit vorgegebenen Optionen und Werten verwendet. Änderungen an den standardmäßigen Befehlszeilen sind nur in seltenen Fällen erforderlich. Die meisten gängigen Einstellungen können über die Serverkonfigurationsbereiche der CMC geändert werden. Dieser Abschnitt enthält eine vollständige Liste der von den einzelnen Servern unterstützten Befehlszeilenoptionen. Durch direkte Änderungen an den Serverbefehlszeilen können Sie Anpassungen an der BI-Plattform vornehmen, die über die Optionen der grafischen Benutzeroberfläche hinausgehen.

Optionale Werte sind in diesem Abschnitt durch eckige Klammern [ ] gekennzeichnet.

> **Hinweis**
>
> Die folgende Tabelle enthält eine Aufstellung der unterstützten Befehlszeilenoptionen. BI-Plattform-Server verwenden eine Reihe interner Optionen, die nicht in den Tabellen enthalten sind. Diese internen Optionen dürfen nicht geändert werden.

27.3.1.1 Befehlszeile eines Servers anzeigen und ändern

1. Stoppen Sie den Server mit der Central Management Console (CMC).
2. Klicken Sie mit der rechten Maustaste auf den Server, und wählen Sie **Eigenschaften** aus.
3. Ändern Sie auf dem Bildschirm *Eigenschaften* die Befehlszeile für den Server, und klicken Sie auf **Speichern & schließen**.
4. Starten Sie den Server.

27.3.2 Standardoptionen für alle Server

Sofern nicht anders angegeben, gelten diese Befehlszeilenoptionen gelten für alle Business-Intelligence-Plattform-Server. Informationen zu Optionen, die nur für bestimmte Servertypen gelten, finden Sie im Rest dieses Abschnitts.

Option	Gültige Argumente	Verhalten
`-requestPort`	`<port >`	Gibt die Nummer des vom Server überwachten Anschlusses an. Dieser Port wird vom Server beim CMS registriert. Wenn diese Option nicht

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Gültige Argumente	Verhalten
		angegeben wird, wählt der Server eine freie Portnummer über 1024. **Hinweis** Dieser Port wird von verschiedenen Servern für unterschiedliche Zwecke verwendet. Bevor Sie Änderungen vornehmen, lesen Sie den Abschnitt über das Ändern der Standardportnummern für Server im *Administratorhandbuch für Business Intelligence* durch.
`-loggingPath`	**`<absoluter Pfad>`**	Geben Sie den Pfad an, in dem Protokolldateien erstellt werden.

27.3.2.1 Signalbehandlung unter UNIX

Unter UNIX behandeln die Dämonen der BI-Plattform die folgenden Signale:

- Das Signal `SIGTERM` bewirkt ein normales Herunterfahren des Servers (Rückgabewert beim Beenden: 0).
- `SIGSEGV`, `SIGBUS`, `SIGSYS`, `SIGFPE` und `SIGILL` bewirken ein schnelles Herunterfahren des Servers (Rückgabewert beim Beenden: 1).

27.3.3 Central Management Server

Die in diesem Abschnitt aufgelisteten Befehlszeilenoptionen gelten nur für den CMS. Unter Windows lautet der Standardpfad des Servers **`<INSTALLVERZ>`**`\BusinessObjects Enterprise XI 4.0\win64_x64\CMS.exe`.

Unter UNIX lautet der Standardpfad des Servers **`<INSTALLVERZ>`**`/sap_bobj/enterprise_xi40/`**`<Plattform>`**`/boe_cmsd`.

Option	Gültige Argumente	Verhalten
`-threads`	**`<Zahl>`**	Gibt die Anzahl der vom CMS initialisierten und verwendeten Arbeitsthreads an. Der Wert kann zwischen 12 und 150 liegen und wird standardmäßig auf 50 festgelegt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Gültige Argumente	Verhalten
`-reinitializedb`		Bewirkt, dass der CMS die Systemdatenbank löscht und eine neue Systemdatenbank anlegt, die nur die standardmäßigen Systemobjekte enthält. Alle in der Datenbank enthaltenen Daten gehen bei der Neuerstellung verloren.
`-quit`		Bewirkt, dass der CMS nach dem Verarbeiten der Option `-reinitializedb` beendet wird.
`-receiverPool`	**<Zahl>**	Geben Sie die Anzahl der Threads an, die der CMS für das Empfangen von Clientanforderungen erstellt. Beim Client kann es sich um einen anderen SAP-BusinessObjects-Server, den Publishing-Assistenten für Berichte, Crystal Reports oder um eine von Ihnen erstellte benutzerdefinierte Clientanwendung handeln. Der Standardwert ist 5. Normalerweise müssen Sie diesen Wert nicht erhöhen, es sei denn, Sie möchten eine benutzerdefinierte Anwendung mit vielen Clients erstellen.
`-maxobjectsincache`	**<Zahl>**	Geben Sie die maximale Anzahl von Objekten an, die der CMS im Speichercache speichert. Durch Erhöhen der Anzahl von Objekten wird die Anzahl der erforderlichen Datenbankaufrufe verringert und die Leistung des CMS deutlich verbessert. Wenn jedoch zu viele Objekte im Speicher platziert werden, kann dies dazu führen, dass der Speicher des CMS zum Verarbeiten von Querys nicht mehr ausreicht. Die obere Begrenzung ist 100000.
`-ndbqthreads`	**<Zahl>**	Geben Sie die Anzahl der CMS-Worker-Threads an, die Anforderungen an die Datenbank senden. Für jeden Thread besteht eine Verbindung mit der Datenbank. Achten Sie daher darauf, die Datenbankkapazität

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Gültige Argumente	Verhalten
		nicht zu überschreiten. In den meisten Fällen empfiehlt es sich, als Höchstwert 20 festzulegen.
-oobthreads	**<Zahl>**	Wenn Ihrem Cluster mehr als acht CMS-Clustermitglieder angehören, stellen Sie sicher, dass die Befehlszeile für jeden CMS diese Option enthält. Geben Sie die Anzahl der CMS-Dienste im Cluster an. Diese Option stellt sicher, dass der Cluster hohe Auslastungen bewältigen kann.

Weitere Informationen

Standardoptionen für alle Server [Seite 895]

27.3.4 Crystal Reports Processing Server und Crystal Reports Cache Server

Bei der Steuerung über die Befehlszeile bestehen zwischen Crystal Reports Processing Servern und Crystal Reports Cache Servern nur geringfügige Unterschiede. Durch Befehlszeilenoptionen wird festgelegt, ob der Server als Processing Server und/oder als Cache Server gestartet wird. Wenn eine Option nur für einen der beiden Servertypen gilt, ist dies im Folgenden gesondert vermerkt.

Unter Windows lauten die Standardpfade der Server:

- **<INSTALLVERZ>**\SAP BusinessObjects Business Intelligence platform 4.0 \win64_x64\cacheserver.exe.
- **<INSTALLVERZ>**\BusinessObjects Business Intelligence platform XI 4.0\win64_x64\pageserver.exe.

Unter UNIX lauten die Standardpfade der Server:

- **<INSTALLVERZ>**/sap_bobj/enterprise_xi40/**<PLATTFORM>**/boe_cachesd.
- **<INSTALLVERZ>**/sap_bobj/enterprise_xi40/**<PLATTFORM>**/boe_procd.

Option	Gültige Argumente	Verhalten
-cache		Startet den Server als Cache Server.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Gültige Argumente	Verhalten
-deleteCache		Mit dieser Option wird das Cache-Verzeichnis bei jedem Starten und Anhalten des Servers gelöscht.
-report_ProcessExtPath	**<Absoluter Pfad>**	Gibt das Standardverzeichnis für Verarbeitungserweiterungen an. Einzelheiten finden Sie im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.

Weitere Informationen

Standardoptionen für alle Server [Seite 895]

27.3.5 Dashboards Processing Server und Dashboards Cache Server

Bei der Steuerung über die Befehlszeile bestehen zwischen Dashboards Processing Servern und Dashboards Cache Servern nur geringfügige Unterschiede. Durch Befehlszeilenoptionen wird festgelegt, ob der Server als Processing Server und/oder als Cache Server gestartet wird. Wenn eine Option nur für einen der beiden Servertypen gilt, ist dies im Folgenden gesondert vermerkt.

Unter Windows lauten die Standardpfade der Server:

- **<INSTALLVERZ>**\SAP BusinessObjects\BI platform 4.0\win64_x64\xccache.exe.
- **<INSTALLVERZ>**\SAP BusinessObjects\BI platform 4.0\win64_x64\xcproc.exe.

Unter UNIX lauten die Standardpfade der Server:

- **<INSTALLVERZ>**/sap_bobj/enterprise_xi40/<platform>_64/boe_xccached.
- **<INSTALLVERZ>**/sap_bobj/enterprise_xi40/<platform>_64/xcprocd.

Option	Gültige Argumente	Verhalten
-cache		Startet den Server als Cache Server.
-dir	**<absoluter Pfad>**	Legt bei einem Cache Server das Cache-Verzeichnis und bei einem Processing Server das temporäre Verzeichnis fest. Im angegebenen absoluten Pfad werden die Unter-

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Gültige Argumente	Verhalten
		verzeichnisse `cache` und `temp` angelegt.
`-deleteCache`		Mit dieser Option wird das Cache-Verzeichnis bei jedem Starten und Anhalten des Servers gelöscht.
`-psdir`	**`<absoluter Pfad>`**	Legt das temporäre Verzeichnis des Processing Servers fest. Diese Option hat Vorrang vor der Option `-dir`.
`-refresh`	**`<Minuten>`**	Gibt an (in Minuten), wie lange die im Cache gespeicherten Seiten zur Verfügung stehen.
`-auditMaxEventsPerFile`	**`<Zahl>`**	Gibt auf dem Cache Server die Höchstzahl von Überwachungsaktionen an, die in der Überwachungsprotokolldatei aufgezeichnet werden. Standardwert: 500. Wenn diese maximale Anzahl von Datensätzen überschritten wird, wird auf dem Server eine neue Protokolldatei geöffnet.

Weitere Informationen

Standardoptionen für alle Server [Seite 895]

27.3.6 Job Server

Die in diesem Abschnitt aufgelisteten Befehlszeilenoptionen gelten nur für Adaptive Job Server.

Unter Windows lautet der Standardpfad zum Server **`<INSTALLVERZ>`**`\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\JobServer.exe`.

Unter Unix lautet der Standardpfad zum Server **`<INSTALLVERZ>`**`/sap_bobj/enterprise_xi40/`**`<PLATTFORM>`**`/boe_jobsd`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Gültige Argumente	Verhalten
`-dir`	**`<Absoluter Pfad>`**	Legt das Datenverzeichnis des Job Servers fest.
`-maxJobs`	**`<Zahl>`**	Legt fest, wie viele Aufträge der Server gleichzeitig verarbeitet. Der Standardwert ist fünf.
`-requestJSChildPorts`	**`<UntererGrenzwert-oberer-Grenzwert>`**	Legt den Bereich der Portnummern für untergeordnete Prozesse in Firewallumgebungen fest. Wenn beispielsweise der Wertebereich `6800-6805` zugewiesen wird, stehen maximal sechs Anschlüsse für untergeordnete Prozesse zur Verfügung. **Hinweis** Damit diese Option wirksam wird, muss außerdem die Einstellung `-requestPort` angegeben werden.
`-report_ProcessExtPath`	**`<Absoluter Pfad>`**	Gibt das Standardverzeichnis für Verarbeitungserweiterungen an. Einzelheiten finden Sie im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.

Weitere Informationen

Standardoptionen für alle Server [Seite 895]

27.3.7 Adaptive Processing Server

Der Adaptive Processing Server arbeitet mit Parametern, die für SAP Java Virtual Machine (SAP JVM) definiert wurden. Weitere Informationen finden Sie in der SAP JVM-Dokumentation.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

27.3.8 Report Application Server

Die in diesem Abschnitt aufgelisteten Befehlszeilenoptionen gelten nur für den Report Application Server.

Unter Windows lautet der Standardpfad zum Server **<INSTALLVERZ>**`\SAP BusinessObjects Business Intelligence platform 4.0\win32_x86\crystalras.exe`.

Unter UNIX lautet der Standardpfad zum Server **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/`**<PLATTFORM>**`/ras/boe_crystalrasd`.

Option	Gültige Argumente	Verhalten
`-ipport`	**<Port>**	Angeben der Portnummer für den Empfang von TCP/IP-Anforderungen bei Ausführung im eigenständigen Modus (außerhalb der BI-Plattform).
`-report_ProcessExtPath`	**<Absoluter Pfad>**	Gibt das Standardverzeichnis für Verarbeitungserweiterungen an. Einzelheiten hierzu finden Sie im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.
`-ProcessAffinityMask`	**<Maske>**	Geben Sie mithilfe einer Maske genau an, auf welche Prozessoren der RAS zugreifen soll, wenn er auf einem Rechner mit mehreren Prozessoren ausgeführt wird. Das Maskenformat lautet `0xffffffff`, wobei jedes `f` für einen Prozessor steht und die Prozessoren von rechts nach links aufgeführt sind (das letzte `f` steht also für den ersten Prozessor). Ersetzen Sie jedes `f` entweder durch eine 0 (Prozessorzugriff nicht gestattet) oder eine `1` (Prozessorzugriff gestattet). Wenn der RAS beispielsweise auf einem Rechner mit vier Prozessoren ausgeführt wird und Sie auf den dritten und den vierten Prozessor zugreifen möchten, verwenden Sie die Maske `0x1100`. Für den Zugriff auf den zweiten und den dritten Prozessor verwenden Sie die Maske `0x0110`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Gültige Argumente	Verhalten
		Hinweis Der RAS greift von rechts nach links auf die Prozessoren in der Zeichenfolge zu, bis zu der lizenzgemäß zulässigen maximalen Anzahl der Prozessoren. Wenn Sie über eine Lizenz für zwei Prozessoren verfügen, wirkt sich die Maske `0x1110` in gleicher Weise aus wie die Maske `0x0110`. **Hinweis** Der Standardwert für die Maske lautet `-1`. Dies ist gleichbedeutend mit `0x1111`.

Weitere Informationen

Standardoptionen für alle Server [Seite 895]

27.3.9 Web Intelligence Processing Server

Die in diesem Abschnitt aufgelisteten Befehlszeilenoptionen gelten nur für den Web Intelligence Processing Server.

Unter Windows lautet der Standardpfad zum Server **<INSTALLVERZ>**`\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\WIReportServer.exe`.

Unter UNIX lautet der Standardpfad zum Server **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/`**<PLATTFORM>**`/WIReportServer`.

Option	Gültige Argumente	Verhalten
`-ConnectionTimeout Minutes`	**<Minuten>**	Legt die Anzahl der Minuten bis zum Erreichen des Zeitüberschreitungswertes für den Server fest.
`-MaxConnections`	**<Zahl>**	Legt die maximale Anzahl der gleichzeitigen Verbindungen fest, die der Server jeweils unterstützt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Gültige Argumente	Verhalten
-DocExpressEnable		Ermöglicht das Zwischenspeichern von Web-Intelligence-Dokumenten, während das Dokument angezeigt wird.
-DocExpressRealTime CachingEnable		Ermöglicht das Speichern von Web-Intelligence-Dokumenten im Echtzeit-Cache.
-DocExpressCache DurationMinutes	**<Minuten>**	Legt die Zeitdauer (in Minuten) fest, über die Inhalte im Cache gespeichert werden.
-DocExpressMaxCache SizeKB	**<Kilobyte>**	Legt die Größe des Dokument-Caches fest.
-EnableListOfValues Cache		Ermöglicht die Zwischenspeicherung von Wertelisten pro Benutzersitzung.
-ListOfValuesBatchSize	**<Zahl>**	Legt die maximale Anzahl von Werten fest, die pro Wertelisten-Batch zurückgegeben werden können.
-UniverseMaxCacheSize	**<Zahl>**	Legt die Anzahl der zwischenzuspeichernden Universen fest.
-WIDMaxCacheSize	**<Zahl>**	Legt die maximale Anzahl der Web-Intelligence-Dokumente fest, die im Cache gespeichert werden können.

Weitere Informationen

Standardoptionen für alle Server [Seite 895]

27.3.10 Input und Output File Repository Server

Die in diesem Abschnitt aufgelisteten Befehlszeilenoptionen gelten nur für Input und Output File Repository Server.

Der Standardpfad zu Servern unter Windows lautet **<INSTALLVERZ>**`\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\fileserver.exe`

Der Standardpfad des Programms, das beide Server unter UNIX bereitstellt, lautet **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/`**<PLATTFORM>**`/boe_filesd`. Der Server Intelligence Agent startet standardmäßig eine

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Instanz von `boe_filesd` für den Input File Repository Server sowie eine Instanz für den Output File Repository Server.

Option	Gültige Argumente	Verhalten
`-rootDir`	**`<Absoluter Pfad>`**	Legt das Root-Verzeichnis für verschiedene Unterordner und Dateien fest, die vom Server verwaltet werden. Das hier angegebene Root-Verzeichnis wird allen Pfadangaben für Dateien des File Repository Servers zugrunde gelegt. **Hinweis** Alle Input File Repository Server müssen dasselbe Root-Verzeichnis haben. Dasselbe gilt für alle Output File Repository Server, andernfalls kann es zu inkonsistenten Instanzen kommen. Das Root-Verzeichnis der Input File Repository Server darf nicht dasselbe sein wie das Root-Verzeichnis der Output File Repository Server. Es wird empfohlen, die Root-Verzeichnisse mithilfe eines RAID-Arrays oder einer anderen Hardware-Lösung zu replizieren.
`-tempDir`	**`<Absoluter Pfad>`**	Legen Sie den Speicherort des temporären Verzeichnisses fest, das der FRS zum Übertragen von Dateien verwendet. Verwenden Sie diese Befehlszeilenoption, wenn Sie den Speicherort des temporären FRS-Verzeichnisses steuern möchten, oder wenn der Name des vom FRS erstellten temporären Standardverzeichnisses das Limit für den Dateisystempfad überschreitet (wodurch der FRS nicht gestartet werden kann). **Hinweis** Geben Sie für diese Option kein vorhandenes Verzeichnis an. Das angegebene Verzeichnis wird

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Option	Gültige Argumente	Verhalten
		beim Start des FRS geleert und beim Herunterfahren des FRS entfernt. Wenn Sie ein vorhandenes Verzeichnis verwenden, wird es geleert und entfernt.
-maxidle	**<Minuten>**	Legt fest, nach wie vielen Minuten eine inaktive Sitzung zurückgesetzt wird.

Weitere Informationen

Standardoptionen für alle Server [Seite 895]

27.3.11 Event Server

Die in diesem Abschnitt aufgelisteten Befehlszeilenoptionen gelten nur für den Event Server.

Unter Windows lautet der Standardpfad des Servers **<INSTALLVERZ>**\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\EventServer.exe.

Unter Unix lautet der Standardpfad des Servers **<INSTALLVERZ>**/sap_bobj/enterprise_xi40/**<<Plattform>>**/boe_eventsd

Option	Gültige Argumente	Verhalten
-cleanup	**<Minuten>**	Gibt an (in Minuten), wie oft der Server die Überwachungs-Proxys zurücksetzt. Der Wert gibt die Zeitdauer für ein zweimaliges Zurücksetzen an. Wenn Sie beispielsweise den Wert 10 angeben, werden die Proxys im Abstand von fünf Minuten bereinigt.

Weitere Informationen

Standardoptionen für alle Server [Seite 895]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

28 Repository Diagnostic Tool

28.1 Übersicht über das Repository Diagnostic Tool

Das Repository Diagnostic Tool (RDT) ist ein Befehlszeilentool, mit dem Inkonsistenzen erkannt, diagnostiziert und repariert werden, die zwischen Ihrer CMS-Systemdatenbank (Central Management Server) und dem FRS-Dateispeicher (File Repository Server) sowie in den Metadaten von InfoObjects auftreten können, die in der CMS-Datenbank gespeichert sind.

Während des normalen Betriebs treten in Zusammenhang mit der CMS-Systemdatenbank gewöhnlich keine Inkonsistenzen auf. Inkonsistenzen können jedoch im Verlauf unerwarteter Ereignisse wie Notfallwiederherstellung, Backup-Wiederherstellung und Netzwerkausfällen auftreten. Während dieser Ereignisse kann die CMS-Systemdatenbank beim Ausführen einer Aufgabe unterbrochen werden. Dadurch können Inkonsistenzen in Zusammenhang mit den Objekten in der CMS-Systemdatenbank auftreten.

Das RDT durchsucht die CMS-Systemdatenbank und erkennt Inkonsistenzen in Objekten wie Berichten, Anwendern, Anwendergruppen, Ordnern, Servern, Universen, Universumsverbindungen und anderen Objekten.

Das RDT sucht zwei Arten von Inkonsistenzen.

- Inkonsistenzen zwischen Objekt und Datei

  Solche Inkonsistenzen können zwischen InfoObjects in der CMS-Datenbank und den entsprechenden Dateien in den File Repositorys auftreten. Eine im FRS gespeicherte Datei hat möglicherweise kein entsprechendes Objekt in der CMS-Systemdatenbank.
- Inkonsistenzen in InfoObject-Metadaten

  Hierbei handelt es sich um Inkonsistenzen, die in der Objektdefinition (den Metadaten) eines InfoObjects in der CMS-Datenbank auftreten können. Ein InfoObject kann beispielsweise auf ein anderes InfoObject verweisen, das in der CMS-Datenbank nicht vorhanden ist.

Das RDT führt abhängig von den Parametern, die bei der Ausführung des Tools angegeben wurden, zwei Funktionen aus:

- Es durchsucht die CMS-Systemdatenbank und den FRS-Dateispeicher, erstellt einen Bericht über Inkonsistenzen und gibt eine Protokolldatei im XML-Format mit Vorschlägen zum Beheben der Inkonsistenzen aus.
- Das Tool sucht und repariert die in der CMS-Systemdatenbank sowie im FRS festgestellten Inkonsistenzen und gibt die vorgenommenen Korrekturmaßnahmen in einer Protokolldatei im XML-Format aus.

28.2 Verwenden des Repository Diagnostic Tool

Das Repository Diagnostic Tool (RDT) ist auf allen Rechnern verfügbar, auf denen der Central Configuration Manager (CCM) installiert ist. Dieses Befehlszeilentool erkennt, diagnostiziert und repariert Inkonsistenzen, die zwischen der CMS-Systemdatenbank (Central Management Server) und dem FRS-Dateispeicher (File Repository Server) bzw. in Metadaten von InfoObjects auftreten können.

Es wird empfohlen, die CMS-Datenbank und den FRS-Dateispeicher zu sichern und das RDT unter Verwendung der gesicherten Version auszuführen, während Ihre BI-Plattform-Dienste deaktiviert sind. Wenn dies nicht möglich ist, kann das RDT auf einer aktiven Datenbank ausgeführt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Wenn Sie das RDT auf einer aktiven Datenbank ausführen möchten, sollten Sie Folgendes berücksichtigen:

- Das RDT verwendet während der Ausführung eine Datenbankverbindung.
- Das RDT überprüft die Konsistenz der Datenbank bis zum Zeitpunkt des Beginns seiner Ausführung. Inkonsistenzen, die während der Ausführung des RDT auftreten, werden weder protokolliert noch behoben.
- Der Speicher des Hostrechners, auf dem das RDT ausgeführt wird, sollte über den üblichen, für die Verarbeitung von RDT-Transaktionen empfohlenen Systemempfehlungen liegen:
  - Für eine Datenbank mit maximal 50.000 InfoObjects sollten mindestens 350 MB zusätzlicher Speicher für die Verarbeitung zur Verfügung stehen.
  - Für eine Datenbank mit 50.000 bis 400.000 InfoObjects sollten mindestens 1,7 GB zusätzlicher Speicher zur Verarbeitung zur Verfügung stehen
  - Eine Datenbank mit 400.000 bis 1.000.000 InfoObjects sollte über zusätzlich 4 GB zur Verarbeitung verfügen.
- Das RDT muss nicht von Ihrem CMS-Server ausgeführt werden. Die Ausführung auf einem separaten Rechner kann bei der Reduzierung der Beeinträchtigung der Systemperformance hilfreich sein.
- Das Tool kann kann die Systemperformance bei seiner Ausführung leicht beeinträchtigen.

Der CMS-Dienst ist für die Ausführung des RDTs nicht erforderlich. Das RDT wird direkt gegen die CMS-Datenbank ausgeführt.

28.2.1 Verwenden des Repository Diagnostic Tool

1. Bei Verwendung des Tools auf einem Windows-Computer öffnen Sie ein Befehlsfenster und führen folgenden Befehl aus:

   <INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\reposcan.exe **<Argumente>**, wobei **<Argumente>** der Liste der Parameter entspricht, die Sie angeben möchten.
2. Bei Verwendung des Tools auf einem UNIX-Computer öffnen Sie eine mit "/usr/bin/sh" kompatible Shell und führen folgenden Befehl aus.

   .**<INSTALLVERZ>**/sap_bobj/enterprise_xi40/**<Plattform>**/boe_reposcan.sh **<Argumente>**. Hierbei steht **<Plattform>** entweder für “linux_x64”, “solaris_sparcv9”, “hpux_ia64” oder “aix_rs6000_64”, und bei **<Argumente>** handelt es sich um die Liste der festzulegenden Parameter.

   > **Hinweis**
   >
   > Bei der Eingabe von Unix-Befehlszeilenparametern müssen Sie bestimmte Shell-Sonderzeichen ggf. einfach oder mehrfach maskieren. Wenn Sie z. B. ein Ausrufezeichen (“!”) in einem Kennwort verwenden, müssen Sie es ggf. wie folgt maskieren: `./ccm.sh -display -username Administrator -password Abc\!defgh123 -cms cmsname`.

Das Repository Diagnostic Tool durchsucht Ihr Repository auf Inkonsistenzen. Abhängig von den festgelegten Parametern werden Inkonsistenzen entweder diagnostiziert und protokolliert oder aber repariert und die dazu ausgeführte Korrekturmaßnahme protokolliert.

Die vom Tool ermittelten Inkonsistenzen werden in `Repo_Scan_yyyy_mm_dd_hh_mm_ss.xml` aufgelistet. Wenn Sie die vom Tool gefundenen Diskrepanzen reparieren lassen, wird zusätzlich die Datei `Repo_Repair_jjjj_mm_tt_hh_mm_ss.xml` erstellt. In dieser Datei sind alle Objekte aufgeführt, die repariert werden sowie alle verwaisten Dateien, die gelöscht wurden. Falls es Inkonisistenzen gibt, die nicht repariert werden konnten, werden diese ebenfalls aufgeführt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Der Pfad zu den Protokolldateien kann mit dem Parameter *outputdir* festgelegt werden. Wenn dieser Parameter nicht angegeben wird, lautet das Standardverzeichnis für die Protokolldateien **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\reposcan` unter Windows und `./sap_bobj/enterprise_xi40/reposcan` unter Unix.

> **Hinweis**
>
> Die Anwendung stellt auch eine XLS-Standarddatei bereit, die mit der XML-Datei zum Erstellen einer HTML-Seite verwendet wird. Die XSL-Datei wird unter Windows im Verzeichnis **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\reposcan` gespeichert und unter UNIX im Verzeichnis `/sap_bobj/enterprisexi_40/reposcan`.

Eine Liste der Warnmeldungen und empfohlenen Aktionen, die das RDT bei Erkennung von Inkonsistenzen ausführt, finden Sie unter *Inkonsistenzen in CMS-Metadaten* und *Inkonsistenzen zwischen CMS und FRS*.

Weitere Informationen

Inkonsistenzen in den CMS-Metadaten [Seite 916]
Inkonsistenzen zwischen CMS und FRS [Seite 915]

28.2.2 Parameter für das Repository Diagnostic Tool

Für das RDT können die Parameter in der folgenden Tabelle verwendet werden:

> **Hinweis**
>
> Parameterdateieinträge werden bei der Ausführung von Befehlszeilenargumenten überschrieben.

Tabelle 24: Allgemeine Parameter

Parameter	Optional oder obligatorisch	Beschreibung
dbdriver	Obligatorisch	Der Treibertyp für die Verbindung zur CMS-Datenbank. Zulässige Werte: • `db2databasesubsystem` • `maxdbdatabasesubsystem` • `mysqldatabasesubsystem` • `oracledatabasesubsystem` • `sqlserverdatabasesubsystem` • `sybasedatabasesubsystem` • `sqlanywheredatabasesubsystem`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Optional oder obligatorisch	Beschreibung
connect	Obligatorisch	Die Verbindungsdetails, über die die Kommunikation mit der CMS-Datenbank erfolgt. Beispiel: `-connect "UID=root;PWD=<Kennwort>;DSN=<dsn>;HOSTNAME=<Hostname>;PORT=<Portnummer>"`
dbkey	Obligatorisch	Geben Sie den Clusterschlüssel für Ihre BI-Plattform-Implementierung ein. Wenn Sie den Clusterschlüssel nicht kennen, setzen Sie ihn über die folgenden Schritte zurück: **Hinweis** Wenn sich der Rechner in einem Cluster befindet, müssen diese Schritte für alle Clustermitglieder durchgeführt werden. Sichern Sie CMS-Datenbank und -Dateispeicher, bevor Sie fortfahren. 1. Starten Sie den Central Configuration Manager (CCM). 2. Klicken Sie im CCM mit der rechten Maustaste auf den Server Intelligence Agent (SIA), und wählen Sie **Stop**. Fahren Sie erst mit Schritt 3 fort, wenn der SIA-Status “Gestoppt” entspricht. 3. Klicken Sie mit der rechten Maustaste auf den SIA, und wählen Sie **Eigenschaften**. 4. Klicken Sie auf der Registerkarte "Konfiguration" auf **Ändern** neben *Konfiguration des CMS-Clusterschlüssels*. 5. Eine Warnmeldung wird angezeigt. Klicken Sie auf "Ja", um fortzufahren. 6. Geben Sie im Dialogfeld *Clusterschlüssel ändern* denselben achtstelligen Schlüssel sowohl im Feld *Neuer Clusterschlüssel* als auch im Feld *Neuen Clusterschlüssel bestätigen* ein. **Hinweis** Das RDT wird nicht ausgeführt, wenn der Parameter *dbkey* ausgelassen wird oder der Clusterschlüssel fehlerhaft ist.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Optional oder obligatorisch	Beschreibung
		Hinweis Der im CCM angezeigte Clusterschlüssel ist verschlüsselt und kann nicht im *dbkey*-Parameter verwendet werden. Weitere Informationen zu Clusterschlüsseln finden Sie im Abschnitt "Sichern der BI-Plattform" im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.
inputfrsdir	Obligatorisch	Der Dateipfad für den Input File Repository Server. **Hinweis** Das Benutzerkonto, unter dem Sie angemeldet sind, wird zum Ausführen des Befehlszeilentools verwendet. Dazu ist vollständiger Zugriff auf den Dateispeicherort erforderlich.
outputfrsdir	Obligatorisch	Der Dateipfad für den Output File Repository Server. **Hinweis** Das Benutzerkonto, unter dem Sie angemeldet sind, wird zum Ausführen des Befehlszeilentools verwendet. Dazu ist der vollständige Zugriff auf den Dateispeicherort erforderlich.
outputdir	Optional	Der Dateipfad, unter dem das RDT die Protokolldateien ablegt. Der Standardwert lautet unter Windows `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\reposcan` und unter Unix `./sap_bobj/enterprise_xi40/reposcan`.
count	Optional	Die Anzahl der ungefähren Fehler, die erkannt werden. Auf diese Weise wird eine optimale Leistung gewährleistet. Der obere Wert beträgt 2e31 - 1. Der Wert 0 wird als gesamtes Repository interpretiert. Standardwert: 0.
repair	Optional	Weist das RDT an, alle gefundenen Inkonsistenzen zu reparieren. Das Standardverhalten besteht darin, die gefundenen Inkonsistenzen nur zu melden, aber keine Reparaturen auszuführen. Wenn der Parameter *-repair* in der Be-

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Optional oder obligatorisch	Beschreibung
		fehlszeile vorhanden ist, meldet und repariert das RDT sämtliche Inkonsistenzen. **Achtung** Mit diesem Prozess werden verwaiste Objekte oder Dateien in der Repository-Datenbank gelöscht.
scanfrs	Optional	Gibt an, ob CMS und FRS vom RDT auf Inkonsistenzen durchsucht werden. Zulässige Werte sind `True` und `False`. Der Standardwert lautet `True`.
scancms	Optional	Gibt an, ob der CMS vom RDT auf Inkonsistenzen zwischen InfoObjects durchsucht wird. Zulässige Werte sind `True` und `False`. Der Standardwert lautet `True`.
submitterid	Optional	Gibt die Anwender-ID an, durch die fehlende oder ungültige IDs für zeitgesteuerte Objekte ersetzt werden. Wenn kein Wert angegeben wird, werden ungültige IDs vom RDT nicht ersetzt. Wenn die angegebene Anwender-ID im CMS nicht vorhanden ist, fordert das RDT eine gültige ID an. Dieser Parameter wird nur verwendet, wenn das RDT im Reparaturmodus ausgeführt wird.
startid	Optional	Gibt das Objekt in der CMS-Datenbank an, bei dem der Suchvorgang gestartet wird. Beispiel: Wenn bereits die ersten 500 Objekte im Repository durchsucht wurden, können Sie `-startid=501` verwenden, um einen neuen Suchvorgang beim 501. Objekt zu starten. Der Standardwert lautet `1`.
optionsfile	Optional	Gibt den Dateipfad zu einer Parameterdatei an. Bei der Parameterdatei handelt es sich um eine Textdatei, in der alle Befehlszeilenoptionen mit den dazugehörigen Werten aufgelistet sind. Die Datei sollte einen Parameter pro Zeile enthalten. **Hinweis** Mit dieser Option können Sie alle Parameter wie oben beschrieben in einer Textdatei festlegen. Verwenden

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Optional oder obligatorisch	Beschreibung
		Sie diese Option, um auf die Parameterdatei zu verweisen, ohne die Parameter über die Befehlszeile einzugeben.
syscopy	Optional	Dieser Parameter wird zum Kopieren der Repository-Datenbank verwendet. Das Tool muss für die neu erstellte Kopie ausgeführt werden. Dadurch wird die Kopie aktualisiert, um zu verhindern, dass sie mit den Quellsystemservern geclustert wird. Wenn die Kopie nicht mit dem Quellsystem kommunizieren kann, ist dies nicht erforderlich. Er sollte nur mit den obligatorischen Parametern verwendet und nicht mit anderen optionalen Parametern in dieser Liste kombiniert werden. **Hinweis** Achten Sie darauf, das RDT nicht mit dem Parameter *syscopy* in Ihrem Quellsystem auszuführen.

Folgende Parameter werden verwendet, wenn das Repository Diagnostic Tool auf einem aktiven geclusterten CMS ausgeführt wird.

Tabelle 25: Verwenden des RDTs mit einem geclusterten CMS

Parameter	Optional oder obligatorisch	Beschreibung
requestport	Optional	Die vom RDT für die Kommunikation mit dem CMS verwendete Portnummer. Akzeptiert ganze, positive Zahlen. Das Tool verwendet standardmäßig den Wert des Betriebssystems auf dem Rechner, auf dem das RDT ausgeführt wird.
numericip	Optional	Gibt an, ob das RDT anstelle des Hostnamens die numerische IP-Adresse für die Kommunikation zwischen CMS und dem Rechner verwendet, auf dem das RDT ausgeführt wird. Zulässige Werte sind `True` und `False`. Der Standardwert lautet `False`.
ipv6	Optional	Der ipv6-Name des Rechners, auf dem das RDT ausgeführt wird. Akzeptiert eine Zeichenfolge. Der Standardwert entspricht dem Hostnamen des Rechners, auf dem das RDT ausgeführt wird.
port	Optional	Der ipv4-Name des Rechners, auf dem das RDT ausgeführt wird. Akzeptiert eine Zeichenfolge.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Parameter	Optional oder obligatorisch	Beschreibung
		Der Standardwert entspricht dem Hostnamen des Rechners, auf dem das RDT ausgeführt wird.
threads	Optional	Die Anzahl der zu verwendenden Threads. Akzeptiert ganze, positive Zahlen. Der Standardwert lautet `12`.

Die folgenden Parameter werden verwendet, wenn das RDT für die Kommunikation mit der durchsuchten CMS-Datenbank SSL einsetzt.

Tabelle 26: Verwenden des RDTs mit SSL

Parameter	Optional oder obligatorisch	Beschreibung
protocol	Optional	Gibt an, ob das Tool im SSL-Modus ausgeführt werden soll. Der allein zulässige Wert lautet `ssl`.
ssl_certdir	Optional	Das Verzeichnis mit den SSL-Zertifikaten.
ssl_trustedcertificate	Optional	Der Dateiname des Zertifikats.
ssl_mycertificate	Optional	Der Dateiname des signierten Zertifikats.
ssl_mykey	Optional	Der Name der Datei mit dem privaten SSL-Schlüssel.
ssl_mykey_passphrase	Optional	Der Name der Datei mit dem SSL-Kennsatz.

Beispiel

Im folgenden Beispiel für Windows werden CMS und FRS auf beide Arten von Inkonsistenzen durchsucht, und die gefundenen Inkonsistenzen werden repariert.

```
reposcan.exe
-dbdriver mysqldatabasesubsystem
-connect "
UID=root;PWD=<Kennwort1>;DSN=<meinDsn>;HOSTNAME=<meinHostname>;PORT=<3306>"
-inputfrsdir "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\FileStore\Input"
-outputfrsdir    "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\FileStore\Output"
-dbkey <Cluster-Schlüssel>
-repair
```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Beispiel

Beispiel für Unix:

```
./boe_reposcan.sh
-dbdriver oracledatabasesubsystem
-connect "UID=<bi_admin>;PWD=<Kennwort1>;DSN=<meinDsn>;PORT=<6400>"
-inputfrsdir /apps/frs/bi/frsinput
-outputfrsdir /apps/frs/bi/frsoutput
-dbkey <Cluster-Schlüssel>
```

28.3 Inkonsistenzen zwischen CMS und FRS

In der folgenden Tabelle sind die Inkonsistenzen beschrieben, die zwischen einer CMS-Datenbank (Central Management Server) und den FRS-Servern (File Repository Servern) auftreten können und die vom Repository Diagnostic Tool (RDT) erkannt werden.

- Warnmeldung

  Die Warnmeldung, die in die Erkennungs- und Reparatur-Protokolldatei geschrieben wird.
- Inkonsistenz

  Eine Erläuterung der Inkonsistenz, die das RDT für das Objekt ermittelt hat.
- Vorschlag

  Die Aktion, die das RDT beim Auffinden einer Inkonsistenz ausführen soll. Sie wird in der Erkennungs-Protokolldatei angegeben.
- Aktion

  Die Aktion, die das RDT zum Reparieren einer Inkonsistenz ausführt. Sie wird in der Reparatur-Protokolldatei angegeben.

Warnmeldung	Inkonsistenz	Vorschlag	Aktion
<Objektname> Objekt <Objekttyp> (Objekt-ID: <ID>) verweist auf Dateien, die nicht im FRS vorhanden sind (<Dateiname>)	Obwohl das Objekt in der CMS-Datenbank vorhanden ist, enthält der FRS keine entsprechende Datei.	Dieses Objekt von der Anwendung löschen lassen. Alle Nachfolgerobjekte dieses Objekts werden ebenfalls gelöscht.	Dieses Objekt wurde aus dem Repository gelöscht.
Die Datei <Dateiname> ist in Input oder Output FRS vorhanden, es gibt jedoch kein entsprechendes InfoObject im Repository.	Obwohl die Datei im FRS vorhanden ist, enthält die CMS-Datenbank keine entsprechende Datei.	Zulassen, dass die Anwendung die nicht verknüpfte Datei entfernt.	Keine Aktion ausgeführt.
<Objekttyp> Objekt <Objektname> (Objekt-ID <ID>) hat den Dateinamen <Dateiname>. Die gespeicherte Dateigröße beträgt <Größe> Byte. Dies	Die Größe der Datei entspricht nicht der Größe der InfoObject-Datei.	Zulassen, dass die Anwendung das Objekt mit der korrekten Dateigröße aktualisiert.	Objekt wurde auf die richtige Dateigröße aktualisiert.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Warnmeldung	Inkonsistenz	Vorschlag	Aktion
entspricht nicht der tatsächlichen Dateigröße von **<Größe>** Byte.			
Dieses Verzeichnis enthält keine Dateien.	Der FRS-Ordner ist leer.	Zulassen, dass die Anwendung das Verzeichnis entfernt.	Leerer Ordner wurde entfernt.

28.4 Inkonsistenzen in den CMS-Metadaten

In der folgenden Tabelle werden die Inkonsistenzen beschrieben, die in den Metadaten der in einer CMS-Systemdatenbank (Central Management Server) gespeicherten Objekte auftreten können und die vom Repository Diagnostic Tool (RDT) erkannt werden.

- Warnmeldung

  Die Warnmeldung, die in die Erkennungs- und Reparatur-Protokolldatei geschrieben wird.
- Inkonsistenz

  Eine Erläuterung der Inkonsistenz, die das RDT für das Objekt ermittelt hat.
- Vorschlag

  Die Aktion, die das RDT beim Auffinden einer Inkonsistenz ausführen soll. Sie wird in der Erkennungs-Protokolldatei angegeben.
- Aktion

  Die Aktion, die das RDT zum Reparieren einer Inkonsistenz ausführt. Sie wird in der Reparatur-Protokolldatei angegeben.

Warnmeldung	Inkonsistenz	Vorschlag	Aktion
Das übergeordnete Objekt von **<Objekttyp>** Objekt **<Objektname>** (Objekt-ID = **<ID>**) fehlt (ID des übergeordneten Objekts = **<ID>**).	Die ID des übergeordneten Objekts für das Objekt ist ungültig oder nicht vorhanden.	Zulassen, dass die Anwendung das Objekt in den Ordner "BOE-Reparatur" verschiebt.	Objekt mit untergeordneten Objekten in den Ordner "BOE-Reparatur" verschoben.
Das Eigentümerobjekt von **<Objekttyp>** Objekt **<Objektname>** (Objekt-ID = **<ID>**) fehlt (ID des Eigentümerobjekts = **<ID>**).	Die ID des Eigentümerobjekts für das Objekt ist ungültig oder nicht vorhanden.	Zulassen, dass die Anwendung das Objekt dem Administrator zuweist.	Das Objekt wurde dem Administrator zugewiesen.
Das Absenderobjekt von **<Objekttyp>** Objekt **<Objektname>** (Objekt-ID = **<ID>**) fehlt (ID des Absenderobjekts = **<ID>**).	Die ID des Absenderobjekts für das Objekt ist ungültig oder nicht vorhanden.	Welche Empfehlung vom RDT angezeigt wird, hängt davon ab, ob Sie für den Parameter *-submitterid* einen Wert angegeben haben.	Wenn Sie für den Parameter *-submitterid* einen Wert bereitstellen, wendet das RDT den Wert auf die Absender-ID des Objekts an. Wenn Sie keinen Wert für diesen Parameter angeben,

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Warnmeldung	Inkonsistenz	Vorschlag	Aktion
		• Wenn Sie diesen Parameter angeben, lautet die Empfehlung " Allow the application to update the object with the provided submitter ID". • Wenn Sie diesen Parameter nicht angeben, lautet die Empfehlung " Verarbeiten Sie das Objekt erneut zeitgesteuert, oder ersetzen Sie die ungültige Absender-ID mithilfe der Befehlszeile "-submitterid"."	führt das RDT keine Aktion aus. Wenn Sie das Objekt erneut zeitgesteuert verarbeiten, wendet der CMS eine neue ID an.
Die Eigenschaft von **<Objekttyp>** Objekt '**<Objektname>**' (Objekt-ID = **<ID>**) der letzten erfolgreichen Instanz bezieht sich auf ein fehlendes Objekt (Objekt-ID der letzten erfolgreichen Instanz = **<ID>**).	Die letzte erfolgreiche Instanz des Objekts ist nicht vorhanden oder ungültig.	Zulassen, dass die Anwendung die Eigenschaft erneut berechnet.	Eigenschaft wurde neu berechnet.
Das Kalenderobjekt von **<Objekttyp>** Objekt '**<Objektname>**' (Objekt-ID = **<ID>**) fehlt (ID des Kalenderobjekts = **<ID>**).	Das Objekt verweist auf einen Kalender, der nicht existiert.	Planen Sie das Objekt mit einem vorhandenen Kalender ein. Diese Anwendung kann nicht eingreifen.	Keine Aktion ausgeführt.
Die erforderliche Zeitsteuerungsservergruppe von **<Objekttyp>** Objekt '**<Objektname>**' (Objekt-ID = **<ID>**) fehlt (ID des Servergruppenobjekts = **<ID>**).	Der bevorzugte Server ist nicht vorhanden.	Planen Sie eine erneute zeitgesteuerte Verarbeitung des Objekts mit einer vorhandenen Servergruppe. Diese Anwendung kann nicht eingreifen.	Keine Aktion ausgeführt.
Die Liste ausstehender Ereignisse von **<Objekttyp>** Objekt '**<Objektname>**' (Objekt-ID = **<ID>**) enthält fehlende Objekte (Ereignisobjekt-ID(s) = **<ID>**).	Das oder die Ereignisse, auf die dieses Objekt wartet, sind nicht vorhanden.	Planen Sie eine erneute zeitgesteuerte Verarbeitung des Objekts, bei der das Objekt auf vorhandene Ereignisobjekte warten soll. Diese Anwendung kann nicht eingreifen.	Keine Aktion ausgeführt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Warnmeldung	Inkonsistenz	Vorschlag	Aktion
Die Liste auszulösender Ereignisse von **<Objekttyp>** Objekt '**<Objektname>**' (Objekt-ID = **<ID>**) enthält fehlende Objekte (Ereignisobjekt-ID(s) = **<ID>**).	Dieses Objekt löst ein Ereignis aus, das nicht existiert.	Zulassen, dass die Anwendung fehlende Ereignisse aus der Liste auszulösender Ereignisse des Objekts entfernt.	Die fehlenden Ereignisse wurden aus der Liste auszulösender Ereignisse des Objekts entfernt.
Die Zugriffskontrollliste von **<Objekttyp>** Objekt '**<Objektname>**' (Objekt-ID = **<ID>**) verweist auf fehlenden Prinzipal (ID des Prinzipal-Objekts = **<ID>**).	Verwaister Zugriffskontrolleintrag.	Zulassen, dass die Anwendung den fehlenden Prinzipal aus der Zugriffskontrollliste des Objekts entfernt.	Der fehlende Prinzipal wurde aus der Zugriffskontrollliste des Objekts entfernt.
Die Zugriffskontrollliste von **<Objekttyp>** Objekt '**<Objektname>**' (Objekt-ID = **<ID>**) verweist auf eine fehlende Zugriffsberechtigung (ID des Zugriffsberechtigungs-Objekts = **<ID>**).	Verwaister Zugriffskontrolleintrag.	Zulassen, dass die fehlende Zugriffsberechtigung aus der Zugriffskontrollliste des Objekts entfernt wird.	Die fehlende Zugriffsberechtigung wurde aus der Zugriffskontrollliste des Objekts entfernt.
<Objekttyp> Objekt **<Objektname>** (Objekt-ID = **<ID>**) enthält mehrere Favoriten-Ordner.	Ein bestimmtes Anwenderkonto verfügt über mehrere Favoriten-Ordner.	Zulassen, dass die Anwendung mehrere Ordner in einen einzigen Favoriten-Ordner konsolidiert.	Alle Favoritenordner wurden in einen einzelnen Favoritenordner konsolidiert.
<Objekttyp> Objekt **<Objektname>** (Objekt-ID = **<ID>**) enthält ungültige Eingabedatei-Einträge (**<Dateien>**).	Das Objekt enthält ungültige Einträge in seiner Eingabedateiliste.	Ungültige Einträge des Objekts vom Tool aus der Eingabedatei-Liste entfernen lassen.	Ungültige Einträge wurden aus der Eingabedatei-Liste des Objekts entfernt.
<Objekttyp> Objekt **<Objektname>** (Objekt-ID = **<ID>**) enthält ungültige Ausgabedatei-Einträge (**<Dateien>**).	Das Objekt enthält ungültige Einträge in seiner Ausgabedateiliste.	Ungültige Einträge des Objekts vom Tool aus der Ausgabedatei-Liste entfernen lassen.	Ungültige Einträge wurden aus der Ausgabedatei-Liste des Objekts entfernt.
Die erforderliche Caching-Servergruppe von **<Objekttyp>** Objekt '**<Objektname>**' (Objekt-ID = **<ID>**) fehlt (ID des Servergruppenobjekts = **<ID>**).	Dem Objekt fehlt die erforderliche Caching-Servergruppe.	Planen Sie eine erneute zeitgesteuerte Verarbeitung des Objekts mit einer vorhandenen Servergruppe.	Keine Aktion ausgeführt.
Die erforderliche Verarbeitungsservergruppe von **<Objekttyp>** Objekt '**<Objektname>**' (Objekt-ID = **<ID>**) fehlt (ID des	Dem Objekt fehlt die erforderliche Verarbeitungsservergruppe.	Planen Sie eine erneute zeitgesteuerte Verarbeitung des Objekts mit einer vorhandenen Servergruppe.	Keine Aktion ausgeführt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Warnmeldung	Inkonsistenz	Vorschlag	Aktion
Servergruppenobjekts = **<ID>**).			
Die Profilliste von **<Objekttyp>** Objekt '**<Objektname>**' (Objekt-ID = **<ID>**) enthält fehlende Objekte (Profilobjekt-ID(s) = **<ID>**).	Das Objekt enthält fehlende Objekte in seiner Profilliste.	Aktualisieren Sie Ihre Veröffentlichung mit vorhandenen Profilen. Diese Anwendung kann nicht eingreifen.	Keine Aktion ausgeführt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

29 Anhang "Rechte"

29.1 Informationen über den Anhang zu Berechtigungen

In diesem Anhang mit Informationen zu Rechten werden die meisten Rechte aufgelistet und beschrieben, die im BI-Plattform-System für die verschiedenen Objekte festgelegt werden können. Für Situationen, in denen mehr als ein Recht zum Ausführen einer Aufgabe für ein Objekt erforderlich ist, finden Sie hier außerdem Informationen zu den zusätzlich erforderlichen Rechten sowie zu den Objekten, denen diese Rechte gewährt werden müssen. Weitere Informationen über das Festlegen von Rechten finden Sie im Kapitel *Festlegen von Rechten* im *Administratorhandbuch für SAP BI*.

29.2 Allgemeine Rechte

Die Rechte in diesem Abschnitt beziehen sich auf mehrere Objekttypen. Für viele dieser Rechte gibt es auch entsprechende Eigentümerrechte. Hierbei handelt es sich um Rechte, die nur für den Eigentümer des Objekts gelten, für das Rechte aktiviert werden.

Die folgenden Rechte beziehen sich nur auf Objekte, die zeitgesteuert verarbeitet werden können:

- Das Recht *Ausführung des Berichts zeitsteuern*.
- Das Recht *Zeitgesteuerte Verarbeitung im Namen von anderen Benutzern*.
- Das Recht *Auf Ziele zeitsteuern*.
- Das Recht *Dokumentinstanzen anzeigen*.
- Das Recht *Instanzen löschen*.
- Das Recht *Berichtsinstanzen anhalten und fortsetzen*.
- Das Recht *Instanzen erneut zeitgesteuert verarbeiten*.

Recht	Beschreibung
Objekte anzeigen	Ermöglicht es, Objekte und deren Eigenschaften anzeigen zu lassen. Wenn Ihnen dieses Recht für ein Objekt nicht gewährt wurde, ist das Objekt im BI-Plattform-System ausgeblendet. Hierbei handelt es sich um ein grundlegendes Recht, das für alle Aufgaben erforderlich ist.
Dem Ordner Objekte hinzufügen	Ermöglicht das Hinzufügen von Objekten zu einem Ordner. Dieses Recht bezieht sich auch auf Objekte, die das Verhalten von Ordnern aufweisen, also Posteingänge, den Ordner `Favoriten` oder Objektpakete.
Objekte bearbeiten	Ermöglicht das Bearbeiten von Objektinhalten und der Eigenschaften für Objekte und Ordner.
Rechte von Benutzern für Objekte ändern	Ermöglicht das Ändern der Sicherheitseinstellungen für ein Objekt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
Sicher Rechte ändern, die Benutzer für Objekte haben	Ermöglicht das Gewähren von Rechten oder Zugriffsberechtigungen, die Sie bereits für ein Objekt besitzen, gegenüber anderen Benutzern. Dazu benötigen Sie dieses Recht für den Benutzer und das Objekt selbst. Weitere Informationen zu diesem Recht finden Sie im Kapitel “"Festlegen von Rechten"” im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.
Servergruppen für die Verarbeitung von Aufträgen definieren	Ermöglicht das Festlegen der Servergruppe, die zum Verarbeiten von Objekten verwendet werden soll. Dieses Recht gilt nur für Objekte, für die Verarbeitungsserver angegeben werden können. Um eine Servergruppe anzugeben, benötigen Sie zusätzlich das Recht *Objekte bearbeiten* für das Objekt.
Objekte löschen	Ermöglicht das Löschen von Objekten und deren Instanzen.
Objekte in einen anderen Ordner kopieren	Ermöglicht das Erstellen von Objektkopien in anderen Ordnern des CMS. Zu diesem Zweck benötigen Sie zusätzlich das Recht *Objekte dem Ordner hinzufügen* für den Zielordner. **Hinweis** Beim Kopieren eines Objekts wird die explizite Sicherheit für das Objekt nicht kopiert; das neue Objekt übernimmt Sicherheitseinstellungen vom Zielordner, die explizite Sicherheit muss jedoch neu eingerichtet werden.
Inhalt replizieren	Ermöglicht die Replikation von Objekten auf ein anderes System in einer föderierten Implementierung.
Ausführung des Berichts zeitsteuern	Ermöglicht die zeitgesteuerte Verarbeitung von Objekten.
Zeitgesteuerte Verarbeitung im Namen von anderen Benutzern	Ermöglicht die zeitgesteuerte Verarbeitung von Objekten für andere Benutzer oder Gruppen. Der Benutzer oder die Gruppe, für den bzw. die das Objekt zeitgesteuert verarbeitet wird, wird zum Eigentümer der Objektinstanz. Um ein Objekt für andere Benutzer oder Gruppen zeitgesteuert zu verarbeiten, benötigen Sie zusätzlich folgende Rechte: • Dieses Recht für den Benutzer oder die Gruppe. • Das Recht *Ausführung des Berichts zeitsteuern*.
Auf Ziele zeitgesteuert verarbeiten	Sie können folgende Aktionen ausführen: • Objekte für andere Ziele als den Enterprise-Standardspeicherort zeitgesteuert verarbeiten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
	• Die für die zeitgesteuerte Verarbeitung angegebenen Standardziele ändern. Um das Objekt für Ziele zeitgesteuert zu verarbeiten, benötigen Sie zusätzlich folgende Rechte: • Das Recht *Ausführung des Berichts zeitsteuern* für das Objekt, das zeitgesteuert verarbeitet werden soll. • Das Recht *Objekte dem Ordner hinzufügen* für den Empfängerposteingang (wenn das Ziel der zeitgesteuerten Verarbeitung ein Posteingang sein soll). • Das Recht *Objekte in einen anderen Ordner kopieren* für das Objekt, das zeitgesteuert verarbeitet werden soll (wenn Sie eine Kopie an ein Posteingangsziel anstatt an eine Verknüpfung senden möchten).
Dokumentinstanzen anzeigen	Ermöglicht das Anzeigen von Objektinstanzen. Hierbei handelt es sich um ein grundlegendes Recht, das für alle Aufgaben erforderlich ist, die Sie für Objektinstanzen ausführen.
Instanzen löschen	Ermöglicht lediglich das Löschen von Objektinstanzen. Wenn Sie über das Recht *Objekte löschen* verfügen, ist dieses Recht nicht erforderlich, um Instanzen zu löschen.
Dokumentinstanzen anhalten und fortsetzen	Ermöglicht das Anhalten und Fortsetzen laufender Objektinstanzen.
Instanzen erneut zeitgesteuert verarbeiten	Ermöglicht das erneute zeitgesteuerte Verarbeiten von Objektinstanzen.

Weitere Informationen

Eigentümerrechte [Seite 152]
Welche der beiden Optionen Rechte von Benutzern für Objekte ändern sollte verwendet werden? [Seite 150]

29.3 Rechte für bestimmte Objekttypen

29.3.1 Ordnerrechte

Um die Verwaltung von Rechten zu vereinfachen, wird empfohlen, Rechte für Ordner festzulegen, damit die Sicherheitseinstellungen von deren Inhalt übernommen werden können. Zu den Ordnerrechten gehören:

- Allgemeine Rechte, die für das Ordnerobjekt gelten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Typspezifische Rechte für die Ordnerinhalte (wie das Recht **Berichtsdaten drucken** für Crystal-Reports-Berichte).

Weitere Informationen

Typspezifische Rechte [Seite 131]

29.3.2 Kategorien

Bei den Rechten in diesem Abschnitt handelt es sich um allgemeine Rechte, die im Kontext öffentlicher und persönlicher Kategorien eine spezielle Bedeutung haben.

> **Hinweis**
>
> Objekte in Kategorien übernehmen keine Rechte, die für die Kategorien festgelegt sind.

Recht	Beschreibung
Dem Ordner Objekte hinzufügen	Ermöglicht das Erstellen neuer Kategorien innerhalb von Kategorien. Dieses Recht wird nicht benötigt, um einer Kategorie Objekte hinzuzufügen.
Objekte bearbeiten	Sie können folgende Aktionen ausführen: • Ändern der Eigenschaften von Kategorien • Verschieben der Kategorie als Unterkategorie in eine andere Kategorie • Hinzufügen von Objekten zur Kategorie • Entfernen von Objekten aus der Kategorie Zum Verschieben einer Kategorie als Unterkategorie in eine andere Kategorie benötigen Sie außerdem folgende Rechte: • Das Recht *Objekte löschen* für die ursprüngliche Kategorie. • Das Recht *Objekte dem Ordner hinzufügen* für die Zielkategorie.
Objekte löschen	Ermöglicht das Löschen der Kategorie.

29.3.3 Desktop Intelligence-Dokumente

Die Rechte in diesem Abschnitt beziehen sich ausschließlich auf Desktop-Intelligence-Dokumente.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
Wertelisten verwenden	Ermöglicht den Benutzern die Verwendung von Wertelisten.
Mit dem Objekt verbundene Dateien herunterladen	Ermöglicht den Benutzern das Herunterladen von mit dem Objekt verbundenen Dateien.
Berichtsdaten exportieren	Ermöglicht den Benutzern das Exportieren von Dokumentdaten in Excel-, PDF- und CSV-Formate. Wenn Sie nicht über dieses Recht verfügen, benötigen Sie das Recht *Im CSV-Format speichern*, *Im Excel-Format speichern* oder *Im PDF-Format speichern*; mit diesen Rechten können Dokumente allerdings nur in das angegebene Format exportiert werden.
SQL anzeigen	Ermöglicht Benutzern, die für die Abfrage generierte SQL anzuzeigen.
Berichtsdaten regenerieren	Ermöglicht den Benutzern das Regenerieren von Dokumentdaten.
Werteliste regenerieren	Ermöglicht den Benutzern das Regenerieren von Wertelisten für Eingabeaufforderungen, während sie die Eingabeaufforderung erstellen oder das Dokument anzeigen. Zu diesem Zweck benötigen Sie zusätzlich das Recht *Wertelisten verwenden* für das Dokument.

Dokumentrechte für die Formate PDF, XLS, Rich Text, Text:

Recht	Beschreibung
Dem Ordner Objekte hinzufügen	Ermöglicht Benutzern, einem Ordner Objekte hinzuzufügen. Dieses Recht bezieht sich auch auf Objekte, die das Verhalten von Ordnern aufweisen, also Posteingänge, Favoritenordner oder Objektpakete.
Objekte in einen anderen Ordner kopieren	Ermöglicht Benutzern, Objektkopien in anderen Ordnern auf dem CMS zu erstellen. Zu diesem Zweck benötigen Sie zusätzlich das Recht "Objekte dem Ordner hinzufügen" für den Zielordner.
Instanzen löschen	Ermöglicht den Benutzern das Löschen von Objektinstanzen. Wenn Sie über das Recht "Objekte löschen" verfügen, ist dieses Recht nicht erforderlich, um Instanzen zu löschen.
Objekte löschen	Ermöglicht den Benutzern das Löschen dieser Kategorie.
Objekte bearbeiten	Ermöglicht den Benutzern das Ändern von Kategorieeigenschaften, Verschieben der Kategorie als Unterkategorie in eine andere Kategorie, Hinzufügen von

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
	Objekten zur Kategorie, Entfernen von Objekten aus der Kategorie.
Rechte von Benutzern für Objekte ändern	Ermöglicht Benutzern, ein Recht für einen Benutzer für dieses Objekt zu ändern.
Dokumentinstanzen anhalten und fortsetzen	Ermöglicht den Benutzern das Anhalten oder Fortsetzen von ausgeführten Objektinstanzen.
Inhalt replizieren	Ermöglicht den Benutzern das Replizieren von Objekten in einem anderen System einer föderierten Implementierung.
Instanzen erneut zeitgesteuert verarbeiten	Ermöglicht den Benutzern das zeitgesteuerte Verarbeiten von Objektinstanzen.
Sicher Rechte ändern, die Anwender für Objekte haben	Ermöglicht den Benutzern das Gewähren, Verweigern oder Zurücksetzen der Rechte, die ihnen selbst bereits eingeräumt wurden.
Dokumentinstanzen anzeigen	Ermöglicht den Benutzern das Anzeigen von Objektinstanzen. Hierbei handelt es sich um ein grundlegendes Recht, das für alle Aufgaben erforderlich ist, die Sie für Objektinstanzen ausführen.
Objekte anzeigen	Ermöglicht den Benutzern das Anzeigen der Kategorie und deren Unterkategorien.

29.3.4 Notizen

Mithilfe von Notizen können Benutzer über die Anwendung Discussions Kommentare zu anderen Objekten erstellen. Notizen werden in Diskussionsthreads miteinander verknüpft. Diese Diskussionsthreads werden als untergeordnete Objekte des Objekts betrachtet, das im Mittelpunkt der Diskussion steht. Sie können Rechte auf Objektebene oder auf Ordnerebene festlegen, um die Verwendung von Diskussionsthreads zu steuern.

Die Rechte in diesem Abschnitt beziehen sich ausschließlich auf Notizen.

Recht	Beschreibung
Ermöglicht Diskussionsthreads	Mit diesem Recht können Sie folgende Aktionen ausführen: • Diskussionsthreads starten und beantworten • Notizen zu einem Diskussionsthread einsehen • Eingestellte Notizen ändern oder löschen

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

29.3.5 Crystal-Reports-Berichte

Die Rechte in diesem Abschnitt beziehen sich ausschließlich auf Crystal-Reports-Berichte.

> **Hinweis**
>
> Diese Rechte gelten nur bei Verwendung der Crystal-Reports-Berichte in der BI-Plattform-Umgebung. Wenn Sie Crystal-Reports-Berichte auf Ihren lokalen Datenträger herunterladen, haben diese Rechte keine Auswirkungen. Um dies zu verhindern, können Sie das Recht *Zum Objekt gehörige Dateien herunterladen* für den Crystal-Reports-Bericht verweigern.

Recht	Beschreibung
Berichtsdaten drucken	Ermöglicht das Ausdrucken des Berichts.
Berichtsdaten regenerieren	Ermöglicht das Regenerieren von Berichtsdaten.
Berichtsdaten exportieren	Ermöglicht das Exportieren der Berichtsdaten in ein beliebiges Format, während der Bericht im Crystal Reports Viewer online angezeigt wird. Um Berichtsdaten in das RPT-Format zu exportieren, benötigen Sie zusätzlich das Recht *Zum Objekt gehörige Dateien herunterladen*.
Zum Objekt gehörige Dateien herunterladen	Mit diesem Recht können Sie folgende Aktionen ausführen: • Bericht in das RPT-Format exportieren • Bericht in Crystal Reports Designer öffnen. • Bericht zeitgesteuert an externe Ziele im RPT-Format verarbeiten.

29.3.6 Web-Intelligence-Dokumente

Die Rechte in diesem Abschnitt beziehen sich ausschließlich auf Web-Intelligence-Dokumente.

Recht	Beschreibung
Wertelisten verwenden	Ermöglicht das Verwenden von Wertelisten.
Berichtsdaten exportieren	Ermöglicht das Exportieren von Dokumentdaten in das Excel-, PDF- und CSV-Format. Wenn Sie nicht über dieses Recht verfügen, benötigen Sie das Recht *Im CSV-Format speichern*, *Im Excel-Format speichern* oder *Im PDF-Format speichern*; mit diesen Rechten können Dokumente allerdings nur in das angegebene Format exportiert werden.
Abfrageskript: Anzeige aktivieren (SQL , MDX...)	Ermöglicht das Anzeigen von Abfrageskripten (SQL und MDX).

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
Berichtsdaten regenerieren	Ermöglicht das Regenerieren von Dokumentdaten.
Abfrage bearbeiten	Ermöglicht das Bearbeiten von Abfragen im Dokument.
Werteliste regenerieren	Ermöglicht das Regenerieren von Wertelisten für Eingabeaufforderungen, während Sie die Eingabeaufforderung erstellen oder das Dokument anzeigen lassen. Zu diesem Zweck benötigen Sie zusätzlich das Recht *Wertelisten verwenden* für das Dokument.
Im CSV-Format speichern	Ermöglicht das Exportieren von Dokumenten ausschließlich als CSV-Dateien. Falls Sie bereits das Recht *Berichtsdaten exportieren* für ein Dokument besitzen, benötigen Sie dieses Recht nicht.
Im Excel-Format speichern	Ermöglicht das Exportieren von Dokumenten ausschließlich als Excel-Dateien. Falls Sie bereits das Recht *Berichtsdaten exportieren* für ein Dokument besitzen, benötigen Sie dieses Recht nicht.
Im PDF-Format speichern	Ermöglicht das Exportieren von Dokumenten ausschließlich als PDF-Dateien. Falls Sie bereits das Recht *Berichtsdaten exportieren* für ein Dokument besitzen, benötigen Sie dieses Recht nicht.
Senden an	Ermöglicht das Senden von Dokumenten an die Zeitsteuerung, an einen BI-Plattform-Posteingang oder das Senden als Hyperlink in einer E-Mail. Mit dieser Berechtigung können Benutzer von Web-Intelligence-Rich-Client auch Dokumente als E-Mail-Anhang senden.

29.3.7 Benutzer und Gruppen

Rechte für Benutzer und Gruppen werden genauso wie für andere Objekte in der BI-Plattform-Umgebung festgelegt. Bei den Rechten in diesem Abschnitt handelt es sich um typspezifische Rechte, die sich ausschließlich auf Benutzer- und Gruppenobjekte beziehen, oder um allgemeine Rechte, die im Kontext von Benutzern und Gruppen eine bestimmte Bedeutung haben.

Hinweis

Benutzer und Untergruppen können Rechte von der Gruppenmitgliedschaft übernehmen.

Hinweis

Die Person, die das Benutzerkonto erstellt, wird als Eigentümer des Kontos angesehen. Nachdem das Benutzerkonto erstellt wurde, wird der Benutzer, für den das Konto eingerichtet wurde, jedoch auch als Eigentümer betrachtet.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
Objekte bearbeiten	Sie können folgende Aktionen ausführen: • Eigenschaften für den Benutzer oder die Gruppe bearbeiten • Gruppenmitgliedschaft verwalten Um einen Benutzer oder eine Gruppe einer anderen Gruppe hinzuzufügen, benötigen Sie dieses Recht für den Benutzer oder die Gruppe sowie für die Zielgruppe.
Benutzerkennwort ändern	Sie können folgende Aktionen ausführen: • Ändern Sie das Kennwort für das Benutzerkonto. Zu diesem Zweck benötigen Sie zusätzlich das Recht *Objekte bearbeiten* für das Benutzerkonto. • Ändern Sie das Kennwort für ein anderes Benutzerkonto. Zu diesem Zweck benötigen Sie auch das Recht *Objekte bearbeiten* und *Rechte von Benutzern für Objekte ändern* für das Benutzerkonto. **Hinweis** Die folgenden Einstellungen für Benutzerkennwörter werden von diesem Recht nicht beeinflusst: *Kennwort ist zeitlich unbegrenzt gültig* *Benutzer muss Kennwort bei der nächsten Anmeldung ändern* *Benutzer kann Kennwort nicht ändern* **Hinweis** Dieses Recht gilt nicht für Datenquellen-Anmeldedaten für SAP-BusinessObjects-Universen.
Veröffentlichungen abonnieren	Ermöglicht es, Veröffentlichungen den Benutzer als Empfänger hinzuzufügen.
Zeitgesteuerte Verarbeitung im Namen von anderen Benutzern	Ermöglicht die zeitgesteuerte Verarbeitung von Objekten im Namen des Benutzers, sodass dieser Benutzer zum Eigentümer der Objektinstanz wird. Zu diesem Zweck benötigen Sie zusätzlich das Recht *Zeitgesteuerte Verarbeitung im Namen von anderen Benutzern* für das Objekt.
Benutzerattribute hinzufügen oder bearbeiten	Ermöglicht die Änderung des Werts der E-Mail-Adresse eines Benutzers oder benutzerdefinierter Benutzerattribute. Dieses Recht gilt für Benutzer.
Benutzerattribute hinzufügen oder bearbeiten (Eigentümerrecht)	Ermöglicht dem Eigentümer eines Benutzerobjekts die Änderung des Werts der E-Mail-Adresse eines Benutzers oder benutzerdefinierter Benutzerattribute.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
	Dieses Recht gilt für Benutzer.

29.3.8 Zugriffsberechtigungen

Die Rechte in diesem Abschnitt beziehen sich ausschließlich auf Zugriffsberechtigungen.

Recht	Beschreibung
Zugriffsberechtigung für Sicherheitszuweisung verwenden	Ermöglicht die Zuweisung der Zugriffsberechtigung, wenn der Zugriffskontrollliste für Objekte Prinzipale hinzugefügt werden. Zu diesem Zweck benötigen Sie auch das Recht *Rechte von Benutzern für Objekte ändern* oder *Sicher Rechte ändern, die Benutzer für Objekte haben* für den Prinzipal und das Objekt. Falls das Recht *Sicher Rechte ändern, die Benutzer für Objekte haben* gewährt wurde, muss Ihnen selbst dieselbe Zugriffsberechtigung für das Objekt gewährt worden sein.

Weitere Informationen

Welche der beiden Optionen Rechte von Benutzern für Objekte ändern sollte verwendet werden? [Seite 150]

29.3.9 Universumsrechte (.unv)

Die Rechte in diesem Abschnitt gelten für Universen, die mit dem Universe-Design-Tool erstellt wurden, d.h. für .unv-Universen. Bei den aufgeführten Rechten handelt es sich um typspezifische Rechte, die sich ausschließlich auf Universen beziehen, oder um allgemeine Rechte, die im Kontext von Universen eine bestimmte Bedeutung haben.

> **Hinweis**
>
> Universumsrechte werden nur angewendet, wenn Sie Universen aus der CMS in die Universe-Design-Tool-Anwendung importieren. Wenn das Universum auf einem lokalen Datenträger gespeichert wird, gelten diese Rechte nicht.

Recht	Beschreibung
Dem Ordner Objekte hinzufügen	Ermöglicht das Hinzufügen von Einschränkungssätzen oder Objekten zum Universum. Dazu benötigen Sie zusätzlich das Recht *Zugriffseinschränkungen bearbeiten*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
Objekte anzeigen	Ermöglicht den Zugriff auf und das Anzeigen des Universums.
Objekte bearbeiten	Mit diesem Recht können Sie folgende Aktionen ausführen: • Bearbeiten Sie das Universum in der CMC oder im Universe-Design-Tool. • Universum sperren bzw. die Universumssperre aufheben. Um die Sperrung eines Universums aufzuheben, benötigen Sie zusätzlich das Recht *Sperrung des Universums aufheben* .
Objekte löschen	Ermöglicht das Löschen des Universums.
Objekte übersetzen	Ermöglicht das speichern übersetzter Universumsobjektnamen mit dem Übersetzungsmanagement-Tool. **Hinweis** Sie können auch Übersetzungen speichern, wenn Ihnen das Recht *Objekte bearbeiten* explizit erteilt und das Recht *Objekte übersetzen* nicht explizit verweigert wurde.
Neue Werteliste	Mit diesem Recht können Sie folgende Aktionen ausführen: • Objekten neue Wertelisten zuordnen • Vorhandene Wertelisten bearbeiten **Hinweis** Dieses Recht hindert Sie nicht daran, kaskadierende Wertelisten zu erstellen
Universum drucken	Ermöglicht das Ausdrucken des Universums.
Tabellen- oder Objektwerte anzeigen	Ermöglicht die Anzeige der mit den Tabellen oder Objekten im Universum verbundenen Werte.
Zugriffseinschränkungen bearbeiten	Ermöglicht das Bearbeiten der Zugriffseinschränkungen für das Universum.
Sperrung des Universums aufheben	Sie können folgende Aktionen ausführen: • Sperrung des Universums aufheben, wenn es von einem anderen Benutzer gesperrt wurde. • Das Universum vom CMS exportieren Um die Sperrung eines Universums aufzuheben, benötigen Sie zusätzlich das Recht *Objekte bearbeiten* .

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
Datenzugriff	Ermöglicht das Abrufen von Daten aus dem Universum sowie das Regenerieren von Dokumenten auf der Grundlage des Universums. Zu diesem Zweck benötigen Sie dieses Recht zusätzlich für die Universe-Design-Tool-Anwendung, das Dokument und die Universumsverbindung.
Auf Universum basierende Abfrage erstellen und bearbeiten	Ermöglicht das Erstellen von Dokumenten und Bearbeiten von Abfragen, die auf dem Universum basieren.

29.3.10 Universumsrechte (.unx)

Die Rechte in diesem Abschnitt gelten für Universen, die mit dem Information-Design-Tool erstellt wurden, d.h. für .unx-Universen. Bei den aufgeführten Rechten handelt es sich um typspezifische Rechte, die sich ausschließlich auf Universen beziehen, oder um allgemeine Rechte, die im Kontext von Universen eine bestimmte Bedeutung haben.

> **Hinweis**
>
> Universumsrechte gelten nur für in einem Repository veröffentlichte Universen. Wenn das Universum in einem lokalen Ordner gespeichert wird, gelten diese Rechte nicht.

Recht	Beschreibung
Objekte anzeigen	Ermöglicht den Zugriff auf und das Anzeigen des Universums.
Objekte bearbeiten	Ermöglicht das erneute Veröffentlichen des Universums.
Objekte löschen	Ermöglicht das Löschen des Universums.
Universum abrufen	Ermöglicht das Abrufen eines veröffentlichten Universums und Bearbeiten der zugrunde liegenden Ressourcen (Business-Schicht und Datengrundlage) im Information-Design-Tool. **Hinweis** Außerdem muss Ihnen das Information-Design-Tool-Anwendungsrecht *Universum abrufen* erteilt worden sein.
Sicherheitsprofile bearbeiten	Ermöglicht das Einfügen, Bearbeiten und Löschen von Sicherheitsprofilen für das Universum im Information-Design-Tool-Sicherheitseditor.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
	Hinweis Dieses Recht wird nicht zum Anzeigen von Sicherheitsprofilen oder Ändern der Aggregationsoptionen des Sicherheitsprofils benötigt.
Sicherheitsprofile zuweisen	Ermöglicht das Zuweisen von Sicherheitsprofilen zu Benutzern und Gruppen im Information-Design-Tool-Sicherheitseditor bzw. das Aufheben von Zuweisungen.
Datenzugriff	Ermöglicht das Abrufen von Daten aus dem Universum sowie das Regenerieren von Dokumenten auf der Grundlage des Universums. Im Information-Design-Tool ermöglicht dieses Recht das Anzeigen der Vorschau der Ergebnismenge im Abfrageeditor.
Abfragen auf der Grundlage eines Universums erstellen und bearbeiten	Ermöglicht das Erstellen und Bearbeiten von Abfragen, die auf dem Universum basieren. Im Information-Design-Tool ermöglicht dieses Recht das Öffnen des Abfrageeditors und das Ausführen einer Abfrage im Universum.
Für alle Benutzer speichern	Ermöglicht das Speichern des Universums für alle Benutzer. **Hinweis** Außerdem muss Ihnen das Information-Design-Tool-Anwendungsrecht *Für alle Benutzer speichern* erteilt worden sein.

29.3.11 Zugriffsberechtigungen für Universumsobjekte

Wenn Designer mit dem Universe-Design-Tool ein Universum oder mit dem Information-Design-Tool eine Business-Schicht erstellen, weisen sie jedem Objekt im Universum eine Objektzugriffsberechtigung zu. Die folgenden Objektzugriffsberechtigungen sind verfügbar:

- Öffentlich (Standard)
- Kontrolliert
- Eingeschränkt
- Vertraulich
- Privat

Nachdem das Universum im Repository veröffentlicht wurde, können Sie auf der Grundlage der in der Anwendung zugewiesenen Objektszugriffsberechtigungen Zugriff auf Objekte erteilen. Sie können beispielsweise der Gruppe "Alle" den Zugriff "Öffentlich" erteilen. Dann können Benutzer aus der Gruppe "Alle" die Objekte in dem als "Öffentlich" bezeichneten Universum sehen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Jede Objektszugriffsberechtigung erteilt einen weiter gehenden Zugriff auf Objekte als die vorherige. "Öffentlich" ist die niedrigste Ebene. Prinzipale, denen der Zugriff "Öffentlich" erteilt wurde, können nur als "Öffentlich" bezeichnete Objekte sehen. Prinzipale, denen der Zugriff "Kontrolliert" erteilt wurde, können als "Öffentlich" und als "Kontrolliert" bezeichnete Objekte sehen. "Privat" ist die höchste Ebeneneinstellung und erteilt Prinzipalen Zugriff auf alle Objektszugriffsberechtigungen, d- h. auf alle Objekte im Universum.

> **Hinweis**
>
> Die Sicherheitseinstellungen der Objektzugriffsberechtigungen setzen alle vom Universum evtl. übernommenen Sicherheitseinstellungen außer Kraft.

> **Hinweis**
>
> Bei .unx-Universen werden die Sicherheitseinstellungen der Objektzugriffsberechtigungen mit der vom Sicherheitsprofil definierten Objektsicherheit berücksichtigt. Weitere Informationen über Sicherheitsprofile finden Sie im *Benutzerhandbuch für das Information-Design-Tool*.

Weitere Informationen

Zuweisen von Zugriffsberechtigungen für Universumsobjekte [Seite 933]

29.3.11.1 Zuweisen von Zugriffsberechtigungen für Universumsobjekte

Zum Festlegen der Zugriffsberechtigungssicherheit für Universumsobjekte benötigen Sie das Recht **Rechte von Benutzern für Objekte ändern** für das Universum.

1. Wählen Sie das Universum im Bereich *Universen* des CMS aus.
2. Klicken Sie auf **Aktion** > **Universumssicherheit**.
3. Wählen Sie im Dialogfeld *Universumssicherheit* die Objektzugriffsberechtigung für den Benutzer oder die Gruppe in der Liste **Objektsicherheitsebene** aus.

29.3.12 Verbindungsrechte

Bei den Rechten in diesem Abschnitt handelt es sich um typspezifische Rechte, die sich auf Universumsverbindungen beziehen, oder um allgemeine Rechte, die im Kontext von Universumsverbindungen eine bestimmte Bedeutung haben. Diese Rechte gelten für im Repository veröffentlichte Verbindungen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Relationale Verbindungsrechte

Recht	Beschreibung
Objekte anzeigen	Ermöglicht es, die Verbindung anzeigen zu lassen.
Objekte bearbeiten	Ermöglicht es, die Verbindungsparameter zu bearbeiten.
Verbindung lokal herunterladen	Ermöglicht die Verwendung von auf der Verbindung im Web-Intelligence-Rich-Client erstellten Universen im Offline-Modus. Ermöglicht die Verwendung des lokalen Middleware-Treibers im Information-Design-Tool. Wählen Sie dazu in den Einstellungen des Information-Design-Tool die Option für die lokale Middleware, andernfalls wird die Server-Middleware von Abfragen an die Datenbank verwendet. Dieses Recht wird auch zum Bearbeiten einer gesicherten Verbindung im Information-Design-Tool benötigt.
Objekte löschen	Ermöglicht es, die Verbindung zu löschen.
Objekte in einen anderen Ordner kopieren	Ermöglicht es, die Verbindung von einem Ordner in einen anderen zu kopieren.
Datenzugriff	Ermöglicht das Abrufen von Inhalten aus der in der Verbindung angegebenen Datenbank. Im Information-Design-Tool ermöglicht dieses Recht das Durchsuchen von Tabellendaten von der Verbindung und von Datengrundlage-Editoren. Außerdem können Sie eine Vorschau der Ergebnismenge im Abfragebereich anzeigen.
Verbindung für gespeicherte Prozeduren verwenden	Ermöglicht die Verwendung der gespeicherten Prozeduren in der Datenbank, die für die Universumsverbindung angegeben wurde. **Hinweis** Dieses Recht gilt nur für .unv-Universen.

OLAP-Verbindungsrechte

Recht	Beschreibung
Objekte anzeigen	Ermöglicht es, die Verbindung anzuzeigen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
Objekte bearbeiten	Ermöglicht das bearbeiten der Verbindungsparameter im Information-Design-Tool-Verbindungseditor.
Objekte löschen	Ermöglicht es, die Verbindung zu löschen.
Objekte in einen anderen Ordner kopieren	Ermöglicht es, die Verbindung von einem Ordner in einen anderen zu kopieren.

29.3.13 Anwendungen

29.3.13.1 CMC

Die Rechte in diesem Abschnitt beziehen sich ausschließlich auf die CMC.

Recht	Beschreibung
An der CMC anmelden und dieses Objekt in der CMC anzeigen	Ermöglicht die Anmeldung an der CMC.
Zugriff auf Instanzen-Manager zulassen	Ermöglicht den Zugriff auf den Instanzen-Manager.
Zugriff auf Beziehungsabfrage zulassen	Ermöglicht das Ausführen von Beziehungsabfragen in der CMC.
Zugriff auf Sicherheitsabfrage zulassen	Ermöglicht das Ausführen von Sicherheitsabfragen in der CMC.

29.3.13.2 BI-Launchpad

Die Rechte in diesem Abschnitt beziehen sich ausschließlich auf BI-Launchpad.

Recht	Beschreibung
Organisieren	Sie können folgende Aktionen ausführen: • Objekte verschieben und kopieren • Objekte zum Favoriten-Ordner hinzufügen • Verknüpfungen mit Objekten erstellen
An Business Objects-Posteingang senden	Ermöglicht das Senden von Objekten an BI-Posteingangsempfänger.
An E-Mail-Ziel senden	Ermöglicht das Senden von Objekten an BI-Posteingangsempfänger.
An Dateispeicherort senden	Ermöglicht das Speichern von Objekten an einem Dateispeicherort.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
An FTP-Adresse senden	Ermöglicht das Speichern von Objekten an einem FTP-Speicherort.

29.3.13.2.1 Rechte für Anwendungen für die Zusammenarbeit

Die Rechte in diesem Abschnitt gelten für SAP Jam oder SAP StreamWork, wenn die Anwendung in der BI-Plattform konfiguriert ist.

Recht	Beschreibung
Dokumente kommentieren	Ermöglicht Ihnen, Kommentare zu Dokumenten und Instanzen zu verfassen
Dem Benutzer gehörende Dokumente kommentieren	Ermöglicht Ihnen, Kommentare zu Dokumenten und Instanzen zu verfassen, deren Eigentümer Sie sind
Posts kommentieren	Ermöglicht Ihnen, Kommentare zu Posts zu Dokumenten oder Instanzen zu verfassen
Kommentare zu dem Benutzer gehörenden Dokumenten anzeigen	Ermöglicht Ihnen, Kommentare zu Dokumenten und Instanzen anzuzeigen, deren Eigentümer Sie sind
Kommentare zu Dokumenten anzeigen	Ermöglicht Ihnen, Kommentare zu Dokumenten und Instanzen anzuzeigen
Kommentar anzeigen	Ermöglicht Ihnen, Kommentare zu Posts zu Dokumenten oder Instanzen anzuzeigen

29.3.13.3 BI-Arbeitsbereiche

Die Rechte in diesem Abschnitt beziehen sich ausschließlich auf BI-Arbeitsbereiche.

Recht	Beschreibung
BI-Arbeitsbereiche erstellen und bearbeiten	Die Benutzer können neue BI-Arbeitsbereiche erstellen und vorhandene BI-Arbeitsbereiche bearbeiten.
Module erstellen und bearbeiten	Der Benutzer kann neue Module erstellen und vorhandene Module bearbeiten.
BI-Arbeitsbereiche bearbeiten	Der Benutzer kann vorhandene BI-Arbeitsbereiche bearbeiten. Die Benutzer können keine neuen BI-Arbeitsbereiche erstellen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

29.3.13.4 Desktop Intelligence

Die Rechte in diesem Abschnitt beziehen sich auf SAP BusinessObjects Desktop Intelligence.

Recht	Beschreibung
Verbindungen erstellen und bearbeiten	Ermöglicht Benutzern, eine neue Verbindung zu erstellen oder eine vorhandene Verbindung zu bearbeiten.
Datenprovider-Verwaltung	Ermöglicht Benutzern, eine Abfrage oder das Universum zu ändern, auf dem diese basiert.
Freehand-SQL bearbeiten	Ermöglicht Benutzern, eine Abfrage zu bearbeiten, die Freehand-SQL-Skripte als Datenprovider verwendet. Das Recht *Freehand-SQL verwenden* muss ebenfalls gewährt werden, um diese Aktion auszuführen.
Freehand-SQL verwenden	Ermöglicht Benutzern, eine Abfrage unter Verwendung von Freehand-SQL-Skripten als Datenprovider zu erstellen.
Dokumentliste und Kategorien regenerieren	Ermöglicht Benutzern, die Dokumentliste zu regenerieren, wenn dieses Recht aktiviert ist.
Dokumente an das Repository senden	Ermöglicht Benutzern, ein Dokument im CMS, in den öffentlichen Ordnern oder in ihren persönlichen Ordnern zu veröffentlichen.
Dokumente über Mail senden	Ermöglicht Benutzern, Dokumente per E-Mail aus Desktop Intelligence zu senden.
Dokumente abrufen	Ermöglicht Benutzern, Dokumente aus dem CMS zu importieren.
VBA-Code ausführen	Ermöglicht Benutzern, den VBA-Code auszuführen.
Add-Ins installieren	Ermöglicht Benutzern, VBA-Add-Ins zu installieren bzw. zu deinstallieren.
Alle öffentlichen Kategorien verwalten	Ermöglicht Benutzern, beliebige Dokumente in der Kategorie zu erstellen, zu bearbeiten oder zu löschen.
Meine öffentlichen Kategorien verwalten	Ermöglicht Benutzern, öffentliche Kategorien innerhalb der Desktop-Intelligence-Anwendung zu erstellen, zu bearbeiten oder zu löschen.
Analysetiefe bearbeiten	Ermöglicht Benutzern, den Analyseumfang zu bearbeiten
Im Drill-Modus arbeiten	Ermöglicht Benutzern, auf einen Drilldown auf eine tiefere Analyseebene in Berichten auszuführen.
Slice-and-Dice-Modus aktivieren	Ermöglicht Benutzern, den Slice-and-Dice-Bereich zu verwenden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
VBA-Code bearbeiten	Ermöglicht Benutzern, in Berichten verwendete VBA-Makros zu bearbeiten.
Euro-Umrechnung	Ermöglicht Benutzern, Währungszahlen in Berichten in und von Euro umzurechnen.
In Zwischenablage kopieren	Ermöglicht Benutzern, Dokumentinhalte auszuschneiden oder zu kopieren.
Drill-Through	Ermöglicht Benutzern, durch Abrufen neuer Daten einen Drilldown auf eine tiefere Ebene in einem Bericht auszuführen.
Euro-Umrechnungskurs bearbeiten	Ermöglicht Benutzern, die von der Euro-Umrechnungsfunktion verwendeten Euro-Umrechnungskurse zu ändern.
Interaktionen zwischen Desktop-Intelligence-Berichten	Ermöglicht Benutzern, einzelne Elemente eines Berichts zum Ausschneiden, Kopieren, Bereinigen, Duplizieren oder Löschen auszuwählen.
Interaktionen zwischen Desktop-Intelligence-Dokumenten	Ermöglicht Benutzern das Umbenennen, Duplizieren, Einfügen oder Löschen eines Berichts in einem Dokument.
Dokumente drucken	Ermöglicht Benutzern, Dokumente zu drucken.
Desktop-Intelligence-Content regenerieren	Ermöglicht Benutzern, Desktop-Intelligence-Dokumente zu regenerieren.
Vorlagen verwenden	Ermöglicht Benutzern, Berichte mit Vorlagen zu erstellen oder Vorlagen auf vorhandene Inhalte anzuwenden.
Vorlagen erstellen	Ermöglicht Benutzern, Dokumente als Vorlagen zu speichern.
Dokumente für alle Benutzer speichern	Ermöglicht Benutzern, Dokumente ohne Sicherheitsbeschränkungen zur Offline-Verwendung zu speichern, damit alle Benutzer dieses Dokument lokal gespeichert anzeigen können.
Desktop-Intelligence-Dokumente erstellen	Ermöglicht Benutzern, ein neues Dokument zu erstellen.
Desktop-Intelligence-Dokumente speichern	Ermöglicht Benutzern, Dokumente lokal zu speichern.
Dokumente an Posteingang senden	Ermöglicht Benutzern, Dokumente an BI-Launchpad-Posteingänge zu senden.
Benutzerobjekte verwenden	Ermöglicht Benutzern, Benutzerobjekte zu erstellen, zu bearbeiten oder zu löschen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
Werteliste regenerieren	Ermöglicht Benutzern, Wertelisten zu regenerieren, wenn dieses Recht erteilt wurde.
Werteliste verwenden	Ermöglicht Benutzern, Wertelisten im Dokument zu verwenden und zu regenerieren.
Werteliste bearbeiten	Ermöglicht Benutzern, in einem Universum definierte Wertelisten zu bearbeiten.
Abfragen verwenden	Ermöglicht Benutzern, neue Abfragen basierend auf einem Universum zu erstellen.
Abfragen bearbeiten	Ermöglicht Benutzern, Abfragen basierend auf einem Universum zu bearbeiten.
SQL anzeigen	Ermöglicht Benutzern, die für die Abfrage generierte SQL anzuzeigen.
Abfrage bearbeiten	Ermöglicht Benutzern, die SQL von Abfragen zu bearbeiten.
SQL immer neu generieren	Ermöglicht, Abfragen bei jeder Regenerierung neu zu generieren.
Gespeicherte Prozeduren verwenden	Ermöglicht Benutzern, einen Bericht anhand einer gespeicherten Prozedur als Datenprovider zu erstellen.
Gespeicherte Prozeduren bearbeiten	Ermöglicht Benutzern, Parameter von gespeicherten Prozeduren zu bearbeiten.
Persönliche Dateien verwenden	Ermöglicht Benutzern, einen Bericht mit Excel-, dBase- oder ASCII-Textdateien als Datenprovider zu erstellen.
Persönliche Dateien bearbeiten	Ermöglicht Benutzern, den persönlichen Datenprovider zu bearbeiten.
Sicher Rechte ändern, die Benutzer für Objekte haben	Ermöglicht Benutzern, Berechtigungen zu gewähren, zu verweigern oder zurückzusetzen, die ihm selbst bereits eingeräumt wurden.
Benutzerrechte für dieses Objekt ändern	Ermöglicht Benutzern, ein Recht für einen Benutzer für dieses Objekt zu ändern.
Dieses Objekt bearbeiten	Ermöglicht Benutzern, die Eigenschaften der Anwendung in der CMC zu ändern.
Bei Desktop Intelligence anmelden und dieses Objekt in der CMC anzeigen	Ermöglicht Benutzern, sich an Desktop Intelligence anzumelden und das Objekt in der CMC anzuzeigen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

29.3.13.5 Web Intelligence

Die Rechte in diesem Abschnitt beziehen sich ausschließlich auf SAP BusinessObjects Web Intelligence (einschließlich der Rich-Client-Schnittstelle) und können sich auf Viewer und Abfrageeditoren in diesen Anwendungen auswirken.

Recht	Beschreibung
Daten: Datentracking aktivieren	Ermöglicht die Verfolgung geänderter Daten.
Daten: Formatierung geänderter Daten aktivieren	Ermöglicht die Wahl von Formaten für geänderte Daten.
Desktop-Schnittstelle – Web Intelligence Desktop aktivieren	Ermöglicht die Verwendung der Desktop-Schnittstelle.
Desktop-Schnittstelle: Dokumente exportieren	Ermöglicht den Export von Dokumenten in den CMS in der Desktop-Schnittstelle.
Desktop-Schnittstelle: Dokumente importieren	Ermöglicht den Import von Dokumenten vom CMS in der Desktop-Schnittstelle.
Desktop-Schnittstelle: Von BI-Launchpad installieren	Ermöglicht das Herunterladen der Desktop-Schnittstelle aus dem BI-Launchpad.
Desktop-Schnittstelle: Dokumente drucken	Ermöglicht das Drucken von Dokumenten von der Desktop-Schnittstelle.
Desktop-Schnittstelle: Dokumentsicherheit entfernen	Ermöglicht das Entfernen der Dokumentsicherheit von der Desktop-Schnittstelle.
Desktop-Schnittstelle: Dokumente für alle Benutzer speichern	Ermöglicht das Speichern von Dokumenten für alle Benutzer von der Desktop-Schnittstelle.
Desktop-Schnittstelle: Dokumente lokal speichern	Ermöglicht den Speichern von Dokumenten auf der lokalen Festplatte in der Desktop-Schnittstelle.
Desktop-Schnittstelle: Per E-Mail senden	Ermöglicht den E-Mail-Versand von Dokumenten in der Desktop-Schnittstelle.
Desktop-Schnittstelle: Lokale Datenprovider aktivieren	Ermöglicht die Verwendung von persönlichen Datenprovidern in der Desktop-Schnittstelle.
Dokumente: Automatische Regenerierung beim Öffnen deaktivieren	Verhindert die automatische Regenerierung von Dokumenten, wenn diese geöffnet werden.
Dokumente: Automatische Speicherung aktivieren	Ermöglicht das automatische Speichern von Dokumenten (wenn das automatische Speichern in der CMC vom Administrator aktiviert wurde).
Dokumente: Erstellung aktivieren	Ermöglicht die Erstellung neuer Dokumente.
Dokumente: Veröffentlichung und Inhaltsverwaltung aktivieren	Ermöglicht die Veröffentlichung von Dokumenten im CMS.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
Interaktiv: Berichterstellung – Alerter erstellen und bearbeiten	Ermöglicht die Erstellung und Bearbeitung von Alertern im interaktiven Viewer.
Schnittstellen: Rich Internet Application aktivieren	Ermöglicht die Verwendung der Anzeige- und Bearbeitungsschnittstelle Rich Internet Application (Javas-Berichteditor in früheren Versionen).
Schnittstellen: Webanzeige-Schnittstelle aktivieren	Ermöglicht die Verwendung der Webanzeige-Schnittstelle (DHTML-Viewer in früheren Versionen).
Schnittstellen: Webabfrageeditor aktivieren	Ermöglicht die Verwendung des Web-Abfrageeditors (Abfrage – HTML in früheren Versionen).
Allgemein: "Meine Einstellungen" bearbeiten	Ermöglicht die Bearbeitung von Einstellungen im BI-Launchpad.
Allgemein: Kontextmenüs aktivieren	Ermöglicht die Verwendung von Kontextmenüs.
Linker Bereich: Dokumentübersicht aktivieren	Ermöglicht die Anzeige der Dokumentübersicht im linken Bereich.
Linker Bereich: Dokumentstruktur und Filter aktivieren	Ermöglicht die Anzeige der Dokumentstruktur im linken Bereich.
Abfrageskript: Bearbeitung aktivieren (SQL, MDX...)	Ermöglicht die Bearbeitung von Abfrageskripten (SQL und MDX).
Abfrageskript: Anzeige aktivieren (SQL, MDX...)	Ermöglicht die Anzeige von Abfrageskripten (SQL und MDX).
Berichterstellung: Umbruchszeichen erstellen und bearbeiten	Ermöglicht die Erstellung und Bearbeitung von Umbruchszeichen.
Berichterstellung: Regeln zur bedingten Formatierung erstellen und bearbeiten	Ermöglicht die Erstellung und Bearbeitung von Regeln zur bedingten Formatierung.
Berichtstellung: Vordefinierte Berechnungen erstellen und bearbeiten	Ermöglicht die Erstellung und Bearbeitung von vordefinierten Berechnungen.
Berichterstellung: Eingabesteuerelemente erstellen und bearbeiten	Ermöglicht die Erstellung und Bearbeitung von Eingabesteuerelementen.
Berichterstellung: Berichtsfilter erstellen und bearbeiten sowie Eingabesteuerelemente nutzen	Ermöglicht die Erstellung und Bearbeitung von Berichtsfiltern und Eingabesteuerelementen. (Eingabesteuerelementbereich im linken Bereich wird nicht angezeigt, wenn deaktiviert.)
Berichterstellung: Sortierungen erstellen und bearbeiten	Ermöglicht die Erstellung und Bearbeitung von Sortierungen.
Berichterstellung: Formeln und Variablen erstellen	Ermöglicht die Erstellung von Formeln und Variablen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
Berichterstellung: Formatierung aktivieren	Ermöglicht die Bearbeitung der Berichtsformatierung. Wenn dieses Recht verweigert wird, sollten der Entwurfsmodus und der Datenmodus nicht für den Benutzer verfügbar sein (deaktiviert).
Berichterstellung: Zusammengeführte Dimensionen aktivieren	Ermöglicht die Datensynchronisierung mithilfe von zusammengeführten Dimensionen in Berichten und im Datenmanager.
Berichterstellung: Berichte, Tabellen, Diagramme und Zellen einfügen und entfernen	Ermöglicht das Einfügen und Entfernen von Berichten, Tabellen, Diagrammen und Zellen. Bestimmt auch den Duplikate-Workflow (Kopieren/Einfügen).

29.3.13.6 Strategy Builder

Strategy Builder ist ein Tool, das mit Performance Management eingesetzt wird. Die Rechte in diesem Abschnitt beziehen sich ausschließlich auf Strategy Builder und können das Zielmanagement in Performance Manager bzw. bestimmte Funktionen in Strategy Builder beeinflussen.

Recht	Beschreibung
Ziele erstellen, ändern oder löschen	Ermöglicht das Hinzufügen, Bearbeiten oder Entfernen von Zielen in Performance Manager.
Ziele anzeigen	Ermöglicht die Anzeige von Zielen in Analysen, die Ziele enthalten.
Zugriff auf Zielmanagement	Ermöglicht das Anzeigen von Zielen auf der Seite *Ziel-Management* in Performance Manager.
Ziele veröffentlichen	Ermöglicht das Veröffentlichen von Zielen in Performance Manager.
Zugriff auf Strategy Builder	Ermöglicht den Zugriff auf das Strategy Builder-Tool in Performance Manager.
Rollen erstellen, ändern oder löschen	Ermöglicht das Verwalten der Rollen, die zum Veröffentlichen von Zielen oder Metriken für bestimmte Zielgruppen in Strategy Builder verwendet werden.
Strategien erstellen, ändern oder löschen	Ermöglicht das Erstellen von Strategien, mit deren Hilfe Rollen verknüpft sowie Ziele und Metriken in Strategy Builder veröffentlicht werden.

29.3.13.7 Universe-Design-Tool-Rechte

Die Rechte in diesem Abschnitt gelten für die Anwendung Universe-Design-Tool.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
Universumintegrität überprüfen	Ermöglicht die Überprüfung der Universumintegrität.
Strukturfenster regenerieren	Ermöglicht das Regenerieren des Strukturfensters.
Tabellenliste verwenden	Ermöglicht es, Datenbankdaten unter Verwendung der Tabellenliste anzeigen zu lassen.
Universumseinschränkungen anwenden	Ermöglicht es Ihnen, vordefinierte Universumseinschränkungen auf Benutzer eines importierten Universums anzuwenden.
Universum verknüpfen	Ermöglicht die Verknüpfung von zwei Universen und das gemeinsame Nutzen der Komponenten.
Verbindungen erstellen, ändern oder löschen	Ermöglicht Ihnen das Erstellen, Ändern und Löschen von Universumsverbindungen, die im Repository oder als persönliche bzw. freigegebene Verbindungen gespeichert sind.

29.3.13.8 Information-Design-Tool-Rechte

Die Rechte in diesem Abschnitt gelten für die Anwendung Information-Design-Tool.

Recht	Beschreibung
Sicherheitsprofile verwalten	Ermöglicht das Öffnen des Sicherheitseditors. **Hinweis** Zum Arbeiten mit Sicherheitsprofilen müssen Ihnen Rechte für das Universum erteilt werden.
Projekte freigeben	Ermöglicht die Freigabe eines lokalen Projekts und das Öffnen der Ansicht "Projekt synchronisieren", um ein freigegebenes Projekt mit dem lokalen Projekt zu synchronisieren.
Verbindungen erstellen, ändern oder löschen	Sie können folgende Aktionen ausführen: • Gesicherte Verbindungen über die Ansicht "Veröffentlichte Ressourcen" erstellen und löschen • Verbindungen im Verbindungseditor bearbeiten • Verbindungen in einem Repository veröffentlichen
Universum veröffentlichen	Ermöglicht das Veröffentlichen von Universen in einem Repository.
Universum abrufen	Ermöglicht das Abrufen von veröffentlichten Universen in einem zu bearbeitenden lokalen Projekt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
Für alle Benutzer speichern	Ermöglicht die Verwendung der Option "Für alle Benutzer speichern" beim Abrufen von Universen.
Statistik berechnen	Ermöglicht die Auswahl von Tabellen und Spalten für die Berechnung und Veröffentlichung von Statistiken.

29.3.13.9 Widgets für die BI-Plattform

Die Rechte in diesem Abschnitt gelten nur für Widgets von SAP BusinessObjects Business Intelligence.

Recht	Beschreibung
Explorer verwenden	Die Benutzer können mit dem Dokumentlisten-Explorer den Inhalt aller verbundenen BI-Plattform-Server durchsuchen.
Warnungseingangsbox verwenden	(Veraltet) Ermöglicht die Verwendung der Warnungsposteingangs
Suche verwenden	Die Benutzer können mit der Inhaltssuche alle verbundenen BI-Plattform-Repositorys auf einmal durchsuchen.

29.3.13.10 Warnmeldungen

Die Rechte in diesem Abschnitt beziehen sich ausschließlich auf die Warnmeldungen.

Recht	Beschreibung
"Warnmeldungen auslösen"	Ermöglicht Ihnen das Auslösen von Warnungsereignissen Um eine Warnmeldung für ein Dokument auszulösen, benötigen Sie folgende Rechte: • Die Rechte "Anzeigen" und "Zeitgesteuert verarbeiten" für das Dokument • Die Rechte "Anzeigen" und "Auslösen" für das betreffende Ereignis
"Objekte abonnieren"	Ermöglicht Ihnen das Abonnieren von Warnungsereignissen Um ein Ereignis zu abonnieren, benötigen Sie folgende Rechte: • Das Recht "Anzeigen" für das betreffende Ereignis • Das Recht "Abonnieren" für das eigene Konto des Benutzers Um eine Warnmeldung in einem Dokument zu abonnieren, benötigen Sie folgende Rechte:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
	• Das Recht "Anzeigen" für das Dokument • Das Recht "Instanz anzeigen" für das Dokument • Das Recht "Anzeigen" für das betreffende Ereignis • Das Recht "Abonnieren" für das eigene Konto des Benutzers

29.3.13.11Explorer-Sortierung

Die Rechte in diesem Abschnitt beziehen sich ausschließlich auf Explorer.

Recht	Beschreibung
Bei Explorer anmelden und dieses Objekt in der CMC anzeigen	Ermöglicht die Anmeldung bei Explorer. Sie benötigen dieses Recht, um andere Aufgaben mit Explorer auszuführen.
Information-Spaces analysieren	Ermöglicht das Analysieren eines Information-Spaces. Zur Ausführung dieser Aufgabe müssen Sie außerdem über das Recht *Bei Explorer anmelden und dieses Objekt in der CMC anzeigen* verfügen.
Information-Spaces analysieren: In Lesezeichen/E-Mail exportieren	Ermöglicht das Hinzufügen und Senden von Lesezeichen per E-Mail. Um diese Aufgabe auszuführen, benötigen Sie die folgenden Rechte: • *Bei Explorer anmelden und dieses Objekt in der CMC anzeigen* • *Information-Spaces analysieren*
Information-Spaces analysieren: Nach CSV exportieren	Ermöglicht den Export einer Exploration in eine CSV- oder Excel-Datei. Um diese Aufgabe auszuführen, benötigen Sie die folgenden Rechte: • *Bei Explorer anmelden und dieses Objekt in der CMC anzeigen* • *Information-Spaces analysieren*
Information-Spaces analysieren: In Bild exportieren	Die Ergebnisse einer Untersuchung können als Bild exportiert werden. Um diese Aufgabe auszuführen, benötigen Sie die folgenden Rechte: • *Bei Explorer anmelden und dieses Objekt in der CMC anzeigen* • *Information-Spaces analysieren*

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
Information-Spaces analysieren: Nach Web Intelligence exportieren	Ermöglicht es, die Ergebnisse einer Untersuchung als Abfrage zu exportieren. Um diese Aufgabe auszuführen, benötigen Sie die folgenden Rechte: • *Bei Explorer anmelden und dieses Objekt in der CMC anzeigen* • *Information-Spaces analysieren*
Information-Spaces verwalten	Ermöglicht es, auf das Menü "Manage Spaces" (Spaces verwalten) zuzugreifen und die zugewiesenen Aufgaben auszuführen. Zur Ausführung dieser Aufgabe müssen Sie außerdem über das Recht *Bei Explorer anmelden und dieses Objekt in der CMC anzeigen* verfügen.
Information-Spaces verwalten: Neuen Raum erstellen	Ermöglicht das Erstellen eines neuen Information-Spaces. Um diese Aufgabe auszuführen, benötigen Sie die folgenden Rechte: • *Bei Explorer anmelden und dieses Objekt in der CMC anzeigen* • *Information-Spaces verwalten*
Information-Space verwalten: Information-Space ändern	Ermöglicht es, einen Information-Space zu ändern oder zu löschen. Um diese Aufgabe auszuführen, benötigen Sie die folgenden Rechte: • *Bei Explorer anmelden und dieses Objekt in der CMC anzeigen* • *Information-Spaces verwalten*
Information-Spaces verwalten: Indizierung planen	Mit dieser Option kann die Indizierung der Information-Space-Daten geplant werden. Um diese Aufgabe auszuführen, benötigen Sie die folgenden Rechte: • *Bei Explorer anmelden und dieses Objekt in der CMC anzeigen* • *Information-Spaces verwalten*
Information-Spaces verwalten: Indizierung starten	Mit dieser Option kann die Indizierung für Information-Space-Daten ausgeführt werden. Um diese Aufgabe auszuführen, benötigen Sie die folgenden Rechte: • *Bei Explorer anmelden und dieses Objekt in der CMC anzeigen*

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Recht	Beschreibung
	• *Information-Spaces verwalten*

29.3.13.12 SAP BusinessObjects Mobile

Die Rechte in diesem Abschnitt gelten nur für SAP BusinessObjects Mobile.

Recht	Beschreibung
Anmelden bei SAP BusinessObjects Mobile	Ermöglicht die Anmeldung bei der BI-Plattform über die Mobile-Anwendung und das Anzeigen von Dokumenten.
Dokumentwarnmeldungen abonnieren	Ermöglicht das Abonnieren von Dokument-/ Wiederholungswarnungen. **Hinweis** Wenn Ihnen das Recht "Abonnement von Dokumentwarnungen" anfänglich gewährt wurde und es Ihnen derzeit verweigert wird, erhalten Sie die abonnierten Warnungen weiterhin. Wenn Sie die Warnungen nicht mehr erhalten möchten, muss das Abonnement ausdrücklich gekündigt werden. **Hinweis** Um Dokumentwarnmeldungen (oder wiederkehrende Instanzen) zur zeitgesteuerten Verarbeitung zu abonnieren, muss der Benutzer über den Sicherheitszugriff "Voller Zugriff" für den Ordner "Systemereignisse" unter "Ereignisse" in der Central Management Console (CMC) verfügen.
Dokumente im lokalen Gerätespeicher speichern	Ermöglicht das Speichern von Dokumenten auf dem mobilen Gerät. **Hinweis** Wenn Sie über das Recht "Dokumente im lokalen Gerätespeicher speichern" verfügen und Dokumente auf dem Gerät speichern, sind diese Dokumente auch dann noch auf dem Gerät vorhanden, wenn Ihnen das Recht entzogen wurde. Diese Dokumente werden jedoch beim Synchronisierungsvorgang nicht berücksichtigt.
Dokumente vom Gerät per E-Mail senden	Ermöglicht das Senden von Berichten per E-Mail.

Weitere Informationen finden Sie im *Installations- und Implementierungshandbuch für SAP BusinessObjects Mobile*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

30 Servereigenschaften (Anhang)

30.1 Über Servereigenschaften (Anhang)

In diesem Anhang zu Servereigenschaften werden Eigenschaften beschrieben, die für die einzelnen Server der BI-Plattform festgelegt werden können.

> **Hinweis**
>
> Weitere Informationen zu den Servereigenschaften und Metriken von SAP BusinessObjects Explorer finden Sie im *SAP BusinessObjects Explorer-Administratorhandbuch*.

30.1.1 Allgemeine Servereigenschaften

Die in diesem Abschnitt beschriebenen Servereigenschaften gelten für alle Servertypen.

Tabelle 27: Anforderungs-Port-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Servername	Name des Servers	Der Standardwert ist der Namen des Knotens, auf dem sich der Server befindet, plus der Name des Servers.
ID, CUID	Die kurze ID und eindeutige Cluster-ID des Servers. Schreibgeschützt.	Diese Werte werden automatisch generiert.
Knoten	Der Name des Knotens, auf dem sich der Server befindet.	Dieser Wert wird während der Installation angegeben.
Beschreibung	Die Serverbeschreibung	Der Standardwert ist der Name des Servers.
Befehlszeilenparameter	Die Befehlszeilenparameter für den Server.	Der Standardwert hängt vom Typ des Servers ab.
Anforderungs-Port	Der Port, über den der Server Anforderungen empfängt. In einer Umgebung mit Firewalls konfigurieren Sie den Server so, dass er nur Anforderungen auf Ports überwacht, die in der Firewall geöffnet sind. Wenn Sie einen Port für den Server angeben, stellen Sie sicher, dass der Port noch nicht von einem anderen Prozess genutzt wird.	**Automatisch zuweisen** ist standardmäßig auf `TRUE` festgelegt, und **Anforderungs-Port** hat keinen Eintrag.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	Hinweis Wenn **Automatisch zuweisen** aktiviert ist, wird der Server an einen dynamisch zugewiesenen Port gebunden. Dies bedeutet, dass dem Server bei jedem Neustart eine zufällige Portnummer zugewiesen wird.	
Automatisch zuweisen	Legt fest, ob der Server bei jedem Neustart an einen dynamisch zugewiesenen Port gebunden wird. Um den Server an einen bestimmten Port zu binden, legen Sie **Automatisch zuweisen** auf `FALSE` fest und geben einen gültigen **Anforderungs-Port** an.	Der Standardwert lautet `TRUE`.

Tabelle 28: Automatisch starten-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Diesen Server beim Start des Server Intelligence Agents automatisch starten	Legt fest, ob der Server beim Start oder Neustart des Server Intelligence Agents (SIA) automatisch gestartet wird. Wenn dieser Wert auf `FALSE` festgelegt ist und der SIA gestartet bzw. neu gestartet wird, wird der Server nicht gestartet.	Der Standardwert lautet `TRUE`.

Tabelle 29: Hostkennungseigenschaften

Eigenschaft	Beschreibung	Standardwert
Automatisch zuweisen	Legt fest, ob der Server an eine Netzwerkschnittstelle gebunden wird, die automatisch zugewiesen wird. Wenn diese Option auf `FALSE` gesetzt ist, wird der Server an eine spezifische Netzwerkschnittstelle gebunden. Wenn die Option auf `TRUE` gesetzt ist, akzeptiert der Server Anforderungen an der ersten verfügbaren IP-Adresse. Auf mehrfach vernetzten Rechnern können Sie eine bestimmte Netzwerkschnittstelle zum Binden festlegen, indem Sie diesen Wert auf `FALSE` setzen und einen gültigen Hostnamen oder eine IP-Adresse angeben.	Der Standardwert lautet `TRUE`.
Hostname	Der Hostname der Netzwerkschnittstelle, an die der Server gebunden wird. Wenn der Hostname angegeben ist, akzeptiert der Server Anforderungen an allen mit dem Hostnamen verknüpften IP-Adressen.	Standardmäßig ist **Automatisch zuweisen** auf `TRUE` gesetzt, und der **Hostname** ist leer.
IP-Adresse	Der IP-Adresse der Netzwerkschnittstelle, an die der Server gebunden wird. Sowohl das IPv4- als auch das IPv6-Protokoll wird unterstützt. Wenn eine IP-Adresse angegeben wird, akzeptiert der Server Anforderungen nur an der IP-Adresse.	Standardmäßig ist **Automatisch zuweisen** auf `TRUE` gesetzt, und die **IP-Adresse** ist leer.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Tabelle 30: Konfigurationsvorlageneigenschaften

Eigenschaft	Beschreibung	Standardwert
Konfigurationsvorlage verwenden	Legt fest, ob eine Konfigurationsvorlage verwendet werden soll.	Der Standardwert lautet `FALSE`.
Systemstandardwerte wiederherstellen	Legt fest, ob die ursprünglichen Standardeinstellungen für diesen Server wiederhergestellt werden.	Der Standardwert lautet `FALSE`.
Klicken Sie auf **Konfigurationsvorlage festlegen**.	Legt fest, ob die Einstellungen des aktuellen Dienstes als Konfigurationsvorlage für alle Dienste desselben Typs verwendet werden sollen. Falls `TRUE`, werden alle Dienste des Typs, für den Sie **Konfigurationsvorlage verwenden** festgelegt haben, sofort neu konfiguriert, sodass sie die Einstellungen des aktuellen Dienstes verwenden.	Der Standardwert lautet `FALSE`.

Tabelle 31: Ablaufverfolgungsprotokoll-Dienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Protokollierungsebene	Gibt die niedrigste Wichtigkeitsstufe für die Aufzeichnung von Meldungen an und legt die Menge der Daten fest, die in der Serverprotokolldatei erfasst werden. Mögliche Protokollierungsschwellenebenen sind: • **Nicht angegeben** • **Keine** • **Niedrig** • **Mittel** • **Hoch**	Der Standardwert lautet `Nicht angegeben`.

Weitere Informationen

Arbeiten mit Konfigurationsvorlagen [Seite 393]
Ablaufverfolgungsprotokollierungsebenen [Seite 595]

30.1.2 Kerndienste-Eigenschaften

Die Kategorie "Kerndienste" umfasst die folgenden Server:

- Adaptive Job Server
- Adaptive Processing Server
- Central Management Server
- Dashboard Server
- Dashboard Analytics Server

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- Event Server
- Input File Repository Server
- Output File Repository Server
- Web Application Container Server

Eigenschaften des Adaptive Job Servers

Tabelle 32: Allgemeine Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Temporäres Verzeichnis	Gibt das Verzeichnis an, in dem temporäre Dateien bei Bedarf erstellt werden. Wenn dieses Verzeichnis nicht über den erforderlichen Speicherplatz verfügt, können Leistungsprobleme auftreten. Sie können eine bessere Leistung gewährleisten, wenn sich dieses Verzeichnis auf einer lokalen Festplatte befindet. **Hinweis** Starten Sie den Server neu, damit die Änderungen wirksam werden.	%DefaultDataDir%

Auf dem Adaptive Job Server können mehrere Dienste gehostet werden. Jeder Dienst hat die folgenden Eigenschaften

Tabelle 33: Diensteigenschaften

Eigenschaft	Beschreibung	Standardwert
Maximale Anzahl gleichzeitiger Aufträge	Gibt die Anzahl der auf dem Server zulässigen untergeordneten Prozesse (Unterprozesse) an. Sie können die maximale Anzahl von Aufträgen an Ihre Berichtsumgebung anpassen. Die Standardeinstellung ist für die meisten Reporting-Szenarios geeignet. Die ideale Einstellung für die Reporting-Umgebung hängt von Hardwarekonfiguration, Datenbanksoftware und Reporting-Anforderungen ab.	5
Maximale Anzahl untergeordneter Anforderungen	Gibt die Anzahl der Aufträge an, die vor einem Neustart vom untergeordneten Element verarbeitet werden.	100

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaften des Adaptive Processing Servers

Tabelle 34: Allgemeine Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Zeitsperre für Dienststart (Sekunden)	Gibt die Zeit in Sekunden an, die der Server auf das Starten von Diensten wartet. Wenn ein Dienst innerhalb der angegebenen Zeit nicht gestartet wird, kann einer von zwei Gründen vorliegen: • Der Dienst ist fehlgeschlagen, weil eine erforderliche Ressource, z.B. eine Datenbank, nicht gefunden wurde, oder beim Dienst ist ein Port-Konflikt aufgetreten. • Der Dienst konnte nicht innerhalb der angegebenen Zeit gestartet werden, da das System beispielsweise zu langsam ist. Um den Grund zu finden, überprüfen Sie die Serverprotokolldatei. Wenn der Dienst nicht in der angegebenen Zeit gestartet werden konnte, kann es hilfreich sein, diesen Wert zu erhöhen.	1200

Tabelle 35: Eigenschaften des Proxydiensts für das Client-Auditing

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Tabelle 36: Eigenschaften des Sicherheitstokendiensts

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Tabelle 37: Eigenschaften des Diensts "Insight to Action"

Metrik	Beschreibung	
Maximale Anzahl an aktiven Verbindungen pro Benutzersitzung	Die maximale Anzahl an Verbindungen, die einem Benutzer zu einem bestimmten Zeitpunkt zur Verfügung stehen. Wenn ein Benutzer einen Bericht oder ein Dashboard öffnet, das BBS-fähig ist, wird die Verbindung mit dem SAP-Server hergestellt, um die verfügbaren BBS-Ziele zu ermitteln.	20
Maximale Anzahl an Verbindungen im Leerlauf pro Benutzersitzung	Die Anzahl an Verbindungen im Leerlauf, die geöffnet bleiben und für nachfolgende BBS-Anforderungen wiederverwendet werden sollen. Durch Erhöhen dieser Einstellung werden zusätzliche Systemressourcen zugeteilt.	20
Maximale Wartezeit für Verbindung (in Sekunden)	Die Zeitdauer, die das Aktionseinblick-Framework auf eine Antwort vom SAP-Server warten sollte, bevor eine Zeitüberschreitung eintritt (in Sekunden).	30

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Tabelle 38: Eigenschaften des Veröffentlichungsdiensts

Eigenschaft	Beschreibung	Standardwert
Thread-Pool-Größe	Gibt an, wie viele Bereichsstapel-Verarbeitungsthreads gleichzeitig ausgeführt werden können. Wenn der Wert dieser Eigenschaft auf "0" gesetzt ist, wird die Thread-Pool-Größe mit einer Formel bestimmt, die auf der Anzahl der CPU-Kerne im betreffenden Rechner basiert.	0

Tabelle 39: Eigenschaften des Übersetzungsdiensts

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Tabelle 40: Eigenschaften des Überwachungsdiensts

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Tabelle 41: Eigenschaften des Plattformsuchdiensts

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Tabelle 42: Eigenschaften des Diensts zur Nachverarbeitung von Veröffentlichungen

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Eigenschaften des Central Management Servers

Hinweis

Wenn Sie eine beliebige dieser Servereigenschaften bearbeiten, muss der Server neu gestartet werden, damit die Änderungen wirksam werden.

Tabelle 43: Eigenschaften des Central Management Service

Eigenschaft	Beschreibung	Standardwert
Name Server-Port	Gibt den Port an, den der CMS auf anfängliche Namensdienstanforderungen überwacht.	6400
Angeforderte Systemdatenbankverbindungen	Gibt die Anzahl der CMS-Systemdatenbankverbindungen an, die der CMS einzurichten versucht. Wenn der Server nicht alle angeforderten Datenbankverbindungen einrichten kann, funktioniert der CMS zwar weiterhin, aber seine Leistung verschlechtert sich, da weniger gleichzeitige Anforderungen auf einmal verarbeitet werden können. Der CMS ver-	14

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	sucht, weitere Verbindungen einzurichten, bis die angeforderte Anzahl von Verbindungen schließlich eingerichtet ist. Die Metrik **Eingerichtete Systemdatenbankverbindungen** des CMS zeigt die aktuelle Anzahl eingerichteter Verbindungen.	
Automatisch Wiederverbindung zur Systemdatenbank herstellen	Legt fest, ob der CMS automatisch versucht, eine Verbindung zur CMS-Datenbank wiederherzustellen, nachdem eine Dienstunterbrechung aufgetreten ist. Wenn dieser Wert auf `FALSE` festgelegt ist, können Sie die Integrität der CMS-Datenbank überprüfen, bevor der Betrieb wiederaufgenommen wird. Starten Sie dazu den CMS neu, um die Datenbankverbindung wiederherzustellen.	`TRUE`

Tabelle 44: Eigenschaften des Einzelanmeldungsdiensts

Eigenschaft	Beschreibung	Standardwert
Ablauf der Einzelanmeldung (Sekunden)	Gibt die Zeit in Sekunden an, die eine SSO-Verbindung zu einer Datenquelle vor Ablauf gültig ist. Dies gilt für Windows AD-Benutzer, die Berichte ausführen, die für die Windows AD-Einzelanmeldung für die Datenquelle konfiguriert sind.	86400

Eigenschaften des Event Servers

Tabelle 45: Eigenschaften des Ereignisdiensts

Eigenschaft	Beschreibung	Standardwert
Ereignis-Abfrageintervall (Sekunden)	Legt fest, wie oft (in Sekunden) der Server eine Datei abfragt, durch die ein Ereignis ausgelöst wird.	10 Der zulässige Wertebereich liegt zwischen 1 und 1.200 Sekunden.
Bereinigungsintervall (Minuten)	Legt fest, wie oft (in Minuten) ein Bereinigungs-Dienstprogramm ausgeführt wird.	20

Eigenschaften des Input File Repository Servers

Tabelle 46: Eigenschaften des Input-Dateispeicherdiensts

Eigenschaft	Beschreibung	Standardwert
Dateispeicherverzeichnis	Gibt das Verzeichnis an, in dem Datei-Repository-Objekte gespeichert werden.	%DefaultInputFRSDir/%

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	Hinweis Wenn dieses Verzeichnis nicht über den erforderlichen Speicherplatz verfügt, können Leistungsprobleme auftreten.	
Temporäres Verzeichnis	Gibt das Verzeichnis an, in dem temporäre Dateien bei Bedarf erstellt werden. Hinweis Wenn dieses Verzeichnis nicht über den erforderlichen Speicherplatz verfügt, können Leistungsprobleme auftreten. Um eine bessere Leistung zu gewährleisten, empfiehlt es sich, das **temporäre Verzeichnis** im selben Dateisystem wie das **Dateispeicherverzeichnis** anzusiedeln.	%DefaultInputFRSDir/temp%
Maximale Leerlaufzeit (Minuten):	Gibt die Zeitdauer an, die der Server wartet, bis er inaktive Verbindungen trennt. Ein zu niedriger Wert kann dazu führen, dass die Anforderung des Benutzers vorzeitig geschlossen wird. Durch einen zu hohen Wert können Systemressourcen, wie Verarbeitungszeit und Festplattenkapazität, übermäßig beansprucht werden.	10
Maximale Wiederholungen für den Dateizugriff	Gibt an, wie häufig der Server versucht, auf eine Datei zuzugreifen.	1

Eigenschaften des Output File Repository Servers

Tabelle 47: Eigenschaften des Output-Dateispeicherdiensts

Eigenschaft	Beschreibung	Standardwert
Dateispeicherverzeichnis	Gibt das Verzeichnis an, in dem Datei-Repository-Objekte gespeichert werden. Hinweis Wenn dieses Verzeichnis nicht über den erforderlichen Speicherplatz verfügt, können Leistungsprobleme auftreten.	%DefaultOutputFRS-Dir/%
Temporäres Verzeichnis	Gibt das Verzeichnis an, in dem temporäre Dateien bei Bedarf erstellt werden.	%DefaultOutputFRS-Dir/temp%

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	Hinweis Wenn dieses Verzeichnis nicht über den erforderlichen Speicherplatz verfügt, können Leistungsprobleme auftreten.	
Maximale Leerlaufzeit (Minuten):	Gibt die Zeitdauer an, die der Server wartet, bis er inaktive Verbindungen trennt. Ein zu niedriger Wert kann dazu führen, dass die Anforderung des Benutzers vorzeitig geschlossen wird. Durch einen zu hohen Wert können Systemressourcen, wie Verarbeitungszeit und Festplattenkapazität, übermäßig beansprucht werden.	10
Maximale Wiederholungen für den Dateizugriff	Gibt an, wie häufig der Server versucht, auf eine Datei zuzugreifen.	1

Eigenschaften des Web Application Container Servers

Tabelle 48: Allgemeine Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Zeitsperre für Dienststart (Sekunden)	Gibt an, wie lange der WACS auf das Starten der gehosteten Dienste wartet, bevor eine Zeitüberschreitung auftritt. Bei Ablauf der Zeitüberschreitung, bietet der WACS keine Dienste an, die noch nicht gestartet wurden. Auf einem langsameren Rechner kann auch ein höherer Wert angegeben werden. Wenn Sie einen zu kleinen Wert angeben und der WACS vor der Zeitüberschreitung nicht gestartet wird, stellen Sie die Standardeinstellungen des WACS über den Central Configuration Manager (CCM) wieder her.	1200

Tabelle 49: Ablaufverfolgungsprotokoll-Dienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Protokollierungsebene	Ermöglicht die Protokollierung und legt den Schwere- und Detaillierungsgrad auf "Kein" (nur kritische Ereignisse werden protokolliert), "Niedrig" (Start, Herunterfahren und Start- und Endanforderungs-Meldungen), "Mittel" (Fehler-, Warn- und die meisten Statusmeldungen) oder "Hoch" (Nichts ausgeschlossen. Nur zur Fehlerbehebung. Die CPU-Auslastung steigt möglicherweise an und beeinträchtigt die Performance).	Nicht angegeben

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	Die verfügbaren Menüoptionen sind: • **Nicht angegeben** • **Keine** • **Niedrig** • **Mittel** • **Hoch**	

Tabelle 50: Eigenschaften des Business-Process-BI-Dienstes

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Tabelle 51: Eigenschaften des Query-Builder-Dienstes

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Tabelle 52: RESTful-Webdienst – Konfiguration der Systemeigenschaften

Eigenschaft	Beschreibung	Standardwert
Fehlerstapel anzeigen	Wenn diese Option aktiviert ist, enthält das Fehlerprotokoll RESTful-Webdienst-Fehlermeldungen zur Fehlerbehebung. Sie sollte sonst nicht verwendet werden, oder bei Sicherheitsbedenken, wenn Details der BI-Plattform angezeigt werden.	Nicht ausgewählt
Standard-Objektanzahl pro Seite	Die Anzahl der Einträge, die auf einer Seite aufgeführt werden. Entwickler können diese Einstellung mit dem Parameter &pageSize=<m> im RESTful-Webdienst-SDK außer Kraft setzen.	50
Zeitüberschreitung für Enterprise-Sitzungstoken (Minuten)	Die Ablaufzeit, in der ein Anmeldetoken gültig bleibt. Nach Ablauf dieser Zeit muss ein neues Anmeldetoken generiert werden.	60
Sitzungspoolgröße	Dies ist die Anzahl zwischengespeicherter Sitzungen, die gleichzeitig gespeichert werden, um die Serverleistung zu verbessern. Der Sitzungspool speichert aktive RESTful-Webdienstsitzungen im Zwischenspeicher, damit sie wiederverwendet werden können, wenn ein Benutzer eine andere Anforderung sendet, die dasselbe Anmeldetoken im HTTP-Request-Header verwendet.	1000
Sitzungspool-Zeitüberschreitung (Minuten)	Die Zeit in Minuten, in der zwischengespeicherte Sitzungen ablaufen.	2
HTTP-Standardauthentifizierung aktivieren	Wenn diese Einstellung nicht aktiviert ist, müssen RESTful-Webdienstanforderungen ein Anmeldetoken verwenden.	Nicht ausgewählt

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	Wenn diese Einstellung aktiviert ist, müssen Benutzer Ihren Namen und Ihr Kennwort bei der ersten RESTful-Webdienstanforderung eingeben. Wenn diese Einstellung aktiviert ist, wird das Dropdown-Menü **Standardmäßiges Authentifizierungsschema für HTTP Basic** angezeigt.	
Standardmäßiges Authentifizierungsschema für HTTP Basic	Wenn **HTTP-Standardauthentifizierung aktivieren** aktiviert ist, kann einer von vier Authentifizierungstypen ausgewählt werden. Die Namen und Kennwörter werden in Klartext übertragen, wenn keine HTTPS-Optionen verwendet werden. Zulässige Werte: • **secEnterprise** • **secDAP** • **SAPR3** • **secWinAD**	Leer. Wenn jedoch **HTTP-Standardauthentifizierung aktivieren** ausgewählt wurde, ist standardmäßig **secEnterprise** aktiviert.

Tabelle 53: RESTful-Webdienst – Eigenschaften der Ressourcenfreigabe-Konfiguration über Ursprungs-URLs hinweg

Eigenschaft	Beschreibung	Standardwert
Ursprungs-URLs zulassen	Diese Einstellung ermöglicht es Benutzern mit CORS-fähigen Browsern, auf JavaScript-Seiten zuzugreifen, die auf mehrere Domänennamen zugreifen müssen. Fügen Sie alle Domänennamen hinzu, und trennen Sie sie durch ein Komma. Zum Beispiel http://origin1.server.com:8080, http://origin2.server.com:8080. Standardmäßig können die Browser auf alle Domänen zugreifen (*).	* (ein Sternchen)
Max. Alter (Minuten)	Dies ist die maximale Zeit, für die HTTP-Anforderungen in den Browsern zwischengespeichert werden können.	1440

Tabelle 54: RESTful-Webdienst – Eigenschaften der Konfiguration der vertrauenswürdigen Authentifizierung

Eigenschaft	Beschreibung	Standardwert
Abrufmethode	Diese Einstellung ist ein Menü, in dem festgelegt wird, welche Abfragemethode zum Abrufen von Anmeldetokens für die vertrauenswürdige Authentifizierung verwendet wird, wenn das RESTful-Webdienst-API */logon/trusted* verwendet wird. • **HTTP_HEADER** wird für GET-Abfragen mit dem Request-Header accept=application/xml (oder application/json) verwendet. • **QUERY_STRING** wird verwendet, um einen Anmeldenamen unter Verwendung des RESTful-Webdienst-APIs, z.B. /logon/trusted/?user=johndoe, am Ende einer URL-Abfrage hinzuzufügen.	`HTTP_HEADER`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	• **COOKIE** wird verwendet, wenn der Anmeldenamen von einem Webbrowser-Cookie abgerufen wird. Domäne, Name, Wert und Pfad müssen in dem Cookie gespeichert sein.	
Benutzernamensparameter	Mit dieser Beschriftung wird der vertrauenswürdige Benutzer zum Abrufen eines Anmeldetokens identifiziert.	`X-SAP-TRUSTED-USER`

Tabelle 55: Eigenschaften des BOE-Webanwendungsdiensts

Eigenschaftstyp	Beschreibung	Standardwert
Authentifizierungstyp	Der Authentifizierungstyp, der zur Authentifizierung von Benutzern verwendet wird, die sich beim BI-Launchpad anmelden. Zulässige Werte: • **AD Kerberos** • **AD Kerberos SSO** • **Enterprise** • **LDAP**	**Enterprise**
AD-Standarddomäne	Die Active Directory-Standarddomäne wird verwendet, damit Benutzer bei der Anmeldung keine Domäne angeben müssen. Wenn die Standarddomäne beispielsweise auf "MeineDomäne" festgelegt ist und sich ein Benutzer mit dem Benutzernamen "Benutzer" anmeldet, versucht die Active Directory-Anmeldestelle, "Benutzer@MeineDomäne.com" zu authentifizieren.	Leer
Dienstprinzipalname	Ein Dienstprinzipalname wird von Clients verwendet, um eine Dienstinstanz eindeutig zu identifizieren. Der Kerberos-Authentifizierungsdienst verwendet einen Dienstprinzipalnamen, um einen Dienst zu authentifizieren.	Leer
Keytab-Datei	Der vollständige Pfad zu einer Keyhan-Datei. Über eine Keytab-Datei können Kerberos-Filter so konfiguriert werden, dass das Kennwort des Benutzerkontos auf dem Webanwendungscomputer nicht offengelegt wird.	Leer

Tabelle 56: Eigenschaften von Web Services SDK und QaaWS

Eigenschaft	Beschreibung	Standardwert
Kerberos Active Directory Einzelanmeldung aktivieren	Gibt an, ob die Kerberos AD-Einzelanmeldung für Web Services SDK und QaaWS aktiviert werden soll.	`FALSE`
AD-Standarddomäne	Die Active Directory-Standarddomäne wird verwendet, damit Benutzer bei der Anmeldung keine Domäne angeben müssen.	Leer
Dienstprinzipalname	Ein Dienstprinzipalname wird von Clients verwendet, um eine Dienstinstanz eindeutig zu identifizieren. Der Kerberos-Au-	Leer

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	thentifizierungsdienst verwendet einen Dienstprinzipalnamen, um einen Dienst zu authentifizieren.	
Keytab-Datei	Der vollständige Pfad zu einer Keyhan-Datei. Über eine Keytab-Datei können Kerberos-Filter so konfiguriert werden, dass das Kennwort des Benutzerkontos auf dem Webanwendungscomputer nicht offengelegt wird.	Leer

Tabelle 57: Eigenschaften der HTTP-Konfiguration

Eigenschaft	Beschreibung	Standardwert
An alle IP-Adressen binden	Gibt an, ob die Bindung an alle Netzwerkschnittstellen erfolgt oder nicht. Wenn Ihr Server über mehrere NICs verfügt und Sie eine Bindung an eine bestimmte Netzwerkschnittstelle vornehmen möchten, deaktivieren Sie diese Eigenschaft.	`TRUE`
An Hostnamen oder IP-Adresse binden	Gibt die Netzwerkschnittstelle (IP-Adresse oder Hostname) an, auf der der HTTP-Dienst bereitgestellt wird. Ein Wert kann nur angegeben werden, wenn Sie **An alle IP-Adressen binden** deaktivieren.	`localhost`
HTTP-Port	Der Port, an dem der HTTP-Dienst bereitgestellt wird.	6405 Der zulässige Wertebereich liegt zwischen 1 und 65535.
Maximale Größe des HTTP-Headers	Die maximal zulässige Größe in Byte des Anforderungs- und Antwort-HTTP-Headers.	32768

Tabelle 58: Konfiguration der Eigenschaften von "HTTP über Proxy"

Eigenschaft	Beschreibung	Standardwert
"HTTP über Proxy" aktivieren	Gibt an, ob der "HTTP über Proxy"-Connector auf dem WACS aktiviert wird. Diese Option ist normalerweise in Implementierungen mit einem Reverse Proxy aktiviert.	`FALSE`
An alle IP-Adressen binden	Gibt an, ob der "HTTP über Proxy"-Port an alle Netzwerkschnittstellen gebunden wird oder nicht.	`TRUE`
An Hostnamen oder IP-Adresse binden	Gibt die Netzwerkschnittstelle (IP-Adresse oder Hostname) an, auf der der "HTTP über Proxy"-Dienst bereitgestellt wird. Ein Wert kann nur angegeben werden, wenn Sie **An alle IP-Adressen binden** deaktivieren.	`localhost`
HTTP-Port	Der Port, an dem der HTTP-Dienst in einer Reverse Proxy-Implementierung bereitgestellt wird. Ein Wert kann nur angegeben werden, wenn Sie **HTTP über Proxy aktivieren** auswählen.	6406 Der zulässige Wertebereich liegt zwischen 1 und 65535.
Proxy-Hostname	IPv4-Adresse, IPv6-Adresse, Hostname oder voll qualifizierter Domänenname Ihres Proxyservers. Ein Wert kann nur an-	Leer

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	gegeben werden, wenn Sie **HTTP über Proxy aktivieren** auswählen.	
Proxy-Port	Der Port des Forward- oder Reverse Proxy-Servers. Ein Wert kann nur angegeben werden, wenn Sie **HTTP über Proxy aktivieren** auswählen.	0 Der zulässige Wertebereich liegt zwischen 1 und 65535.
Maximale Größe des HTTP-Headers	Die maximal zulässige Größe in Byte des Anforderungs- und Antwort-HTTP-Headers.	32768

Tabelle 59: HTTPS-Konfigurationseigenschaften

Eigenschaft	Beschreibung	Standardwert
HTTPS aktivieren	Gibt an, ob die HTTPS/SSL-Kommunikation aktiviert wird.	`FALSE`
An Hostnamen oder IP-Adresse binden	Gibt die Netzwerkschnittstelle (IP-Adresse oder Hostname) an, auf der der HTTPS-Dienst bereitgestellt wird. Ein Wert kann nur angegeben werden, wenn Sie **HTTPS aktivieren** auswählen.	`localhost`
HTTPS-Port	Der Port, an dem der HTTPS-Dienst bereitgestellt wird. Ein Wert kann nur angegeben werden, wenn Sie **HTTPS aktivieren** auswählen.	443 Der zulässige Wertebereich liegt zwischen 1 und 65535.
Proxy-Hostname	IPv4-Adresse, IPv6-Adresse, Hostname oder voll qualifizierter Domänenname Ihres Proxyservers. Ein Wert kann nur angegeben werden, wenn Sie **HTTPS aktivieren** auswählen.	Leer
Proxy-Port	Der Port des Forward- oder Reverse Proxy-Servers. Ein Wert kann nur angegeben werden, wenn Sie **HTTPS aktivieren** auswählen.	0 Der zulässige Wertebereich liegt zwischen 1 und 65535.
Protokoll	Das zu verwendende Verschlüsselungsprotokoll. Ein Wert kann nur angegeben werden, wenn Sie **HTTPS aktivieren** auswählen.	TLS Zulässgie Werte sind TLS oder SSL.
Zertifikatspeichertyp	Der Typ des Zertifikatspeichers, der Ihre Zertifikate und privaten Schlüssel enthält. In den meisten Fällen handelt es sich um **PCKS12**. Ein Wert kann nur angegeben werden, wenn Sie **HTTPS aktivieren** auswählen.	PKCS12 Zulässige Werte sind PKCS12 oder JKS.
Speicherort der Zertifikatspeicherdatei	Der vollständige Pfad zur Zertifikatdatei. Ein Wert kann nur angegeben werden, wenn Sie **HTTPS aktivieren** auswählen.	Leer
Zugangskennwort für den privaten Schlüssel	PKCS12-Zertifikatspeicher und JKS-Keystores verfügen über kennwortgeschützte private Schlüssel, die den unbefugten Zugriff oder Datendiebstahl verhindern. Geben Sie hier das Kennwort ein, das Sie beim Generieren des Zertifikatspei-	Leer

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	chers angegeben haben, sodass der WACS auf private Schlüssel aus dem Zertifikatspeicher zugreifen kann. Ein Wert kann nur angegeben werden, wenn Sie **HTTPS aktivieren** auswählen.	
Zertifikat-Alias	Der Alias des Zertifikats innerhalb des Zertifikatspeichers. Wenn kein Alias angegeben wurde und ein Zertifikatspeicher verwendet wird, der mehrere Zertifikate enthält, wird das erste Zertifikat im Speicher verwendet. In den meisten Fällen muss kein Wert angegeben werden. Ein Wert kann nur angegeben werden, wenn Sie **HTTPS aktivieren** auswählen.	Leer
Clientauthentifizierung aktivieren	Wenn die Clientauthentifizierung aktiviert ist, können WACS-Dienste nur von Clients abgerufen werden, für die Schlüssel in der Datei der Zertifikatvertrauensliste gespeichert sind. Andere Clients werden abgewiesen. Sie können die Clientauthentifizierung nur aktivieren, wenn Sie **HTTPS aktivieren** auswählen.	`FALSE`
Speicherort der Datei mit der Zertifikatvertrauensliste	Der vollständige Pfad zur Datei mit der Zertifikatvertrauensliste. Ein Wert kann nur angegeben werden, wenn Sie **HTTPS aktivieren** und **Clientauthentifizierung aktivieren** auswählen.	Leer
Zertifikatvertrauensliste – Zugangskennwort für den privaten Schlüssel	Das Kennwort, durch das der Zugriff auf die privaten Schlüssel in der Datei der Zertifikatvertrauensliste geschützt wird. Ein Wert kann nur angegeben werden, wenn Sie **HTTPS aktivieren** und **Clientauthentifizierung aktivieren** auswählen.	Leer
Maximale Größe des HTTP-Headers	Die maximal zulässige Größe in Byte des Anforderungs- und Antwort-HTTP-Headers.	32768

Tabelle 60: Eigenschaften für gleichzeitigen Zugriff (pro Connector)

Eigenschaft	Beschreibung	Standardwert
Maximale Anzahl gleichzeitiger Anforderungen	Die Anzahl gleichzeitiger HTTP- oder HTTPS-Anforderungen, die von den einzelnen Connectors (HTTP, HTTP über Proxy oder HTTPS) gleichzeitig verarbeitet werden können.	`150` Der zulässige Wertebereich liegt zwischen 1 und 1000.

Tabelle 61: Eigenschaften für die Konfiguration von Active Directory

Eigenschaft	Beschreibung	Standardwert
Speicherort der Datei Krb5.ini	Der vollständige Pfad zu einer `krb5.ini`-Datei, in der Kerberos-Konfigurationseinstellungen gespeichert werden.	Leer
Speicherort der Datei bscLogin.conf	Der vollständige Pfad zu einer `bscLogin.conf`-Datei.	Leer

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

30.1.3 Eigenschaften von Konnektivitätsdiensten

Die Konnektivitäts-Dienstkategorie umfasst die folgenden Dienste:

- Systemeigener Konnektivitätsdienst (auf Standalone-Server gehostet)
- Systemeigener Konnektivitätsdienst (32 Bit, auf Standalone-Server gehostet)
- Adaptiver Konnektivitätsdienst (auf APS gehostet)

Alle Dienste besitzen dieselben Konfigurationseinstellungen.

Tabelle 62: Eigenschaften des Excel-Datenzugriffsdiensts

Eigenschaft	Beschreibung	Standardwert
Zeitüberschreitung bei Bereinigung des Excel-Datenzugriffs (in Sekunden)	Gibt (in Sekunden) an, wie lange der Dienst auf einen inaktiven Client wartet, bevor er die Sitzung des Clients bereinigt.	Der Standardwert beträgt 1200 Sekunden.
Zeitüberschreitung bei Austausch des Excel-Datenzugriffs (in Sekunden)	Gibt (in Sekunden) an, wie lange der Dienst auf einen inaktiven Client wartet, bevor er die Sitzung des Clients auf der Festplatte austauscht. Es wird empfohlen, einen Wert anzugeben, der kleiner als der für die Eigenschaft **Zeitüberschreitung bei Bereinigung des Excel-Datenzugriffs (in Sekunden)** angegebene ist.	Der Standardwert beträgt 600 Sekunden.

Tabelle 63: Dienstvorgangseigenschaften

Eigenschaft	Beschreibung	Standardwert
	Nicht vergessen Nach Änderung der folgenden Dienstvorgangseigenschaften ist kein Neustart des Servers erforderlich.	
Verbindungspool	Aktiviert oder deaktiviert den Verbindungspool. Mögliche Werte: • Aktiviert – mit Zeitüberschreitung • Aktiviert – ohne Zeitüberschreitung • Deaktiviert **Hinweis** Der Verbindungspool ist eine Zwischenspeicherfunktion, die die Verbindungen zur Verbesserung der Serverleistung in einem wiederverwendbarem Zustand hält.	Aktiviert – mit Zeitüberschreitung
Verbindungspool-Zeitüberschreitung	Gibt die maximale Leerlaufzeit für Verbindungen im Pool (in Minuten) an.	60

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	Hinweis Diese Eigenschaft entspricht dem Parameter `Max Pool Time` der Datei `cs.cfg`. Die Deaktivierung des Pools entspricht der Festlegung von `Max Pool Time` auf `0`. Die Aktivierung des Pools ohne Zeitüberschreitung entspricht der Festlegung von `Max Pool Time` auf `-1`. Weitere Informationen finden Sie im *Datenzugriffshandbuch*.	
Standby-Zeitlimit des transienten Objekts	Gibt an, wie viele Minuten ein nicht genutztes temporäres Objekt im Server gehalten werden soll. Das Objekt wird im Anschluss daran entfernt und dessen Ressourcen freigegeben.	`60`
Zeitgeberintervall des transienten Objekts	Gibt die Zeit zwischen Aktivitätsprüfungen (in Minuten) an. Der Server sucht in regelmäßigen Abständen nach Kandidatenobjekten zur Entfernung.	`5`
HTTP-Segmentierung aktivieren	Aktiviert oder deaktiviert die HTTP-Segmentierung. **Hinweis** Die HTTP-Segmentierung ist nur für die 3-Schichten-Implementierung relevant. Sie wirkt sich auf die Leistung beim Öffnen/Regenerieren von Dokumenten aus, da größere Antworten weniger Roundtrips beim Abrufen großer Dokumente verursachen. Die Deaktivierung der HTTP-Segmentierung entspricht der Festlegung von **HTTP-Segmentgröße** auf `0`.	Aktiviert
HTTP-Segmentgröße	Gibt die Größe der vom Server ausgegebenen HTTP-Antworten (in Kilobyte) an.	`64`

Tabelle 64: Low-Level-Verfolgungseigenschaften

Eigenschaft	Beschreibung	Standardwert
Nicht vergessen Nach Änderung der folgenden Low-Level-Verfolgungseigenschaften ist kein Neustart des Servers erforderlich.		
Auftragsverfolgung aktivieren	Aktiviert die Verfolgung von Connection Server-Aufträgen.	Deaktiviert

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	Hinweis Hierfür muss die Eigenschaft **Protokollierungsebene** auf **Hoch** gesetzt werden.	
Middleware-Verfolgung aktivieren	Aktiviert die Verfolgung der gesamten Middleware. Um bestimmte Middleware zu verfolgen, konfigurieren Sie die Datei `cs.cfg` und starten den Server neu. **Hinweis** Hierfür muss die Eigenschaft **Protokollierungsebene** auf **Hoch** gesetzt werden.	Deaktiviert

Tabelle 65: Eigenschaften der aktiven Datenquellen

Eigenschaft	Beschreibung	Standardwert
Achtung Nach Änderung der Eigenschaften für aktive Datenquellen ist ein Neustart des Servers erforderlich.		
Datenquelle aktivieren	Ermöglicht die Auswahl der Datenquellen, für die Verbindungen hergestellt werden sollen. Diese Eigenschaft dient als Filter für Treiber. Sie können hier die aktiven Datenquellen angeben, um die gewünschten Treiber zu laden. **Achtung** Beim Standardserververhalten werden alle verfügbaren Treiber geladen. Spezialisieren Sie Server anhand dieser Einstellung. Dies ist besonders nützlich, wenn Sie mehrere CORBA-Server auf dem Netzwerk implementieren. **Nicht vergessen** Nur Treiber für ausgewählte Datenquellen werden geladen. Alle anderen werden ignoriert. Wenn Sie keine Datenquellen auswählen, lädt der Server alle verfügbaren Treiber. **Hinweis** Stellen Sie in den Servermetriken sicher, dass die ausgewählten Datenquellen aktiviert wurden. Die Netzwerk-	Nicht markiert

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	schichten und Datenbanken werden unter *Konnektivitätsdienst-Metriken* angezeigt.	
Netzwerkschicht	Gibt die von der Verbindung verwendete Netzwerkschicht an. **Hinweis** Nur der nicht lokalisierte Name wird berücksichtigt. Die Liste der verfügbaren Netzwerkschichten finden Sie in der Datei `driver.cfg`, die sich im Verzeichnis **`<connectionserver-install-dir>`**`\connectionServer` befindet.	• `ODBC` für systemeigene CORBA-Server • `JDBC` für Adaptive CORBA-Server
Datenbank	Gibt die von der Verbindung verwendete Datenbank an. **Hinweis** Nur der nicht lokalisierte Name wird berücksichtigt. Datenbanknamen können reguläre Ausdrücke sein, wenn es sich dabei um reine ASCII-Zeichenfolgen handelt. Bei Mustern wird die GNU-regexp-Syntax verwendet. Verwenden Sie `.*`, um nach allen Zeichen zu filtern. Der Ausdruck `MS SQL Server.*$` bedeutet beispielsweise, dass alle MS SQL Server-Datenbanken verwendet werden. Weitere Informationen über reguläre Ausdrucke finden Sie auf der PERL-Webseite unter *http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions* .	Das Feld bleibt solange leer, bis Sie einen Datenbanknamen eingeben.

Tabelle 66: Eigenschaften des benutzerdefinierten Datenzugriffsdiensts

Eigenschaft	Beschreibung	Standardwert
Zeitsperre zur Bereinigung des benutzerdefinierten Datenzugriffs (in Sekunden)	Gibt (in Sekunden) an, wie lange der Dienst auf einen inaktiven Client wartet, bevor er die Sitzung des Clients bereinigt.	Der Standardwert beträgt 1200 Sekunden.
Zeitsperre zum Vertauschen des benutzerdefinierten Datenzugriffs (in Sekunden)	Gibt (in Sekunden) an, wie lange der Dienst auf einen inaktiven Client wartet, bevor er die Sitzung des Clients auf der Festplatte austauscht. Es wird empfohlen, einen Wert anzugeben, der kleiner als der für die Eigenschaft **Zeitsperre zur Bereinigung des benutzerdefinierten Datenzugriffs (in Sekunden)** angegebene ist.	Der Standardwert beträgt 600 Sekunden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Tabelle 67: Einzelanmeldungsdienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Ablauf der Einzelanmeldung (Sekunden)	Gibt die Zeit in Sekunden an, die eine SSO-Verbindung vor Ablauf gültig ist.	Der Standardwert beträgt 86400 Sekunden.

Tabelle 68: Hochstufverwaltungsdienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Tabelle 69: Hochstufverwaltung-ClearCase-Dienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Tabelle 70: Eigenschaften des grafischen Vergleichsdienstes

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Weitere Informationen

Allgemeine Servereigenschaften [Seite 948]

30.1.4 Eigenschaften von Crystal-Reports-Diensten

Die Kategorie "Crystal-Reports-Dienste" umfasst die folgenden Server:

- Crystal Reports Cache Server
- Crystal Reports Processing Server
- Eigenschaften von Crystal Reports 2013 Report Application Server
- Crystal Reports 2013 Processing Server

Crystal Reports Cache Server-Eigenschaften

Alle Eigenschaften, die sowohl für Crystal Reports Cache Server als auch für Crystal Reports Processing Server gelten, sollten denselben Wert aufweisen. Wenn Sie die Einstellung **Viewer-Regenerierung gibt immer die aktuellsten Daten zurück** auf dem Cache Server auf `TRUE` festlegen, sollten Sie dieselbe Einstellung auf dem Processing Server ebenfalls auf `TRUE` festlegen.

> **Hinweis**
>
> Wenn Sie eine beliebige dieser Servereigenschaften bearbeiten, muss der Server neu gestartet werden, damit die Änderungen wirksam werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Tabelle 71: Crystal Reports Cache-Dienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Viewer-Regenerierung gibt immer die aktuellsten Daten zurück	Legt fest, ob alle zwischengespeicherten Seiten ignoriert und neue Daten direkt aus der Datenbank abgerufen werden, wenn Benutzer einen Bericht explizit regenerieren. **Hinweis** Diese Eigenschaft kann für ein Berichtsobjekt selbst festgelegt werden und je nach Bericht variieren. Die Servereinstellungen werden von den für das Berichtsobjekt festgelegten Werten überschrieben. Um einen Wert für das Berichtsobjekt anzugeben, wählen Sie den Bericht in der CMC aus und klicken auf **Standardeinstellungen** > **Anzeigeserver-Gruppe**.	Der Standardwert lautet `FALSE`.
Berichtsdaten für Clients freigeben	Legt fest, ob Berichtsdaten auf verschiedenen Clients gemeinsam verwendet werden. **Hinweis** Diese Eigenschaft kann für ein Berichtsobjekt selbst festgelegt werden und je nach Bericht variieren. Die Servereinstellungen werden von den für das Berichtsobjekt festgelegten Werten überschrieben.	Der Standardwert lautet `TRUE`.
Zeitsperre für Verbindung im Leerlauf (Minuten)	Legt fest, wie viele Minuten der Crystal Reports Cache Server auf Anforderungen von einer Verbindung wartet, die sich im Leerlauf befindet. Der Standardwert muss normalerweise nicht geändert werden.	Der Standardwert beträgt 20 Minuten.
Sicherheitscache-Zeitüberschreitung (Minuten)	Legt fest (in Minuten), wie lange der Server zwischengespeicherte Anmeldedaten, Berichtsparameter und Datenbankverbindungsinformationen verwendet, um Anforderungen zu verarbeiten, bevor er den CMS abfragt.	Der Standardwert beträgt 20 Minuten.
Älteste an einen Client übergebene Abrufdaten (Sekunden)	Gibt die Zeit in Sekunden an, die der Server zwischengespeicherte Daten verwendet, um die Anforderungen der auf Abruf erstellten Berichte zu erfüllen. Wenn der Server eine Anforderung empfängt, die mit Daten aus einer früheren Anforderung beantwortet werden kann und der seit Generierung der Daten verstrichene Zeitraum kürzer als der hier festgelegte Wert ist, verwendet der Server die Daten für die Beantwortung der nachfolgenden Anforderung erneut. Mit dem erneuten Verwenden von Daten auf diese Art und Weise wird die Systemleistung beträchtlich gesteigert, wenn mehrere Benutzer die gleichen Informationen benötigen.	Der Standardwert beträgt 0 Sekunden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	Berücksichtigen Sie beim Einstellen dieses Werts, wie wichtig es für Benutzer ist, aktuelle Daten zu erhalten. Wenn es äußerst wichtig ist, dass alle Benutzer aktuelle Daten empfangen (weil sich wichtige Daten vielleicht sehr häufig ändern), können Sie diese Art der erneuten Verwendung von Daten unterbinden, indem Sie den Wert auf Null setzen. **Hinweis** Diese Eigenschaft kann für ein Berichtsobjekt selbst festgelegt werden und je nach Bericht variieren. Die Servereinstellungen werden von den für das Berichtsobjekt festgelegten Werten überschrieben.	
Maximale Cache-Größe (KB)	Legt die Größe des Festplattenspeichers (in KB) fest, die zum Zwischenspeichern von Berichten verwendet wird. Ein großer Cache kann erforderlich sein, wenn der Server zahlreiche Berichte oder besonders komplexe Berichte verarbeiten muss.	Der Standardwert beträgt 256.000 KB.
Cache-Dateiverzeichnis	Gibt den Speicherort des Cache-Dateiverzeichnisses an.	`%DefaultDataDir%/CrystalReportsCachingServer/temp`
Java VM-Argumente	Legt die Befehlszeilenargumente fest, die der JVM bereitgestellt werden können.	Standardmäßig ist kein Wert angegeben.
DLL-Name	Legt den Namen des Dokumenttyp-Plugins fest, das derzeit geladen wird. Diese Eigenschaft ist schreibgeschützt.	rasprocReport

Crystal Reports Processing Server-Eigenschaften

Alle Eigenschaften, die sowohl für Crystal Reports Cache Server als auch für Crystal Reports Processing Server gelten, sollten denselben Wert aufweisen. Wenn Sie die Einstellung **Viewer-Regenerierung gibt immer die aktuellsten Daten zurück** auf dem Cache Server auf `TRUE` festlegen, sollten Sie dieselbe Einstellung auf dem Processing Server ebenfalls auf `TRUE` festlegen.

Hinweis

Wenn Sie eine beliebige dieser Servereigenschaften bearbeiten, muss der Server neu gestartet werden, damit die Änderungen wirksam werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Tabelle 72: Crystal-Reports-Verarbeitungsdienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Zeitsperre für Auftrag im Leerlauf (Minuten)	Gibt an, wie viele Minuten der Crystal Reports Processing Server zwischen Anforderungen für einen bestimmten Auftrag wartet.	Der Standardwert beträgt 20 Minuten.
Maximale Lebensdauer von Aufträgen pro untergeordnetem Element	Gibt die maximale Anzahl von Aufträgen an, die jeder untergeordneter Prozess pro Lebensdauer verwalten kann.	Der Standardwert beträgt 1.000.
Viewer-Regenerierung gibt immer die aktuellsten Daten zurück	Legt fest, ob alle zwischengespeicherten Seiten ignoriert und neue Daten direkt aus der Datenbank abgerufen werden, wenn Benutzer einen Bericht explizit regenerieren. Legt fest, ob Berichtsdaten auf verschiedenen Clients gemeinsam verwendet werden. Hinweis Diese Eigenschaft kann für ein Berichtsobjekt selbst festgelegt werden und je nach Bericht variieren. Die Servereinstellungen werden von den für das Berichtsobjekt festgelegten Werten überschrieben. Um einen Wert für das Berichtsobjekt anzugeben, wählen Sie den Bericht in der CMC aus und klicken auf **Standardeinstellungen** > **Anzeigeserver-Gruppe**.	Der Standardwert lautet `FALSE`.
Berichtsdaten für Clients freigeben	Legt fest, ob Berichtsdaten auf verschiedenen Clients gemeinsam verwendet werden. Legt fest, ob Berichtsdaten auf verschiedenen Clients gemeinsam verwendet werden. Hinweis Diese Eigenschaft kann für ein Berichtsobjekt selbst festgelegt werden und je nach Bericht variieren. Die Servereinstellungen werden von den für das Berichtsobjekt festgelegten Werten überschrieben.	Der Standardwert lautet `TRUE`.
Zeitsperre für Verbindung im Leerlauf (Minuten)	Legt fest, wie viele Minuten der Crystal Reports Processing Server auf Anforderungen von einer Verbindung wartet, die sich im Leerlauf befindet. Der Standardwert muss normalerweise nicht geändert werden.	Der Standardwert beträgt 20 Minuten.
Maximale Anzahl gleichzeitiger Aufträge (0 für automatisch)	Gibt die maximale Anzahl unabhängiger Aufträge an, die gleichzeitig auf dem Crystal Reports Processing Server ausgeführt werden dürfen. Wenn der Wert dieser Eigenschaft auf "0" festgelegt wird, wendet der Server einen geeigneten Wert an, der auf der CPU und dem Arbeitsspeicher des Rechners basiert, auf dem der Server ausgeführt wird.	Der Standardwert ist 0.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
Älteste an einen Client übergebene Abrufdaten (Sekunden)	Gibt die Zeit in Sekunden an, die der Server zwischengespeicherte Daten verwendet, um die Anforderungen der auf Abruf erstellten Berichte zu erfüllen. Wenn der Server eine Anforderung empfängt, die mit Daten aus einer früheren Anforderung beantwortet werden kann und der seit Generierung der Daten verstrichene Zeitraum kürzer als der hier festgelegte Wert ist, verwendet der Server die Daten für die Beantwortung der nachfolgenden Anforderung erneut. Mit dem erneuten Verwenden von Daten auf diese Art und Weise wird die Systemleistung beträchtlich gesteigert, wenn mehrere Benutzer die gleichen Informationen benötigen. Berücksichtigen Sie beim Einstellen dieses Werts, wie wichtig es für Benutzer ist, aktuelle Daten zu erhalten. Wenn es äußerst wichtig ist, dass alle Benutzer aktuelle Daten empfangen (weil sich wichtige Daten vielleicht sehr häufig ändern), können Sie diese Art der erneuten Verwendung von Daten unterbinden, indem Sie den Wert auf Null setzen. **Hinweis** Diese Eigenschaft kann für ein Berichtsobjekt selbst festgelegt werden und je nach Bericht variieren. Die Servereinstellungen werden von den für das Berichtsobjekt festgelegten Werten überschrieben.	Der Standardwert ist 0.
Maximale Anzahl vorab gestarteter Prozesse	Legt die maximale Anzahl zuvor gestarteter untergeordneter Prozesse fest, die für den Server zulässig sind. Ein zu niedriger Wert führt dazu, dass der Server untergeordnete Prozesse erstellt, sobald Anforderungen generiert werden, was zu einer Wartezeit für den Benutzer führen kann. Ein zu hoher Wert kann dazu führen, dass Systemressourcen unnötigerweise durch untergeordnete Prozesse belegt werden, die sich im Leerlauf befinden.	Der Standardwert entspricht einem (1) untergeordneten Prozess.
Temporäres Verzeichnis	Gibt das Verzeichnis an, in dem temporäre Dateien bei Bedarf erstellt werden. **Hinweis** Wenn dieses Verzeichnis nicht über den erforderlichen Speicherplatz verfügt, können Leistungsprobleme auftreten.	%DefaultDataDir%/CrystalReportsProcessingServer/temp
Java-Klassenpfad	Der Name und der Pfad der vom Server angeforderten Java-Klassen.	%CommonJavaLibDir%/procCR.jar

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
Untergeordnete Java Virtual Machine-Argumente	Legt die Befehlszeilenargumente fest, die vom Server erstellten untergeordneten Prozessen bereitgestellt werden.	Dbusinessobjects.connectivity.directory=%CONNECTIONSERVER_DIR%,Dcom.businessobjects.mds.cs.ImplementationID=csEX

Tabelle 73: Einzelanmeldungsdienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Ablauf der Einzelanmeldung (Sekunden)	Gibt die Zeit in Sekunden an, die eine SSO-Verbindung vor Ablauf gültig ist.	Der Standardwert beträgt 86.400 Sekunden.

Eigenschaften von Crystal Reports 2013 Report Application Server

Hinweis

Wenn Sie eine beliebige dieser Eigenschaften bearbeiten, muss der Server neu gestartet werden, damit die Änderungen wirksam werden.

Tabelle 74: Eigenschaften des Diensts zum Anzeigen und Ändern von Crystal-Reports-2013-Berichten

Eigenschaft	Beschreibung	Standardwert
Berichtsaufträge können bis zum Schließen des Berichtsauftrags mit der Datenbank verbunden bleiben	Legt fest, ob der Berichtsauftrag mit der Datenbank verbunden bleibt, bis der Prozess ausgeführt wurde.	Der Standardwert lautet `FALSE`.
Suchdatengröße (Datensätze)	Legt fest, wie viele unterschiedliche Datensätze von der Datenbank zurückgegeben werden, wenn die Werte eines bestimmten Felds durchsucht werden. Die Daten werden zuerst aus dem Cache des Clients, falls verfügbar, und anschließend aus dem Cache des Servers abgerufen. Sind die Daten in keinem der Caches vorhanden, werden sie aus der Datenbank abgerufen.	Der Standardwert beträgt 100 Datensätze.
Zeitsperre für Verbindung im Leerlauf (Minuten)	Legt fest, wie viele Minuten der Report Application Server (RAS) auf Anforderungen von einem Client im Leerlauf wartet, bevor eine Zeitüberschreitung auftritt. Die Wahl eines zu niedrigen Werts kann bewirken, dass eine Benutzeranforderung zu früh geschlossen wird. Die Wahl eines zu hohen Werts kann sich auf die Skalierbarkeit des Servers auswirken (wenn beispielsweise das Objekt `ReportClientDocument` nicht explizit geschlossen wird, wartet der	Der Standardwert beträgt 30 Minuten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	Server unnötigerweise darauf, dass ein Auftrag im Leerlauf geschlossen wird).	
Stapelgröße (Datensätze)	Legt fest, wie viele Zeilen während jeder Datenübertragung von der Datenbank aus dem Ergebnissatz zurückgegeben werden. Beispiel: Wenn 500 Datensätze angefordert werden und die Eigenschaft "Stapelgröße" auf 100 Datensätze festgelegt ist, werden die Daten in fünf einzelnen Stapeln zu je 100 Zeilen zurückgegeben. Um die Leistung Ihres RAS zu optimieren und die geeignete Stapelgröße festzulegen, sollten Sie Ihre Netzwerkumgebung und Datenbank sowie die unterschiedlichen Anforderungstypen kennen.	Der Standardwert beträgt 100 Datensätze.
Anzahl der beim Anzeigen der Vorschau oder Regenerieren eines Berichts zu lesenden Datenbankdatensätze (-1 für ungeschränkt)	Legt die Anzahl der Datenbankdatensätze fest, die beim Anzeigen oder Regenerieren eines Berichts gelesen werden. Diese Einstellung begrenzt die Anzahl der Datensätze, die der Server aus der Datenbank abruft, wenn ein Benutzer eine Abfrage oder einen Bericht ausführt. Diese Einstellung ist sinnvoll, wenn Sie verhindern möchten, dass Benutzer Berichte auf Abruf ausführen, bei denen zu große Datensatzpakete zurückgegeben werden. Solche Berichte sollten zeitgesteuert verarbeitet werden, damit einerseits die Berichte den Benutzern schneller zur Verfügung gestellt werden können und andererseits die Belastung der Datenbank mit zu umfangreichen Abfragen verringert werden kann.	Der Standardwert beträgt 20.000 Datensätze.
Maximale Anzahl gleichzeitiger Berichtsaufträge (0 für unbeschränkt)	Gibt die maximale Anzahl unabhängiger Aufträge an, die gleichzeitig auf dem RAS ausgeführt werden dürfen.	Der Standardwert beträgt 75 Aufträge.
Älteste an einen Client übergebene Abrufdaten (Minuten)	Gibt an, wie viele Minuten ein Bericht auf Abruf zwischengespeicherte Berichtsdaten bereitstellt.	Der Standardwert beträgt 20 Minuten.
Temporäres Verzeichnis	Gibt das Verzeichnis an, in dem temporäre Dateien bei Bedarf erstellt werden. **Hinweis** Wenn dieses Verzeichnis nicht über den erforderlichen Speicherplatz verfügt, können Leistungsprobleme auftreten.	`%DefaultDataDir%/CrystalReportsRasServer/temp`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Tabelle 75: Einzelanmeldungsdienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Ablauf der Einzelanmeldung (Sekunden)	Gibt die Zeit in Sekunden an, die eine SSO-Verbindung vor Ablauf gültig ist.	Der Standardwert beträgt 86.400 Sekunden.

Eigenschaften des Crystal Reports 2013 Processing Servers

> **Hinweis**
>
> Wenn Sie eine beliebige dieser Eigenschaften bearbeiten, muss der Server neu gestartet werden, damit die Änderungen wirksam werden.

Tabelle 76: Eigenschaften des Crystal-Reports-2013-Verarbeitungsdiensts

Eigenschaft	Beschreibung	Standardwert
Zeitsperre für Auftrag im Leerlauf (Minuten)	Gibt an, wie viele Minuten der Crystal Reports Processing Server zwischen Anforderungen für einen bestimmten Auftrag wartet.	Der Standardwert beträgt 20 Minuten.
Maximale Lebensdauer von Aufträgen pro untergeordnetem Element	Gibt die maximale Anzahl von Aufträgen an, die jeder untergeordneter Prozess pro Lebensdauer verwalten kann.	Der Standardwert beträgt 1.000.
Viewer-Regenerierung gibt immer die aktuellsten Daten zurück	Legt fest, ob alle zwischengespeicherten Seiten ignoriert und neue Daten direkt aus der Datenbank abgerufen werden, wenn Benutzer einen Bericht explizit regenerieren. Legt fest, ob Berichtsdaten auf verschiedenen Clients gemeinsam verwendet werden. **Hinweis** Diese Eigenschaft kann für ein Berichtsobjekt selbst festgelegt werden und je nach Bericht variieren. Die Servereinstellungen werden von den für das Berichtsobjekt festgelegten Werten überschrieben. Um einen Wert für das Berichtsobjekt anzugeben, wählen Sie den Bericht in der CMC aus und klicken auf **Standardeinstellungen** > **Anzeigeserver-Gruppe**.	Der Standardwert lautet `FALSE`.
Berichtsdaten für Clients freigeben	Legt fest, ob Berichtsdaten auf verschiedenen Clients gemeinsam verwendet werden. Legt fest, ob Berichtsdaten auf verschiedenen Clients gemeinsam verwendet werden.	Der Standardwert lautet `TRUE`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	Hinweis Diese Eigenschaft kann für ein Berichtsobjekt selbst festgelegt werden und je nach Bericht variieren. Die Servereinstellungen werden von den für das Berichtsobjekt festgelegten Werten überschrieben.	
Zeitsperre für Verbindung im Leerlauf (Minuten)	Legt fest, wie viele Minuten der Crystal Reports Processing Server auf Anforderungen von einer Verbindung wartet, die sich im Leerlauf befindet. Der Standardwert muss normalerweise nicht geändert werden.	Der Standardwert beträgt 20 Minuten.
Maximale Anzahl gleichzeitiger Aufträge (0 für automatisch)	Gibt die maximale Anzahl unabhängiger Aufträge an, die gleichzeitig auf dem Crystal Reports Processing Server ausgeführt werden dürfen. Wenn der Wert dieser Eigenschaft auf "0" festgelegt wird, wendet der Server einen geeigneten Wert an, der auf der CPU und dem Arbeitsspeicher des Rechners basiert, auf dem der Server ausgeführt wird.	Der Standardwert ist 0.
Älteste an einen Client übergebene Abrufdaten (Sekunden)	Gibt die Zeit in Sekunden an, die der Server zwischengespeicherte Daten verwendet, um die Anforderungen der auf Abruf erstellten Berichte zu erfüllen. Wenn der Server eine Anforderung empfängt, die mit Daten aus einer früheren Anforderung beantwortet werden kann und der seit Generierung der Daten verstrichene Zeitraum kürzer als der hier festgelegte Wert ist, verwendet der Server die Daten für die Beantwortung der nachfolgenden Anforderung erneut. Mit dem erneuten Verwenden von Daten auf diese Art und Weise wird die Systemleistung beträchtlich gesteigert, wenn mehrere Benutzer die gleichen Informationen benötigen. Berücksichtigen Sie beim Einstellen dieses Werts, wie wichtig es für Benutzer ist, aktuelle Daten zu erhalten. Wenn es äußerst wichtig ist, dass alle Benutzer aktuelle Daten empfangen (weil sich wichtige Daten vielleicht sehr häufig ändern), können Sie diese Art der erneuten Verwendung von Daten unterbinden, indem Sie den Wert auf Null setzen. **Hinweis** Diese Eigenschaft kann für ein Berichtsobjekt selbst festgelegt werden und je nach Bericht variieren. Die Servereinstellungen werden von den für das Berichtsobjekt festgelegten Werten überschrieben.	Der Standardwert ist 0.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
Maximale Anzahl vorab gestarteter Prozesse	Legt die maximale Anzahl zuvor gestarteter untergeordneter Prozesse fest, die für den Server zulässig sind. Ein zu niedriger Wert führt dazu, dass der Server untergeordnete Prozesse erstellt, sobald Anforderungen generiert werden, was zu einer Wartezeit für den Benutzer führen kann. Ein zu hoher Wert kann dazu führen, dass Systemressourcen unnötigerweise durch untergeordnete Prozesse belegt werden, die sich im Leerlauf befinden.	Der Standardwert entspricht einem (1) untergeordneten Prozess.
Temporäres Verzeichnis	Gibt das Verzeichnis an, in dem temporäre Dateien bei Bedarf erstellt werden. **Hinweis** Wenn dieses Verzeichnis nicht über den erforderlichen Speicherplatz verfügt, können Leistungsprobleme auftreten.	%DefaultDataDir%/CrystalReports2013ProcessingServer/temp
Berichtsaufträge können bis zum Schließen des Berichtsauftrags mit der Datenbank verbunden bleiben	Legt fest, ob der Berichtsauftrag bis zum Schließen des Auftrags mit der Datenbank verbunden bleibt.	Der Standardwert lautet FALSE.
Anzahl der beim Anzeigen der Vorschau oder Regenerieren eines Berichts zu lesenden Datenbankdatensätze (0 für unbeschränkt)	Legt die Anzahl der Datenbankdatensätze fest, die beim Anzeigen oder Regenerieren eines Berichts gelesen werden. Diese Einstellung begrenzt die Anzahl der Datensätze, die der Server aus der Datenbank abruft, wenn ein Benutzer eine Abfrage oder einen Bericht ausführt. Diese Einstellung ist sinnvoll, wenn Sie verhindern möchten, dass Benutzer Berichte auf Abruf ausführen, bei denen zu große Datensatzpakete zurückgegeben werden. Solche Berichte sollten zeitgesteuert verarbeitet werden, damit einerseits die Berichte den Benutzern schneller zur Verfügung gestellt werden können und andererseits die Belastung der Datenbank mit zu umfangreichen Abfragen verringert werden kann.	Der Standardwert beträgt 20.000.

Tabelle 77: Einzelanmeldungsdienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Ablauf der Einzelanmeldung (Sekunden)	Gibt die Zeit in Sekunden an, die eine SSO-Verbindung vor Ablauf gültig ist.	Der Standardwert beträgt 86.400 Sekunden.

30.1.5 Analysis Services-Eigenschaften

Die Analysis Services-Kategorie umfasst den Adaptive Processing Server:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Tabelle 78: Multi-Dimensional Analysis Service-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Maximale Anzahl von Client-Sitzungen	Legt die maximale Anzahl von MDAS-Sitzungen fest, die gleichzeitig auf dem Server geöffnet sein können. Wenn die Anzahl von offenen Sitzungen diese Zahl erreicht, wird bei dem Versuch, weitere MDAS-Sitzungen zu starten, die Fehlermeldung "Server nicht verfügbar" angezeigt. Sie können diesen Wert ändern, um die Leistung des MDAS-Servers entsprechend Ihren Anforderungen und der verfügbaren Hardware zu optimieren. Das Erhöhen dieses Werts kann zu Leistungsproblemen auf dem MDAS-Server und der Datenbank führen. Eine vorsichtige Einschätzung des Standardwerts liegt bei 15 Sitzungen. Bei Installationen mit wenigen Benutzeranforderungen können Sie diesen Wert deutlich erhöhen, während Installationen mit umfangreichen Benutzeranforderungen einen niedrigeren Wert erfordern.	Der Standardwert beträgt 15. Der gültige Bereich liegt zwischen 1 und 100.
Maximale Anzahl an von einer Abfrage zurückgegebenen Zellen	Legt die Anzahl der Zellen fest, die in einer einzigen Abfrage an den Benutzer zurückgegeben werden. Der Benutzer kann keine Abfrage ausführen, die eine sehr große Anzahl von Zellen zurückgibt und dabei sehr viel Speicher beansprucht. Wenn der Benutzer dieses Zellengrenze überschreitet, wird eine Fehlermeldung angezeigt.	Der Standardwert ist 100.000 Zellen.
Die maximale Anzahl der Elemente, die beim Filtern zurückgegeben wird	Legt die Anzahl der abgerufenen Elemente fest, wenn nach Element gefiltert wird. Eine sehr große Anzahl von abgerufenen Elementen kann sehr viel Speicher beanspruchen.	Der Standardwert ist 100.000 Elemente.

Tabelle 79: BEx Web Applications-Diensteigenschaften

Eigenschaft	Beschreibung	Standardwert
Maximale Anzahl von Client-Sitzungen	Die maximale Anzahl der auf dem Dienst zulässigen Clientsitzungen.	Der Standardwert beträgt 15 Sitzungen.
SAP BW Mastersystem	Der Name der OLAP-Verbindung zum BW-System, die Sie in der BI-Plattform erstellt haben.	Der Standardwert lautet SAP_BW.
RFC-Destination des JCo-Servers	Der Name der RFC-Destination des JCo-Servers, den Sie im BW-System eingegeben haben.	Dieser Wert hat standardmäßig keinen Eintrag.
Gateway-Host des JCo-Servers	Der Name des Gateway-Hosts des JCo-Servers, den Sie im BW-System festgelegt haben.	Dieser Wert hat standardmäßig keinen Eintrag.
Gateway-Dienst des JCo-Servers	Der Name des Gateway-Diensts des JCo-Servers, den Sie im BW-System festgelegt haben.	Dieser Wert hat standardmäßig keinen Eintrag.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
Verbindungsanzahl des JCo-Servers	Gibt die Anzahl der automatisch erstellten Programme an, mit denen ABAP-Aufrufe von Java für den Dienst verarbeitet werden können.	Der Standardwert beträgt 3 Verbindungen.

30.1.6 Eigenschaften des Datenföderations-Diensts

Die Datenföderations-Dienstekategorie umfasst den Adaptive Processing Server:

Tabelle 80: Eigenschaften des Datenföderations-Diensts

Eigenschaft	Beschreibung	Standardwert
Max Verbindungen	Legt die maximale Anzahl der auf dem Server zulässigen Verbindungen fest.	Der Standardwert beträgt 32.767.
Poolgröße des Ausführungs-Threads	Legt die maximale Anzahl von Abfragen fest, die zu einem bestimmten Zeitpunkt parallel ausgeführt werden können.	Der Standardwert beträgt 10.
Standby-Zeitlimit für Verbindungen	Legt fest, nach wie vielen Sekunden eine nicht aktive Verbindung geschlossen wird.	Der Standardwert ist 10800 Sekunden.
Standby-Zeitlimit für Anweisungen	Legt fest, nach wie vielen Sekunden eine nicht aktive Abfrageanweisung geschlossen wird.	Der Standardwert ist 600 Sekunden.

30.1.7 Eigenschaften der Web-Intelligence-Dienste

Die Kategorie "Web-Intelligence-Dienste" umfasst die folgenden Server:

- Adaptive Processing Server
- Web Intelligence Processing Server

Einstellungen für den Adaptive Processing Server

Tabelle 81: Befehlszeilenparameter

Eigenschaft	Beschreibung	Standardwert
Bis Ebene aufklappen	Gibt die Ebene an, bis zu der Daten von BEx Querys abgerufen werden. Hierarchien werden standardmäßig nicht auf eine bestimmte Ebene erweitert. Ebene 00 ist immer die Standardebene. Sie können dieses Verhalten ändern, indem Sie diesen Parameter zur Befehlszeile hinzufügen, wenn der Wert jedoch zu hoch gesetzt wird, ruft Web Intelli-	`-Dsap.sl.bics.expandToLevel=n` n kann eine Ganzzahl zwischen 0 und 99 sein. Falls n=0 oder falls dieser Parameter nicht angegeben wird, verwenden die Hierarchien den Parameter "Bis Ebene aufklappen".

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	gence alle Hierarchiedaten ab, was sich auf die Leistung und Stabilität des Systems auswirken kann.	

Tabelle 82: Eigenschaften des Web-Intelligence-Überwachungsdienstes

Eigenschaft	Beschreibung	Standardwert
Überwachung aktivieren	Gibt an, ob die Überwachung für den Dienst aktiviert ist.	`TRUE`
Verzögerung der Überwachungsthread-Schleife (in Sekunden)	Gibt die Zeitspanne in Sekunden zwischen den Ping-Versuchen an, die der Dienst für Clients durchführt.	300
Zeitüberschreitung bei Bereinigung der standardmäßig überwachten Ressource (in Sekunden)	Gibt (in Sekunden) an, wie lange der Dienst auf einen inaktiven Client wartet, bevor er die Sitzung des Clients bereinigt.	1200
Zeitüberschreitung bei Austausch der standardmäßig überwachten Ressource (in Sekunden)	Gibt (in Sekunden) an, wie lange der Dienst auf einen inaktiven Client wartet, bevor er die Sitzung des Clients auf der Festplatte austauscht. Es wird empfohlen, einen Wert anzugeben, der kleiner als der für die Eigenschaft "Zeitüberschreitung bei Bereinigung der standardmäßig überwachten Ressource (in Sekunden)" angegebene ist.	600
Dienst-Profilerstellung aktivieren		`TRUE`
Dienst-Aktivitätsüberwachung aktivieren		`TRUE`

Tabelle 83: Eigenschaften des Visualisierungsdiensts

Eigenschaft	Beschreibung	Standardwert
Zeitlimit bei Bereinigung der Visualisierungs-Engine (in Sekunden)	Gibt (in Sekunden) an, wie lange der Dienst auf einen inaktiven Client wartet, bevor er die Sitzung des Clients bereinigt.	1200
Zeitlimit bei Austausch der Visualisierungs-Engine (in Sekunden)	Gibt (in Sekunden) an, wie lange der Dienst auf einen inaktiven Client wartet, bevor er die Sitzung des Clients auf der Festplatte austauscht. Es wird empfohlen, einen Wert anzugeben, der kleiner als der für die Eigenschaft **Zeitlimit bei Bereinigung der Visualisierungs-Engine (in Sekunden)** angegebene ist.	600

Tabelle 84: Eigenschaften des Rebean-Diensts

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Tabelle 85: Eigenschaften des Dokument-Wiederherstellungsdiensts

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Tabelle 86: Eigenschaften des DSL-Bridge-Diensts

Eigenschaft	Beschreibung	Standardwert
Zeitsperre zur Bereinigung der DSL-Bridge-Engine (in Sekunden)	Gibt (in Sekunden) an, wie lange der Dienst auf einen inaktiven Client wartet, bevor er die Sitzung des Clients bereinigt.	1200

Eigenschaften für Web Intelligence Processing Server

Die Eigenschaften für Web Intelligence Processing Server sind in folgende Dienste gruppiert:

- Information Engine-Dienst
- Web Intelligence Core
- Web Intelligence Processing
- Web Intelligence Common

Einstellungen für Grenzwerte werden in eigenen Tabellen beschrieben.

Tabelle 87: Eigenschaften des Information-Engine-Diensts

Eigenschaft	Beschreibung	Standardwert
Wertelisten-Cache aktivieren	Gibt an, ob das Zwischenspeichern von Wertelisten auf dem Web Intelligence Processing Server aktiviert ist.	`TRUE`
Batch-Größe für Wertelisten (Einträge)	Gibt die maximale Anzahl von Einträgen (bzw. Werten) für jeden Wertelisten-Batch an.	1000
Maximale Größe für benutzerdefinierte Sortierung (Einträge)	Gibt die maximale Anzahl von Einträgen in der benutzerdefinierten Sortierung an.	100
Maximale Größe für Universum-Cache (Universen)	Gibt die Anzahl der Universen an, die auf dem Web Intelligence Processing Server zwischengespeichert werden sollen.	20
Maximale Wertelistengröße (Einträge)	Gibt die maximale Anzahl von Einträgen (bzw. Werten) für jede Werteliste an.	50000

Tabelle 88: Eigenschaften des Web-Intelligence-Kerndiensts

Eigenschaft	Beschreibung	Standardwert
Zeitlimit vor Recycling (Sekunden)	Gibt an, wie viele Sekunden sich der Server im Leerlauf befinden darf, bevor er vom Server Intelligence Agent (SIA) gestoppt und neu gestartet wird, sobald die Gesamtanzahl der verarbeiteten Dokumente den mit der Eigenschaft **Ma-**	1200

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	ximale Anzahl der Dokumente vor dem Recycling festgelegten Wert überschreitet.	
Zeitsperre für Dokument im Leerlauf (Sekunden)	Legt die Zeitdauer in Sekunden fest, nach der die Web Intelligence Processing Server-Sitzung ausgelagert wird. Wenn der Client in diesem Zeitraum keine Anforderungen generiert, wird die Sitzung daher auf die Festplatte ausgelagert, um Ressourcen für eine aktive Sitzung freizugeben.	300 Der gültige Bereich geht von 100 bis 10000 Sekunden.
Intervall für Serverabfrage (Sekunden)	Gibt das Intervall in Sekunden an, das verstreichen muss, bevor der Server neue Threadanforderungen abfragt. In der Abfragephase führt der Server Bereinigungsaktionen aus, indem beispielsweise nicht verwendete Dokumente ausgelagert werden, um den Serverspeicher unter dem oberen Arbeitsspeicher-Grenzwert zu halten.	120
Maximale Anzahl der Dokumente pro Benutzer	Gibt die maximale Anzahl aktiver Sitzungen (Web-Intelligence-Dokumente) an, die jeweils mit einem Benutzer verknüpft werden können. Wenn der Wert 5 lautet, kann der Benutzer folglich bis zu fünf aktive Sitzungen gleichzeitig nutzen.	5 Der gültige Bereich geht von 1 bis 20.
Maximale Anzahl der Dokumente vor dem Recycling	Gibt an, wie viele Web-Intelligence-Dokumente verarbeitet werden können, bevor ein Server-Recycling in Betracht gezogen wird. Wenn die Anzahl der verarbeiteten Dokumente erreicht wurde und der Server sich im Leerlauf befindet, wird der Server beendet und vom Server Intelligence Agent (SIA) eine neue Instanz des Servers gestartet. Es gibt jedoch eine Verzögerung, bevor eine neue Serverinstanz gestartet wird. Diese Verzögerung wird durch die Eigenschaft **Zeitlimit vor Recycling** definiert.	50
Fehler für maximale Größe der Dokumentstruktur zulassen	Gibt an, ob die Eigenschaft `<Maximale Verbindungen>` eingeschränkt ist. Wenn diese Eigenschaft aktiviert wird, wird der für die Eigenschaft `<Maximale Verbindungen>` festgelegte Wert vom Server berücksichtigt. Andernfalls wird die Eigenschaft ignoriert.	`TRUE`
Zeitsperre für Verbindung im Leerlauf (Minuten)	Legt fest, wie viele Minuten der Server auf Anforderungen von einer Verbindung wartet, die sich im Leerlauf befindet. Ein zu niedriger Wert kann dazu führen, dass eine Anforderung vorzeitig geschlossen wird. Ein zu hoher Wert kann dazu führen, dass Anforderungen in die Warteschlange eingereiht werden, während der Server darauf wartet, dass Anforderungen im Leerlauf geschlossen werden.	20
Maximale Verbindungen	Legt die maximale Anzahl von Verbindungen fest, die gleichzeitig geöffnet sein können. Hierbei handelt es sich um einen ungefähren Wert. Inaktive Sitzungen, die ausgelagert werden, oder die Sitzung, die zum Analysieren der Anzahl der Sitzungen erstellt wird, werden bei Verwendung	50 Der gültige Bereich liegt zwischen 5 und 65.535.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	dieser Einstellung nicht gezählt. Wenn dieser Grenzwert erreicht wird und kein anderer Server für die Verarbeitung der Anforderung verfügbar ist, erhält der Benutzer eine Fehlermeldung. **Hinweis** Damit diese Eigenschaft vom Server berücksichtigt wird, muss die Eigenschaft `<Fehler für maximale Größe der Dokumentstruktur zulassen>` aktiviert sein.	
Speicheranalyse aktivieren	Gibt an, ob die Speicheranalyse aktiviert wird. Wenn diese Eigenschaft aktiviert ist, werden die folgenden Eigenschaften aktiviert und vom Server berücksichtigt: • `<Maximaler Grenzwert für Arbeitsspeicher>` • `<Oberer Grenzwert für Arbeitsspeicher>` • `<Unterer Grenzwert für Arbeitsspeicher>` Wenn der Prozessspeicher des Servers den Wert unter `<Oberer Grenzwert für Arbeitsspeicher>` überschreitet, ist als einziger Vorgang das Speichern von Dokumenten zulässig. Wenn der Prozessspeicher den Wert unter `<Maximaler Grenzwert für Arbeitsspeicher>` überschreitet, werden alle Vorgänge gestoppt und schlagen fehl.	`TRUE`
Unterer Grenzwert für Arbeitsspeicher (MB)	Gibt den unteren Grenzwert für die Arbeitsspeichernutzung an.	`3500`
Oberer Grenzwert für Arbeitsspeicher (MB)	Gibt den oberen Grenzwert für die Arbeitsspeichernutzung an.	`4500`
Maximaler Grenzwert für Arbeitsspeicher (MB)	Gibt den maximalen Grenzwert für die Arbeitsspeichernutzung an.	`6000`
APS-Serviceüberwachung aktivieren	Aktiviert die Überwachung des Servers durch den APS-Service, der vom Adaptive Processing Server gehostet wird.	`TRUE`
Zahl der Neuversuche bei APS-Service-Ping-Fehler	Legt fest, wie viele Male der Server versucht, den APS-Service zu erreichen, bevor er die Versuche einstellt.	3
Thread-Periode der APS-Serviceüberwachung	Gibt die Verzögerungszeit zwischen den Versuchen an, den APS-Service zu erreichen.	300
Protokolle für aktuelle Aktivität aktivieren	Gibt an, ob vollständige Ablaufverfolgungen in den Protokolldateien des Servers generiert werden.	`FALSE`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	Hinweis Diese Eigenschaft sollte nur zu Debugging-Zwecke bei der Behebung von Fehlern aktiviert werden. Ist während des normalen Betriebs auf `FALSE` eingestellt.	

Tabelle 89: Eigenschaften des Web-Intelligence-Verarbeitungsdiensts

Eigenschaft	Beschreibung	Standardwert
Verwendung der HTTP URL aktivieren	Legt fest, ob der Server auf remote gespeicherte Dateien zugreifen kann.	`TRUE`
Proxy-Wert	Legt die Adresse des Proxy-Servers Ihres Netzwerks fest. Ein Wert muss nur dann angegeben werden, wenn das Netzwerk über einen Proxy-Server verfügt und Sie versuchen, auf remote gespeicherte Dateien zuzugreifen.	Leer

Tabelle 90: Eigenschaften des gemeinsamen Web-Intelligence-Diensts

Eigenschaft	Beschreibung	Standardwert
Cache-Zeitsperre (Minuten)	Gibt an, nach wie vielen Minuten der Inhalt des Dokument-Caches gelöscht wird. Die Zeitsperre richtet sich jeweils nach dem Zeitpunkt des letzten Dokumentzugriffs.	4370
Bereinigungsintervall für Dokument-Cache (Minuten)	Gibt das Zeitintervall (in Minuten) an, in dem der Dokument-Cache durchsucht und mit den Einstellungen `<Maximale Größe für Dokument-Cache>`, `<Maximale Größe für Dokument-Cache-Reduzierung>` und `<Maximale Anzahl von Dokumenten im Cache>` abgeglichen wird.	120
Cache-Freigabe deaktivieren	Gibt an, ob die Cache-Freigabe deaktiviert ist. Die Cache-Freigabe ist standardmäßig aktiviert. Dies bedeutet, dass alle Web Intelligence Processing Server-Instanzen denselben Cache nutzen. Wenn Sie jedoch einen Cache pro Web Intelligence Processing Server-Instanz bevorzugen, sollten Sie diese Eigenschaft aktivieren.	`FALSE`
Dokument-Cache aktivieren	Gibt an, ob der Dokument-Cache aktiviert ist. Wenn die Eigenschaft aktiviert ist, können zeitgesteuerte Web-Intelligence-Dokumente vorab in den Cache geladen werden.	`TRUE`
Echtzeit-Cache aktivieren	Gibt an, ob der Echtzeit-Cache aktiviert ist. Wenn die Eigenschaft aktiviert ist, kann der Cache dynamisch geladen werden. Aus diesem Grund werden Web-Intelligence-Dokumente bei der Anzeige vom Web Intelligence Processing Server zwischengespeichert. Außerdem werden die Dokumente vom Server zwischengespeichert, wenn sie als zeitgesteuerte Aufträge ausgeführt werden, vorausgesetzt, der Pre-Cache wurde im Dokument aktiviert.	`TRUE`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
Maximale Größe für Dokument-Cache (KB)	Legt die maximale Größe des Dokument-Caches fest. Sobald dieser Grenzwert erreicht ist, wird der Dokument-Cache unter Berücksichtigung der Eigenschaft `<Maximale Größe für Dokument-Cache-Reduzierung>` gelöscht.	1000000
Maximale Größe für Dokument-Cache-Reduzierung (Prozent)	Legt den prozentualen Cache-Anteil fest, der geleert wird, damit neuere Aktionen und Ergebnisse im Cache gespeichert werden können. Dokumente mit der ältesten "letzten Zugriffsuhrzeit" werden gelöscht.	70
Maximale Zeichenstreamgröße (MB)	Gibt die maximale Größe des an den Web-Intelligence-Client gesendeten Zeichenstreams an. **Hinweis** Wenn der Wert der Eigenschaft **Maximale Zeichenstreamgröße** überschritten wird, wird das Web-Intelligence-Dokument nicht erstellt und eine Fehlermeldung an den Client gesendet.	5 Der gültige Bereich liegt zwischen 1 und 65.535 MB.
Maximale Binärstreamgröße (MB)	Gibt die maximale Größe eines an den Web-Intelligence-Client gesendeten Binärstreams in MB an. **Hinweis** Wenn der Wert der Eigenschaft **Maximale Binärstreamgröße** überschritten wird, wird das Web-Intelligence-Dokument nicht erstellt und eine Fehlermeldung an den Client gesendet.	50 Der gültige Bereich liegt zwischen 1 und 65.535 MB.
Verzeichnis für Bilder	Gibt den Speicherort des Bildverzeichnisses an.	Leer
Verzeichnis für Cache-Ausgabe	Gibt den Speicherort des Caches an.	Leer

Tabelle 91: Allgemeine Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Ablauf der Einzelanmeldung (Sekunden)	Gibt die Zeit in Sekunden an, die eine SSO-Verbindung vor Ablauf gültig ist.	86400

Weitere Informationen

Einstellungen für Grenzwerte für den Web Intelligence Server-Arbeitsspeicher [Seite 985]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

30.1.7.1 Einstellungen für Grenzwerte für den Web Intelligence Server-Arbeitsspeicher

In den folgenden Abschnitten wird erläutert, was auf einem Web-Intelligence-Server geschieht, wenn die Werte unter "Maximaler Grenzwert für Arbeitsspeicher", "Oberer Grenzwert für Arbeitsspeicher" oder "Unterer Grenzwert für Arbeitsspeicher" erreicht werden.

Maximaler Grenzwert für Arbeitsspeicher

Wenn **<Maximaler Grenzwert für Arbeitsspeicher>** erreicht wird, werden alle aktuellen Vorgänge abgebrochen.

Oberer Grenzwert für Arbeitsspeicher

Wenn **<Oberer Grenzwert für Arbeitsspeicher>** erreicht wird, werden die folgenden Serveraktionen ausgeführt, um Ressourcen freizugeben und den Server zu schützen:

- Der Server verhindert, dass neue Verbindungen hergestellt und andere Threads, die den Arbeitsspeicher beanspruchen, gestartet werden. Für Web-Intelligence-Dokumente ist nur die Option **Speichern** zulässig. Benutzer, die eine Aktion anfordern, für die eine Speicherzuweisung benötigt wird, erhalten die Meldung `Server ist ausgelastet` und werden angewiesen, ausstehende Änderungen zu speichern.
- Der Server aktiviert die Systembereinigung, um so viele Ressourcen freizugeben, dass die Menge des zugewiesenen Speichers unter den Wert der Eigenschaft **<Oberer Grenzwert für Arbeitsspeicher>** fällt.
- Der Server versucht, schreibgeschützte Dokumente zu löschen.
- Wenn während der Systembereinigung nicht genügend Arbeitsspeicher freigegeben werden konnte, beginnt der Server, Dokumente im *Ansichtsmodus* zu schließen. Der Server beginnt auf der Grundlage des LIFO-Protokolls, Dokumente zu schließen. Das aktuellste aktive Dokument wird zuerst aus dem Arbeitsspeicher gelöscht. Der Server schließt so lange Dokumente, bis die sichere Stufe erreicht ist, die auf der folgenden Berechnung basiert: **<Oberer Grenzwert für Arbeitsspeicher>** - (20%*(**<Oberer Grenzwert für Arbeitsspeicher>**)). Wenn die Eigenschaft "Oberer Grenzwert für Arbeitsspeicher (MB)" auf 4.500 MB festgelegt wird, würde die sichere Ebene beispielsweise wie folgt lauten:

  ```
  4500MB - .20*4500MB = 3600MB
  ```

- Wenn beim Schließen von Dokumenten im *Ansichtsmodus* nicht genügend Speicher freigegeben werden konnte, beginnt der Server, alle übrigen geöffneten Dokumente zu schließen, einschließlich der Dokumente im *Bearbeitungsmodus*. Der Server beginnt auf der Grundlage des LIFO-Protokolls, Dokumente zu schließen. Das aktuellste aktive Dokument wird zuerst aus dem Arbeitsspeicher gelöscht. Der Server schließt so lange Dokumente, bis die sichere Stufe erreicht ist, die auf der folgenden Berechnung basiert: **<Oberer Grenzwert für Arbeitsspeicher>** - (20%*(**<Oberer Grenzwert für Arbeitsspeicher>**)). Wenn die Eigenschaft "Oberer Grenzwert für Arbeitsspeicher (MB)" auf 4.500 MB festgelegt wird, würde die sichere Ebene beispielsweise wie folgt lauten:

  ```
  4500MB - .20*4500MB = 3600MB
  ```


© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Unterer Grenzwert für Arbeitsspeicher

Beim Erreichen des Wertes für `<Unterer Grenzwert für Arbeitsspeicher>` lagert der Server inaktive Dokumente auf die Festplatte aus, um zusätzlichen Arbeitsspeicher für aktive Dokumente zuzuweisen.

30.1.8 Eigenschaften der Dashboards-Dienste

Eigenschaften des Dashboards Cache Servers

Tabelle 92: Eigenschaften des Dashboards-Cache-Diensts

Eigenschaft	Beschreibung	Standardwert
Maximale Cache-Größe (KB)	Legt die Größe des Festplattenspeichers (in KB) fest, die zum Zwischenspeichern von Abfragen verwendet wird. Ein großes Cache kann erforderlich sein, wenn der Server eine große Anzahl von Abfragen oder sehr komplexe Abfragen verarbeiten muss.	Der Standardwert beträgt 256.000 KB.
Zeitüberschreitung für Verbindungen im Leerlauf (Minuten)	Gibt an, wie viele Minuten der Dashboards-Cache-Server auf eine Anforderung von einer Verbindung im Leerlauf wartet. Der Standardwert muss normalerweise nicht geändert werden.	Der Standardwert beträgt 15 Minuten.
Daten für Clients freigeben	Legt fest, ob Berichtsdaten auf verschiedenen Clients gemeinsam verwendet werden.	Der Standardwert lautet *TRUE*.
Älteste an einen Client übergebene Abrufdaten (Sekunden)	Gibt (in Sekunden) an, wie lange der Server zwischengespeicherte Daten verwendet, um die Anforderungen der auf Abruf erstellten Abfragen zu erfüllen. Wenn der Server eine Anforderung empfängt, die mit Daten aus einer früheren Anforderung beantwortet werden kann und der seit Generierung der Daten verstrichene Zeitraum kürzer als der hier festgelegte Wert ist, verwendet der Server die Daten für die Beantwortung der nachfolgenden Anforderung erneut. Mit dem erneuten Verwenden von Daten auf diese Art und Weise wird die Systemleistung beträchtlich gesteigert, wenn mehrere Benutzer die gleichen Informationen benötigen. Berücksichtigen Sie beim Einstellen dieses Werts, wie wichtig es für Benutzer ist, aktuelle Daten zu erhalten. Wenn es äußerst wichtig ist, dass alle Benutzer aktuelle Daten empfangen (weil sich wichtige Daten vielleicht sehr häufig ändern), können Sie diese Art der erneuten Verwendung von Daten unterbinden, indem Sie den Wert auf null setzen.	Der Standardwert beträgt 0 Sekunden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
	Hinweis Diese Eigenschaft kann im Berichtsobjekt selbst eingestellt werden. Im Berichtsobjekt angegebene Werte setzen die Servereinstellungen außer Kraft.	
Sicherheitscache-Zeitüberschreitung (Minuten)	Legt fest (in Minuten), wie lange der Server zwischengespeicherte Anmeldedaten, Abfrageeigenschaften und Datenbankverbindungsinformationen verwendet, um Anforderungen zu verarbeiten, bevor er den CMS abfragt.	Der Standardwert beträgt 20 Minuten.
Java VM-Argumente	Legt die Befehlszeilenargumente fest, die der JVM bereitgestellt werden können.	Xmx858M

Eigenschaften des Dashboards Processing Servers

Tabelle 93: Eigenschaften des Dashboards-Verarbeitungsdiensts

Eigenschaft	Beschreibung	Standardwert
Maximale Anzahl gleichzeitiger Aufträge	Gibt die maximale Anzahl unabhängiger Aufträge an, die gleichzeitig auf dem Server ausgeführt werden dürfen. Wenn der Wert dieser Eigenschaft auf "0" festgelegt wird, wendet der Server einen geeigneten Wert an, der auf der CPU und dem Arbeitsspeicher des Rechners basiert, auf dem der Server ausgeführt wird.	Der Standardwert ist 0.
Maximale Lebensdauer von Aufträgen pro untergeordnetem Element	Gibt die maximale Anzahl von Aufträgen an, die jeder untergeordneter Prozess pro Lebensdauer verwalten kann.	Der Standardwert ist 10000.
Maximale Anzahl vorab gestarteter untergeordneter Prozesse	Legt die maximale Anzahl zuvor gestarteter untergeordneter Prozesse fest, die für den Server zulässig sind. Ein zu niedriger Wert führt dazu, dass der Server untergeordnete Prozesse erstellt, sobald Anforderungen generiert werden, was zu einer Wartezeit für den Benutzer führen kann. Ein zu hoher Wert kann dazu führen, dass Systemressourcen unnötigerweise durch untergeordnete Prozesse belegt werden, die sich im Leerlauf befinden.	Der Standardwert ist 1.
Zeitsperre für Verbindung im Leerlauf (Minuten)	Legt fest, wie viele Minuten der Server auf Anforderungen von einer Verbindung wartet, die sich im Leerlauf befindet. Der Standardwert muss normalerweise nicht geändert werden.	Der Standardwert beträgt 15 Minuten.
Zeitsperre für Auftrag im Leerlauf (Minuten)	Gibt an, wie viele Minuten der Server zwischen Anforderungen für einen bestimmten Auftrag wartet.	Der Standardwert beträgt 15 Minuten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Eigenschaft	Beschreibung	Standardwert
Untergeordnete Java Virtual Machine-Argumente	Legt die Befehlszeilenargumente fest, die vom Server erstellten untergeordneten Prozessen bereitgestellt werden.	Xmx858M,Dswfinjection.lang.directory=%CommonJavaLibDir%,Dbusinessobjects.connectivity.directory=%CONNECTIONSERVER_DIR%

Tabelle 94: Einzelanmeldungsdienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Ablauf der Einzelanmeldung (Sekunden)	Gibt die Zeit in Sekunden an, die eine SSO-Verbindung vor Ablauf gültig ist.	Der Standardwert beträgt 86.400 Sekunden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

31 Anhang "Servermetrik"

31.1 Info zu Servermetriken (Anhang)

In diesem Anhang bezieht sich der Begriff "Server", sofern nichts anderes angegeben ist, auf SAP-BusinessObjects-Server und nicht auf den Rechner, auf dem die BI-Plattform installiert ist oder ausgeführt wird.

Servermetriken sind nicht auf Servern verfügbar, die nicht ausgeführt werden.

Neben den in diesem Anhang beschriebenen Metriken kann das Überwachungstool auf die folgenden Serverzustände überwachen:

Serverstatus	Beschreibung
Status	Der "Status" zeigt den allgemeinen Funktionsstatus eines Servers an. Es gibt zwei mögliche Werte: • 0 = Rot (Gefahr) • 1 = Gelb (Achtung) • 2 = Grün (fehlerfrei)
Status "Server aktiviert"	Dieser Status zeigt an, ob der Server aktiviert oder deaktiviert ist. Es gibt zwei mögliche Werte: • 0 = Deaktiviert • 1 = Aktiviert
Status "Server wird ausgeführt"	Dieser Status zeigt den allgemeinen Ausführungsstatus eines Servers an. Es gibt zwei mögliche Werte: • 0 = GESTOPPT • 1 = WIRD GESTARTET • 2 = WIRD INITIALISIERT • 3 = WIRD AUSGEFÜHRT • 4 = WIRD GESTOPPT • 5 = FEHLGESCHLAGEN • 6 = WIRD MIT FEHLERN AUSGEFÜHRT • 7 = WIRD MIT WARNUNGEN AUSGEFÜHRT

Hinweis

Weitere Informationen zu den Servereigenschaften und Metriken von SAP BusinessObjects Explorer finden Sie im *SAP BusinessObjects Explorer-Administratorhandbuch*.

Weitere Informationen

Analysieren der Servermetrik [Seite 389]

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

31.1.1 Allgemeine Servermetriken

Anhand der folgenden Metriken wird der Rechner beschrieben, auf dem der angegebene Server ausgeführt wird.

Tabelle 95: Rechnerspezifische Metriken

Metrik	Beschreibung
Rechnername	Der Hostname des Rechners, auf dem der Server ausgeführt wird.
Betriebssystem	Das Betriebssystem des Rechners, auf dem der Server ausgeführt wird.
CPU-Typ	Der CPU-Typ des Rechners, auf dem der Server ausgeführt wird. Diese Metrik ist nicht auf Adaptive Processing Servern oder Web Application Container Servern (WACS) verfügbar.
CPUs	Die Anzahl der dem Server zur Verfügung stehen CPUs. Bei Mehrkern-CPUs gibt diese Metrik möglicherweise die Anzahl der logischen CPUs anstatt der physischen Prozessoren an. Diese Metrik ist nicht auf Adaptive Processing Servern oder Web Application Container Servern (WACS) verfügbar.
RAM (MB)	Die Speichermenge in Megabyte, die auf dem Rechner zur Verfügung steht, auf dem der Server ausgeführt wird. Diese Metrik ist nicht auf Adaptive Processing Servern oder Web Application Container Servern (WACS) verfügbar.
Lokale Zeit	Die lokale Uhrzeit.
Festplattengröße (GB)	Die Größe der Festplatte in Gigabyte, auf der die BI-Plattform installiert ist. Diese Metrik ist nicht auf Adaptive Processing Servern oder Web Application Container Servern (WACS) verfügbar.
Belegter Speicherplatz (GB)	Die Menge in Gigabyte des belegten Speicherplatzes auf der Festplatte, auf der die BI-Plattform installiert ist. Dies beinhaltet Festplattenspeicher, der von anderen Programmen auf dem Rechner belegt ist, und nicht nur den von der BI-Plattform belegten Speicher. Diese Metrik ist nicht auf Adaptive Processing Servern oder Web Application Container Servern (WACS) verfügbar.

Die folgenden Metriken beschreiben den angegebenen SAP BusinessObjects-Server.

Tabelle 96: Serverspezifische Metriken

Metrik	Beschreibung
Name Server	Name und Portnummer des CMS-Servers, auf dem dieser Server seine Adresse veröffentlicht.
Registrierter Name	Der interne Name des Servers. Hierbei handelt es sich nicht um den Namen, der auf dem Bildschirm *Server* der CMC angezeigt wird.
Version	Die Version des Servers.
Startzeit	Der Zeitpunkt, an dem der Server das letzte Mal gestartet wurde.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
PID	Die eindeutige Prozess-ID für den Server. Die PID wird von dem Betriebssystem des Rechners erstellt, auf dem der Server ausgeführt wird. Der spezifische Server kann anhand der PID identifiziert werden.
Hostname	Eine kommagetrennte Liste der Hostnamen, die momentan vom Server verwendet werden.
Host-IP-Adresse	Eine kommagetrennte Liste der IP-Adressen, die vom Server auf Anforderungen überwacht wird.
Anforderungs-Port	Der Port, über den der Server Anforderungen von anderen Servern empfängt. Wenn der Server mehrere IP-Adressen auf Anforderungen überwacht, ist der Anforderungs-Port immer derselbe. Wenn andere Prozesse diesen Anforderungs-Port verwenden, wird der Server nicht gestartet. Stellen Sie sicher, dieser Port nicht von anderen Prozessen verwendet wird.
Ausgelastete Serverthreads	Die Anzahl an Serverthreads, die momentan eine Anforderung verarbeiten. Wenn diese Zahl der maximalen Thread-Pool-Größe des Servers entspricht, bedeutet dies, dass das System weitere Anforderungen nicht parallel verarbeiten kann und neue Anforderungen warten müssen, bis die beanspruchten Threads wieder verfügbar werden.

Tabelle 97: Audit-Metriken

Metrik	Beschreibung
Aktuelle Anzahl der Audit-Ereignisse in der Warteschlange	Die Anzahl der Audit-Ereignisse, die von einem überwachten Objekt aufgezeichnet wurden, die jedoch noch nicht vom CMS-Auditor abgerufen wurden. Wenn diese Zahl sich grenzenlos erhöht, könnte dies bedeuten, dass das Auditing nicht ordnungsgemäß konfiguriert wurde, oder dass das System stark ausgelastet ist und Audit-Ereignisse schneller generiert, als sie vom Auditor abgerufen werden können. **Hinweis** Zum Anhalten eines Servers ist dieser zunächst zu deaktivieren und dann zu warten, bis diese Metrik “0” erreicht. Andernfalls können Audit-Ereignisse in der Warteschlange verbleiben und erst dann in den Audit-Datenspeicher (ADS) gelangen, wenn der Server neu gestartet wird und der CMS die Ereignisse abruft.

Tabelle 98: Protokollierungsdienst-Metriken

Metrik	Beschreibung
Protokollierungsverzeichnis	Dieses Verzeichnis enthält die Protokolldateien für den Server .

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

31.1.2 Central Management Server-Metriken

In der folgenden Tabelle werden die Servermetriken beschrieben, die im Fenster *Metriken* für die Central Management Server angezeigt werden.

Tabelle 99: Central Management Server-Metriken

Metrik	Beschreibung
Verbindung zur Audit-Datenbank wurde hergestellt	Zeigt an, ob der CMS eine funktionierende Verbindung zur Audit-Datenbank hat. Der Wert "1" zeigt an, dass eine Verbindung besteht. Der Wert "0" zeigt an, dass keine Verbindung zur Audit-Datenbank besteht. Falls der CMS ein Auditor ist, muss dieser Wert "1" sein. Stellen Sie bei Festlegung auf "0" fest, warum keine Verbindung zur Audit-Datenbank hergestellt werden kann.
CMS-Auditor	Zeigt an, ob der CMS als Auditor fungiert. Der Wert "1" zeigt an, dass der CMS als Auditor fungiert. Der Wert "0" zeigt an, dass der CMS nicht als Auditor fungiert.
Name der Audit-Datenbankverbindung	Der Name der Audit-Datenbankverbindung Dies ist nicht unbedingt der Name der Audit-Datenbank selbst. Wenn diese Metrik leer ist, gibt sie an, dass keine Verbindung zur Audit-Datenbank hergestellt werden kann.
Name des Audit-Datenbankbenutzers	Der Name des Benutzerkontos, das zum Herstellen einer Verbindung zur Audit-Datenbank verwendet wird.
Letzter Aktualisierungstermin der Audit-Datenbank	Das aktuelle Datum und die aktuelle Uhrzeit, an dem der CMS erfolgreich gestartet wurde, um die Ereignisse eines Auditors abzurufen. Falls der CMS ein Auditor ist, muss diese Metrik eine Zeit anzeigen, die nah am Zeitpunkt des Ladens des Bildschirms "Metriken" liegt. Liegt der Wert über zwei Stunden vor der Zeit, zu der der Bildschirm geladen wird, kann dies auf ein nicht korrekt funktionierendes Auditing hindeuten.
Dauer des letzten Abrufzyklus (Sekunden) des Audit-Threads	Die Dauer des letzten Abrufzyklus in Sekunden. Dieser Wert zeigt die maximale Verzögerung für Ereignisdaten bis zum Eingang bei der Audit-Datenbank während des vorherigen Abrufzyklus an. • Ein Wert von weniger als 20 Sekunden gibt an, dass das System fehlerfrei ist. • Ein Wert zwischen 20 Minuten und 2 Stunden gibt an, dass das System ausgelastet ist. • Ein Wert größer als 2 Stunden gibt an, dass das System stark ausgelastet ist. Wenn dieser Status anhält, und die Verzögerung Ihnen zu lange erscheint, sollten Sie Ihre Implementierung so aktualisieren, dass alle Audit-Datenbanken Daten mit einer höheren Datenrate empfangen, oder die Anzahl der von Ihrem System verfolgten Audit-Ereignisse erhöhen.
Auslastung des Audit-Threads	Der Prozentsatz des Abrufzyklus, die der Auditor-CMS mit dem Abrufen von Daten von überwachten Objekten verbringt. Die restliche Zeit besteht in Pausen zwischen Abrufen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
	Wenn dieser Wert 100 % erreicht, erfasst der Auditor noch immer Daten von den überwachten Objekten, wenn der nächste Abruf beginnen soll. Dies kann zu Verzögerungen des Empfangs von Ereignissen durch die Audit-Datenbank führen. Wenn die Thread-Auslastung häufig 100 % erreicht und mehrere Tage bei dieser Rate bleibt, sollten Sie die Implementierung aktualisieren, damit die Audit-Datenbank Daten mit einer höheren Datenrate empfangen kann, oder die Anzahl der von Ihrem System verfolgten Audit-Ereignisse verringern.
Geclusterte CMS-Server	Eine semikolongetrennte Liste von Hostnamen und Portnummern der ausgeführten Central Management Server im Cluster
Anzahl der von Zugriffslizenzbenutzern eingerichteten Sitzungen	Gesamtanzahl der Sitzungen für Zugriffslizenzbenutzer.
Anzahl der von Namenslizenzbenutzern eingerichteten Sitzungen	Die Gesamtzahl der Sitzungen für Namenslizenzbenutzer.
Höchstanzahl an Benutzersitzungen seit dem Start	Die Höchstzahl gleichzeitiger Benutzersitzungen, die der CMS seit dem Start verwaltet hat.
Anzahl der von Servern eingerichteten Sitzungen	Die Anzahl gleichzeitiger Sitzungen, die BI-Plattform-Server mit dem CMS erstellt haben. Wenn diese Zahl größer als 250 ist, erstellen Sie einen zusätzlichen CMS.
Anzahl der von allen Benutzern eingerichteten Sitzungen	Die Anzahl gleichzeitiger Benutzersitzungen, die vom CMS verwaltet werden, wenn der Bildschirm *Metriken* geladen wird. Je größer die Anzahl, desto größer die Anzahl der Benutzer, die das System nutzen. Wenn diese Zahl größer als 250 ist, erstellen Sie einen zusätzlichen CMS.
Fehlgeschlagene Aufträge	Die Anzahl der fehlgeschlagenen Aufträge im System.
Ausstehende Aufträge	Die Anzahl der Aufträge, die zeitgesteuert verarbeitet werden sollen, aber nicht zur Ausführung bereit sind, da die geplante Zeit oder das geplante Ereignis noch nicht erreicht wurde.
Laufende Aufträge	Die Anzahl der gleichzeitig ausgeführten Aufträge.
Abgeschlossene Aufträge	Die Anzahl der abgeschlossenen Aufträge im System.
Wartende Aufträge	Die Anzahl der Aufträge im System, die zeitgesteuert verarbeitet werden sollen und auf freie Ressourcen warten.
Zugriffslizenzbenutzer-Lizenzen	Die Anzahl der durch den Schlüsselcode angezeigten Zugriffslizenzbenutzer-Lizenzen.
Namenslizenzbenutzer-Lizenzen	Die Anzahl der durch den Schlüsselcode angezeigten Namenslizenzbenutzer-Lizenzen
Build-Datum	Das Build-Datum des CMS.
Systemdatenbank-Verbindungsname	Der Name der CMS-Systemdatenbankverbindung. Dies ist nicht unbedingt der Name der CMS-Systemdatenbank.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
Systemdatenbank-Servername	Der Name des Servers, auf dem die CMS-Systemdatenbank ausgeführt wird. Dies ist nicht unbedingt der Name der CMS-Systemdatenbank.
Systemdatenbank-Benutzername	Der Name des Benutzerkontos, das zum Herstellen einer Verbindung zur CMS-Systemdatenbank verwendet wird.
Datenquellenname	Der Name der CMS-Systemdatenbankverbindung.
Build-Nummer	Die Build-Nummer des CMS. Anhand dieser Nummer kann die von Ihnen installierte Version von SAP BusinessObjects Business Intelligence ermittelt werden.
Produktversion:	Die Produktversion des CMS.
Ressourcenversion	Die Ressourcenversion des CMS.
Durchschnittliche Commit-Antwortzeit seit dem Start (ms)	Durchschnittliche Zeitdauer in Millisekunden, die der CMS zum Durchführen von Commit-Vorgängen seit dem Start des Servers gebraucht hat. Eine Reaktionszeit von über 1000 Millisekunden kann bedeuten, dass der CMS oder die CMS-Systemdatenbank angepasst werden muss.
Durchschnittliche Abfragenantwortzeit seit dem Start (ms)	Durchschnittliche Zeitdauer in Millisekunden, die der CMS zum Durchführen von Abfragevorgängen seit dem Start des Servers gebraucht hat. Eine Reaktionszeit von über 1000 Millisekunden kann bedeuten, dass der CMS oder die CMS-Systemdatenbank angepasst werden muss.
Längste Commit-Antwortzeit seit dem Start (ms)	Die längste Zeitdauer in Millisekunden, die der CMS zum Durchführen von Commit-Vorgängen seit dem Start des Servers gebraucht hat. Eine Reaktionszeit von über 10.000 ms deutet möglicherweise darauf hin, dass der CMS oder die CMS-Systemdatenbank angepasst werden muss.
Längste Abfragenantwortzeit seit dem Start (ms)	Längste Zeit (in ms), die der CMS seit dem Start des Servers für Abfragevorgänge gebraucht hat. Eine Reaktionszeit von über 10.000 ms deutet möglicherweise darauf hin, dass der CMS oder die CMS-Systemdatenbank angepasst werden muss.
Anzahl der Commits seit dem Start	Die Anzahl der Commits auf der CMS-Systemdatenbank seit dem Start des Servers.
Anzahl der Abfragen seit dem Start	Die Gesamtzahl der Datenbankabfragen seit dem Start des Servers. Ein große Anzahl deutet möglicherweise auf ein aktiveres oder stark ausgelastetes System hin.
Anzahl der Benutzeranmeldungen seit dem Start	Die Anzahl der Benutzeranmeldungen seit dem Start des Servers. Ein große Anzahl deutet möglicherweise auf ein aktiveres oder stark ausgelastetes System hin.
Eingerichtete Systemdatenbankverbindungen	Die Anzahl der Verbindungen mit der CMS-Systemdatenbank, die der CMS herstellen konnte. Wenn eine Verbindung unterbrochen wird, versucht der CMS, die Verbindung wiederherzustellen. Ist die Anzahl der eingerichteten Datenbankverbindungen durchweg geringer als die Anzahl der in der Eigenschaft **Systemdatenbankverbindungen angefragt**

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
	(Bereich *"Central Management Service"* des Fensters *Eigenschaften*) angegebenen Systemdatenbankverbindungen, deutet dies unter Umständen darauf hin, dass der CMS keine weiteren Verbindungen herstellen kann und dass das System nicht optimal funktioniert. Eine mögliche Lösung ist, den Datenbankserver so zu konfigurieren, dass mehr Datenbankverbindungen für den CMS zugelassen werden.
Momentan verwendete Systemdatenbankverbindungen	Die Anzahl der Verbindungen zu der CMS-Systemdatenbank, die der CMS momentan verwendet. Die Anzahl der momentan verwendeten Verbindungen ist möglicherweise kleiner oder gleich der Anzahl der eingerichteten Systemdatenbankverbindungen. Ist die Anzahl der eingerichteten Verbindungen für einige Zeit mit der Anzahl der verwendeten Verbindungen identisch, kann dies auf einen Engpass hinweisen. Eine Erhöhung des Werts für die Eigenschaft **Systemdatenbankverbindungen angefragt** im Fenster *Eigenschaften* kann zu einer Verbesserung der Leistung des CMS führen. Durch Anpassung der CMS-Systemdatenbank kann die Leistung ebenfalls verbessert werden.
Ausstehende Systemdatenbankanfragen	Die Anzahl an Anfragen an die CMS-Systemdatenbank, die auf eine verfügbare Verbindung warten. Ist diese Anzahl hoch, sollten Sie möglicherweise den Wert für die Eigenschaft **Systemdatenbankverbindungen angefragt** erhöhen. Durch Anpassung der CMS-Systemdatenbank kann die Leistung ebenfalls verbessert werden.
Anzahl der Objekte im CMS-System-Cache	Die Gesamtzahl der Objekte, die momentan im CMS-System-Cache gespeichert sind.
Anzahl der Objekte in CMS-Systemdatenbank	Die Gesamtzahl der Objekte, die momentan in der CMS-Systemdatenbank gespeichert sind.
Vorhandene Zugriffslizenzbenutzer-Konten	Die Gesamtzahl der vorhandenen Benutzer mit Zugriffslizenzen im Cluster.
Vorhandene Namenslizenzbenutzer-Konten	Die Gesamtzahl der vorhandenen Benutzer mit Namenslizenzen im Cluster.

31.1.3 Connection Server-Metriken

Die folgenden Metriken gelten speziell für den Connection Server.

Tabelle 100: Konnektivitätsdienst-Metriken

Metrik	Beschreibung
Datenquellen	Listet in einer Tabelle die Datenquellen auf, die über die Seite *Eigenschaften* aktiviert wurden. Zeigt die folgenden Informationen für jedes Netzwerkschicht- und Datenbankpaar an:

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
	• *Status* (*Geladen* oder *Fehlgeschlagen!*): aktueller Status des Treibers • *Verfügbare Verbindungen: Anzahl der Poolverbindungen, die verwendet werden können* • *Aufträge (CORBA): Anzahl der Aufträge, die gerade verarbeitet werden (2-Schichtimplementierung)* • *Aufträge (HTTP): Anzahl der Aufträge, die gerade verarbeitet werden (Webschichtimplementierung)* Hinweis Weitere Informationen über Verbindungspools finden Sie im *Datenzugriffshandbuch*.

31.1.4 Event Server-Metriken

In der folgenden Tabelle werden die Servermetriken beschrieben, die im Fenster *Metriken* für Event Server angezeigt werden.

Tabelle 101: Ereignisdienst-Metriken

Metrik	Beschreibung
Liste überwachter Dateien	Eine Tabelle, in der die vom Event Server überwachten Dateien aufgelistet sind. In der Spalte "Dateiname" werden der Name und der Pfad der Datei angezeigt. In der Spalte "Uhrzeit der letzten Benachrichtigung" wird der letzte Zeitstempel einer Abfrage des Servers angezeigt, die ergab, dass die Datei vorhanden ist.
Überwachte Dateien	Die Gesamtzahl der vom Event Server momentan überwachten Dateien.

31.1.5 File Repository Server-Metriken

In der folgenden Tabelle sind die Servermetriken beschrieben, die im Bildschirm *Metriken* für Input und Output File Repository Server angezeigt werden.

Tabelle 102: Dateispeicherdienst-Metriken

Metrik	Beschreibung
Aktive Dateien	Die Anzahl an Dateien im File Repository Server, auf die momentan zugegriffen wird.
Geschriebene Daten (MB)	Die Gesamtzahl an Megabyte, die in Dateien auf dem Server geschrieben wurden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
Gesendete Daten (MB)	Die Gesamtzahl an Megabyte, die aus Dateien auf dem Server gelesen wurden.
Liste aktiver Dateien	Eine Tabelle der Dateien im File Repository Server, auf die momentan zugegriffen wird.
Aktive Verbindungen	Die Gesamtzahl aktiver Verbindungen von Clients und zu anderen Servern.
Verfügbarer Speicherplatz im Root-Verzeichnis (GB)	Die Gesamtmenge des verfügbaren Speicherplatzes in Gigabyte auf der Festplatte, die die ausführbare Datei des Servers enthält.
Verfügbarer Speicherplatz im Root-Verzeichnis (GB)	Die Gesamtmenge des freien Speicherplatzes in Gigabyte auf der Festplatte, die die ausführbare Datei des Servers enthält.
Gesamtspeicherplatz im Root-Verzeichnis (GB)	Die Gesamtmenge des Speicherplatzes in Gigabyte auf der Festplatte, die die ausführbare Datei des Servers enthält.
Verfügbarer Speicherplatz im Root-Verzeichnis (%)	Die Menge des verfügbaren Speicherplatzes in Prozent auf der Festplatte, die die ausführbare Datei des Servers enthält.

31.1.6 Adaptive Processing Server-Metriken

In der folgenden Tabelle werden die Servermetriken beschrieben, die im Fenster *Metriken* für Adaptive Processing Server angezeigt werden.

Tabelle 103: Adaptive-Processing-Server-Metriken

Metrik	Beschreibung
Threads in Transportschicht	Die Gesamtzahl an Threads in allen Threadpools der Transportschicht.
Größe des Transportschicht-Threadpools	Die Gesamtzahl der gemeinsamen Transportschicht-Threads. Diese Threads können von den gehosteten Diensten auf dem Adaptive Processing Server verwendet werden.
Verfügbare Prozessoren	Die Anzahl der für die Java Virtual Machine (JVM), auf der der Server ausgeführt wird, verfügbaren Prozessoren.
Maximaler Arbeitsspeicher (MB)	Der maximale Umfang des Arbeitsspeichers in Megabyte, die die Java Virtual Machine verwendet.
Freier Arbeitsspeicher (MB)	Die Größe des Arbeitsspeichers in Megabyte, der der JVM zum Zuordnen von neuen Objekten zur Verfügung steht.
Gesamtarbeitsspeicher (MB)	Der Gesamtarbeitsspeicher der Java Virtual Machine in Megabyte. Dieser Wert kann sich im Laufe der Zeit ändern, abhängig von der Hostumgebung.
Prozentsatz der CPU-Auslastung (letzte 5 Minuten)	Der Prozentsatz der CPU-Gesamtauslastung durch den Server in den letzten 5 Minuten. Wenn z.B. ein einzelner Thread eine CPU eines Systems mit 4 CPUs vollständig nutzt, beträgt die Auslastung 25 %. Alle

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
	der JVM zugeordneten Prozesse werden berücksichtigt. Ein Wert, der größer als 80 % ist, kann einen CPU-Engpass anzeigen.
Prozentsatz der CPU-Auslastung (letzte 15 Minuten)	Der Prozentsatz der CPU-Gesamtauslastung durch den Server in den letzten 15 Minuten. Wenn z.B. ein einzelner Thread eine CPU eines Systems mit 4 CPUs vollständig nutzt, beträgt die Auslastung 25 %. Alle der JVM zugeordneten Prozesse werden berücksichtigt. Ein Wert, der größer als 70 % ist, kann einen Engpass anzeigen.
Prozentsatz der Systemstopps bei Speicherbereinigung (letzte 5 Minuten)	Der Prozentsatz der Systemstopps während der Ausführung von Speicherbereinigungen in den letzten 5 Minuten. In diesem Zustand wird die Ausführung aller APS-Dienste verhindert, während die Virtual Machine eine kritische Phase der Speicherbereinigung durchführt, für die ausschließlicher Zugriff erforderlich ist. Im Allgemeinen sollte ein niedriger, einstelliger Wert das Normalverhalten darstellen, selbst unter Belastung. Ein zweistelliger Wert über Nacht könnte auf ein Problem bezüglich niedrigem Durchsatz hinweisen, das ermittelt werden muss.
Prozentsatz der Systemstopps bei Speicherbereinigung (letzte 15 Minuten)	Der Prozentsatz der Systemstopps während der Ausführung von Speicherbereinigungen in den letzten 15 Minuten. In diesem Zustand wird die Ausführung aller APS-Dienste verhindert, während die Virtual Machine eine kritische Phase der Speicherbereinigung durchführt, für die ausschließlicher Zugriff erforderlich ist. Im Allgemeinen sollte ein niedriger, einstelliger Wert das Normalverhalten darstellen, selbst unter Belastung. Ein zweistelliger Wert über Nacht könnte auf ein Problem bezüglich niedrigem Durchsatz hinweisen, das ermittelt werden muss.
Seitenfehleranzahl bei Speicherbereinigung (letzte 5 Minuten)	Die Anzahl der Seitenfehler, die bei der Speicherbereinigung in den letzten fünf Minuten aufgetreten sind. Werte über 0 zeigen an, dass das System stark ausgelastet ist und nur wenig Speicher hat.
Seitenfehleranzahl bei Speicherbereinigung (letzte 15 Minuten)	Die Anzahl der Seitenfehler, die bei der Speicherbereinigung in den letzten 15 Minuten aufgetreten sind. Werte über 0 zeigen an, dass das System stark ausgelastet ist und nur wenig Speicher hat.
Anzahl der vollständigen Speicherbereinigungen	Die Anzahl der vollständigen Speicherbereinigung seit dem Start des Servers. Ein rascher Anstieg dieses Werts zeigt an, dass das System möglicherweise nur noch wenig Speicher hat.
Anzahl der JVM-Sperrkonflikte	Die Anzahl der synchronisierten Objekte, die über Threads verfügen, die auf Zugriff warten. Ein durchgehend über 0 liegender Wert deutet darauf hin, dass die Threads möglicherweise nicht erneut ausgeführt werden. Führen Sie einen Thread Dump aus, um mehr Informationen über die Ursache des Problems zu erhalten.
JVM-Debuginformationen	Debugging-Informationen über die SAP Java Virtual Machine, einschließlich Status, Port und verbundener Client, falls vorhanden.
JVM-Versionsinformationen	Versionsinformationen über die SAP Java Virtual Machine.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
Anzahl der JVM-Threads mit Deadlocks	Die Anzahl der Threads mit Deadlock. Werte, die über 0 liegen deuten darauf hin, dass die Threads möglicherweise nicht erneut ausgeführt werden. Führen Sie einen Thread Dump aus, um mehr Informationen über die Ursache des Problems zu erhalten.
JVM-Ablaufverfolgungsflags	Die Ablaufverfolgungsflags, die momentan für die JVM aktiviert sind. Dies zeigt den Umfang der Ablaufverfolgung der JVM an.
Dienste	Eine kommagetrennte Liste der vom Server gehosteten Dienste.

Tabelle 104: DSL-Bridge-Dienst-Metriken

Metrik	Beschreibung
DSLServiceMetrics.queryCount	Die Anzahl der offenen Datenanforderungen zwischen Clients und dem Dienst
DSLServiceMetrics.activeConnectionCount	Die Anzahl der derzeit offenen Verbindungen zwischen Clients und dem Dienst.
DSLServiceMetrics.activeSessionCount	Die Anzahl der derzeit offenen Sitzungen zwischen Clients und dem Dienst.
DSLServiceMetrics.activeOLAPConnectionCount	Die Anzahl der derzeit offenen Verbindungen zwischen OLAP-Clients und dem Dienst.

Tabelle 105: Metriken des Proxydiensts für das Client-Auditing

Metrik	Beschreibung
Anzahl der empfangenen Audit-Ereignisse seit Serverstart	Die Anzahl der Client-Audit-Ereignisse, die der Dienst seit seinem Start empfangen hat. Mithilfe dieser Metrik kann geprüft werden, ob der Client-Audit korrekt konfiguriert wurde. Werte größer “0” geben an, dass Audit-Ereignisse von Clients erfolgreich durch diesen Client-Audit-Dienst geroutet wurden.

Tabelle 106: Plattformsuchdienst-Metriken

Metrik	Beschreibung
Anzahl erfolgreicher Extrahierungsversuche seit Dienststart	Die Anzahl der erfolgreichen Versuche, Dokumente zu extrahieren, seit der Plattformsuchdienst gestartet wurde.
Zeitstempel der letzten Indexaktualisierung	Datum und Uhrzeit der letzten Indexaktualisierung.
Zeitstempel der letzten Inhaltsspeichergenerierung	Datum und Uhrzeit der Generierung des letzten Inhaltsspeichers.
Anzahl fehlgeschlagener Extrahierungsversuche seit Dienststart	Die Anzahl der fehlgeschlagenen Versuche, Dokumente zu extrahieren, seit der Plattformsuchdienst gestartet wurde.
Dienst verfügbar	TRUE, wenn der Dienst verfügbar ist. Ansonsten FALSE.
Indizierung wird ausgeführt	TRUE, wenn die Indizierung ausgeführt wird. Ansonsten FALSE.
Anzahl der indizierten Dokumente	Zeigt die Anzahl der Dokumente an, die seit dem Start des Dienstes indiziert wurden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Tabelle 107: Metriken von Multi-Dimensional Analysis Service

Metrik	Beschreibung
Anzahl an Sitzungen	Die aktuelle Anzahl der Verbindungen von MDAS-Clients zu dem Server.
Cube-Anzahl	Die Anzahl der Datenquellen, die Daten für die Verbindungen bereitstellen, deren Zeitlimit noch nicht überschritten wurde.
Abfrageanzahl	Die Anzahl der offenen Datenanforderungen zwischen MDAS-Clients und dem Server.

Tabelle 108: Datenföderations-Dienstmetriken

Metrik	Beschreibung
Anzahl der momentan ausgeführten Abfragen	Die Gesamtzahl der laufenden Abfragen (die Speicherkapazität beanspruchen oder nicht).
Anzahl der Verbindungen	Die Gesamtzahl der Benutzerverbindungen mit der Datenföderations-Abfrage-Engine.
Von Datenquellen übertragene Gesamtbyte	Die Menge der von den Datenquellen gelesenen Daten (in Byte)
Von Datenquellen übertragene Gesamtdatensätze	Die Gesamtzahl der von den Datenquellen gelesenen Einträge.
Von Abfrageausführung erzeugte Gesamtbyte	Die im Ergebnis von Abfragen erzeugte Datenmenge (in Byte).
Von Abfrageausführung erzeugte Gesamtdatensätze	Die Anzahl der im Ergebnis von Abfragen erzeugten Einträge (gesamt).
Anzahl der Speicher verbrauchenden Abfragen	Die Anzahl der laufenden Abfragen, die Speicherkapazität beanspruchen
Von Abfrageausführung verbrauchte Gesamtbyte an Speicher	Die momentan von laufenden Abfragen beanspruchte Speicherkapazität (in Byte).
Von Abfrageausführung verwendete Gesamtbyte auf Datenträger	Die momentan von laufenden Abfragen beanspruchte Festplattenkapazität (in Byte).
Anzahl der den Datenträger verwendenden Abfragen	Die Gesamtzahl der laufenden Abfragen, die Festplattenkapazität beanspruchen.
Anzahl der auf Ressourcen wartenden Abfragen	Die Gesamtzahl der laufenden Abfragen, die momentan zur Ausführung anstehen.
Anzahl der aktiven Threads	Die Gesamtzahl der für die Ausführung von Abfragen genutzten aktiven Threads.
Gesamtbyte des vom Metadaten-Cache verwendeten Speichers	Der Speicheranteil, der zum Ablegen von Metadaten, Statistik und Connector-Konfiguration im Cache beansprucht wird (in Byte).
Anzahl fehlgeschlagener Abfragen	Die Gesamtanzahl der fehlgeschlagenen Abfragen (Ausnahme ausgelöst).

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
Anzahl der Abfragen im Abfrageanalyseschritt	Die Gesamtzahl der momentan im Analyseschritt befindlichen laufenden Abfragen.
Anzahl der Abfragen im Abfrageoptimierungsschritt	Die Gesamtanzahl der momentan im Optimierungsschritt befindlichen laufenden Abfragen.
Anzahl der Abfragen im Abfrageausführungsschritt	Die Gesamtanzahl der momentan im Ausführungsschritt befindlichen laufenden Abfragen.
Anzahl der geladenen Connectors	Die Gesamtanzahl der im Dienst geladenen Connectors.
Anzahl der aktiven Verbindungen zu geladenen Connectors	Die Gesamtanzahl der aktiven zu den im Dienst geladenen Connectors.
Datenföderations-Dienst ist verfügbar	*TRUE*, wenn der Dienst verfügbar ist. Ansonsten *FALSCH*.

Tabelle 109: Konnektivitätsdienst-Metriken

Metrik	Beschreibung
Datenquellen	Auflisten der Datenquellen in einer Tabelle, die über die Seite *Eigenschaften* aktiviert wurden. Zeigt die folgenden Informationen für jedes Netzwerkschicht- und Datenbankpaar an: • Status (“Geladen” oder “Fehlgeschlagen”): der aktuelle Status des Treibers • Verfügbare Verbindungen: Anzahl der Poolverbindungen, die verwendet werden können • Aufträge (CORBA): Anzahl der Aufträge, die gerade verarbeitet werden (in einer 2-Schichtimplementierung) • Aufträge (HTTP): Anzahl der Aufträge, die gerade verarbeitet werden (in einer Webschichtimplementierung) Weitere Informationen über Verbindungspools finden Sie im *Datenzugriffshandbuch*.

Tabelle 110: Metriken des Überwachungsdienstes

Metrik	Beschreibung
Durchschnittliche Berechnungszeit für Kontrollmodulstatus für die letzten 15 Zyklen (msek)	Die durchschnittliche Zeit, die zur Berechnung des Kontrollmodulstatus über die letzten 15 Zyklen für diese Überwachungsdienstinstanz benötigt wurde.
Anzahl der von Benutzern erstellten Metriken	Gesamtzahl der von Benutzern erstellten Metriken im Cluster für alle Benutzer.
Anzahl an Kontrollmodulen	Die Gesamtzahl an Kontrollmodulen im Cluster, einschließlich deaktivierter und aktivierter Kontrollmodule.
serviceBean.monitoringAppPropEnabled	WAHR, wenn das Überwachungstool aktiviert ist. Ansonsten FALSCH. Diese Metrik entspricht der Einstellung auf der Seite "Überwachungstool-Eigenschaften" der CMC.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
Regenerierungsintervall für Überwachungsmetrik (Sekunden)	Das Regenerierungsintervall, das gerade von dieser Überwachungsdienstinstanz verwendet wird. Beim Dienststart wird diese Metrik auf die zu diesem Zeitpunkt vorhandene Einstellung auf der Seite "Überwachungstool-Eigenschaften" der CMC initialisiert, sodass die Metrik zu anderen Zeiten von der aktuellen Einstellung auf der CMC-Seite abweichen kann.
Dienst verfügbar	WAHR, wenn dieser Überwachungsdienst aktiv ist. Ansonsten FALSCH. Nur ein einziger Überwachungsdienst ist im Cluster aktiv.
Anzahl an Metriken mit Trend	Die Gesamtzahl der Metriken, die aktuell in der Überwachungsdatenbank aufgezeichnet werden.

Tabelle 111: BEx-Web-Applications-Dienstmetriken

Metrik	Beschreibung
Anzahl an Sitzungen	Die Gesamtzahl der Sitzungen, die in einem BEx-Web-Applications-Dienst aktiv sind.

31.1.7 Web Application Container Server-Metriken

In der folgenden Tabelle sind die Servermetriken beschrieben, die im Bildschirm *Metriken* für Web Application Container Server angezeigt werden.

> **Hinweis**
>
> Web Application Container Server verfügen auch über sämtliche Metriken, die im Abschnitt "Adaptive Processing Server-Metriken" beschrieben werden.

Tabelle 112: Web Application Container Server-Metriken

Metrik	Beschreibung
Liste der derzeit ausgeführten WACS-Konnektoren	Eine Liste der auf dem Server ausgeführen Konnektoren. Wenn nicht alle Konnektoren (HTTP, HTTPS und HTTP über Proxy) angezeigt werden, bedeutet dies, dass der Konnektor entweder nicht aktiviert oder dass er beim Start fehlgeschlagen ist.
WACS-Konnektor(en) bei Start fehlgeschlagen	Gibt an, ob fehlerhafte Konnektoren vorliegen. Falls ja, konnte mindestens ein Konnektor nicht gestartet werden. Falls nein, sind alle Konnektoren aktiv. Führen Sie einen Server nicht aus, wenn ein oder mehrere Konnektoren nicht gestartet werden konnten. Sie müssen auf dem Server nach dem Fehler suchen, um sicherzustellen, dass alle Konnektoren korrekt starten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitere Informationen

Adaptive Processing Server-Metriken [Seite 997]

31.1.8 Adaptive Job Server-Metriken

Tabelle 113: Job Server-Metriken

Metrik	Beschreibung
Eingegangene Auftragsanforderungen	Die Anzahl an Aufträgen, die auf dem Server ausgeführt worden sein sollten.
Gleichzeitige Aufträge	Die Anzahl an Aufträgen, die momentan auf dem Server ausgeführt werden. Bei einer hohen Anzahl ist der Server ausgelastet.
Maximalwertaufträge	Die maximale Anzahl gleichzeitiger Aufträge, die gleichzeitig auf dem Server ausgeführt wurden. Die Anzahl geht erst zurück, wenn der Server neu gestartet wird.
Fehler bei der Auftragserstellung	Die Anzahl der Aufträge, die auf dem Server fehlgeschlagen sind.
Temporäres Verzeichnis	Das Verzeichnis, in dem temporäre Dateien erstellt werden. Dies kann auf dem Bildschirm *Eigenschaften* für den Server angegeben werden. Wenn dieses Verzeichnis nicht über den erforderlichen Speicherplatz verfügt, können Probleme auftreten.
Standardeinstellungen für (erweitertes) Dateisystemziel gültig	*WAHR*, wenn der Server Dokumente an das im Fenster *Ziel* für den Server angegebene Dateisystemziel senden kann. Ansonsten *FALSCH*.
Standardeinstellungen für FTP-Ziel gültig	*WAHR*, wenn der Server Dokumente an das im Fenster *Ziel* für den Server angegebene FTP-Serverziel senden kann. Ansonsten *FALSCH*.
Standardeinstellungen für Posteingangsziel gültig	*WAHR*, wenn der Server Objekte an das im Fenster *Ziel* für den Server angegebene Posteingangsziel senden kann. Ansonsten *FALSCH*.
Standardeinstellungen für E-Mail-Ziel gültig	*WAHR*, wenn der Server Objekte an das im Fenster *Ziel* für den Server angegebene E-Mail-Ziel senden kann. Ansonsten *FALSCH*.
Dienste zur zeitgesteuerten Verarbeitung	Eine Tabelle mit den Diensten, die auf dem Server ausgeführt werden.
Untergeordnete Elemente	Eine Tabelle mit den untergeordneten Prozessen, die auf dem Server ausgeführt werden.
SAP-StreamWork-Standardeinstellungen für Ziel gültig	*WAHR*, wenn der Server Objekte an das im Fenster *Ziel* für den Server angegebene SAP-StreamWork-Ziel senden kann. Ansonsten *FALSCH*.

In der folgenden Tabelle werden die Metriken der einzelnen Dienste zur zeitgesteuerten Verarbeitung beschrieben, die auf dem Server ausgeführt werden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Tabelle 114: Zeitsteuerungsdienst-Metriken

Metrik	Beschreibung
Dienst zur zeitgesteuerten Verarbeitung	Der Name des Diensts.
Eingegangene Auftragsanforderungen	Die Anzahl an Aufträgen, die auf dem Dienst ausgeführt worden sein sollten.
Gleichzeitige Aufträge	Die Anzahl an Aufträgen, die momentan gleichzeitig auf dem Dienst ausgeführt werden. Bei einer hohen Anzahl ist der Dienst ausgelastet.
Maximalwertaufträge	Die maximale Anzahl gleichzeitiger Aufträge, die gleichzeitig auf dem Dienst ausgeführt wurden.
Maximal zulässige Anzahl gleichzeitiger Aufträge	Die Anzahl der auf dem Server zulässigen gleichzeitigen untergeordneten Prozesse (Unterprozesse). Dies kann auf dem Bildschirm *Eigenschaften* für den Server angegeben werden.
Fehler bei der Auftragserstellung	Die Anzahl der Aufträge, die auf dem Dienst fehlgeschlagen sind.

In der folgenden Tabelle werden die Metriken der einzelnen untergeordneten Prozesse beschrieben, die auf dem Server ausgeführt werden.

Tabelle 115: Metrik für untergeordnete Prozesse

Metrik	Beschreibung
Dienst zur zeitgesteuerten Verarbeitung	Der Name des untergeordneten Prozesses.
PID	Die ID des untergeordneten Prozesses.
Eingegangene Auftragsanforderungen	Die Anzahl an Aufträgen, die auf dem untergeordneten Prozess ausgeführt worden sein sollten.
Gleichzeitige Aufträge	Die Anzahl an Aufträgen, die momentan gleichzeitig auf dem untergeordneten Prozess ausgeführt werden. Normalerweise muss diese Zahl " 1" sein.
Maximalwertaufträge	Die maximale Anzahl gleichzeitiger Aufträge, die gleichzeitig auf dem untergeordneten Prozess ausgeführt wurden.
Maximal zulässige Anzahl von Aufträgen	Die zulässige Anzahl gleichzeitiger Aufträge für den untergeordneten Prozess.
Kommunikationsfehler	Die Anzahl an aufgetretenen Kommunikationsfehlern mit dem übergeordneten Adaptive Job Server. Bei einer großen Anzahl wird der untergeordnete Prozess neu gestartet.
Initialisieren	*WAHR*, wenn der untergeordnete Prozess gerade initialisiert wird. Ansonsten *FALSCH*.
Wird heruntergefahren	*WAHR*, wenn der untergeordnete Prozess gerade heruntergefahren wird. Ansonsten *FALSCH*.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

31.1.9 Crystal-Reports-Server-Metriken

Die folgende Tabelle enthält Beschreibungen der Servermetriken, die im Bildschirm *Metriken* für den Crystal Reports Processing Server und den Crystal Reports 2013 Processing Server angezeigt werden.

Tabelle 116: Crystal Reports Processing Server-Metriken

Metrik	Beschreibung
Offene Aufträge	Eine Tabelle, in der die Aufträge aufgelistet sind, die derzeit auf dem Server ausgeführt werden. Diese Tabelle enthält die ID und den Namen des Dokuments, den Namen des Benutzers, der den Auftrag ausführt, das Datum des letzten Zugriffs auf das Dokument und die Dauer der Ausführung des Auftrags.
Anzahl der verarbeiteten Anforderungen	Die Gesamtzahl der Anforderungen, die der Server seit seinem Start verarbeitet hat.
Anzahl der offenen Aufträge	Die Anzahl von Aufträgen, die der Server und seine untergeordneten Prozesse zurzeit verarbeiten.
Objekttyp	Der InfoObject-Typ, mit dem sich der Server vorrangig befasst. Der Wert dieser Metrik ändert sich nicht.
Durchschnittliche Verarbeitungszeit (ms)	Die durchschnittliche Zeit in Millisekunden, die der Server für die Verarbeitung der letzten 500 von ihm empfangenen Anforderungen benötigt hat. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Maximale Verarbeitungszeit (ms)	Die maximale Zeit in Millisekunden, die der Server für die Verarbeitung einer der letzten 500 Anforderungen benötigt hat. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Minimale Verarbeitungszeit (ms)	Die minimale Zeit in Millisekunden, die der Server für die Verarbeitung einer der letzten 500 Anforderungen benötigt hat. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Anzahl der Anforderungen in der Warteschlange	Die Anzahl der Anforderungen, die auf die Verarbeitung warten oder gerade verarbeitet werden. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Objekt-Dll-Name	Der Name des Verarbeitungs-Plug-ins für den Server. Der Wert dieser Metrik ändert sich nicht.
Anzahl der offenen Verbindungen	Die Anzahl der Verbindungen, die zurzeit zwischen dem Server und den Clients offen sind.
Anforderungsfehlerrate	Die Anzahl der Anforderungen, die der Server nicht verarbeiten konnte, als Prozentsatz der letzten 500 von ihm empfangenen Anforderungen.
Übertragene Daten (KB)	Die Gesamtmenge von Daten in Kilobyte, die seit dem Start des Servers an die Clients übertragen wurde.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
Anzahl der fehlgeschlagenen Anforderungen	Die Anzahl der Anforderungen, die der Server seit seinem Start nicht abschließen konnte.
Maximale Anzahl untergeordneter Prozesse	Die maximale Anzahl gleichzeitiger untergeordneter Prozesse, die auf dem Server zulässig sind.

In der folgenden Tabelle sind die Servermetriken beschrieben, die im Bildschirm *Metriken* für Crystal Reports Cache Server angezeigt werden.

Tabelle 117: Crystal Reports Cache Server-Metriken

Metrik	Beschreibung
Cache-Trefferquote (%)	Der Prozentsatz der letzten 500 Anforderungen, die mit zwischengespeicherten Daten verarbeitet wurden.
Verbundene Verarbeitungsserver	Eine Tabelle, in der die Crystal Reports Processing Server in Ihrer Implementierung aufgelistet sind. Die Tabelle enthält den Namen des Servers und die Anzahl der Verbindungen, die zurzeit zum Server offen sind.
Anzahl der verarbeiteten Anforderungen	Die Gesamtzahl der Anforderungen, die der Server seit seinem Start verarbeitet hat.
Objekttyp	Der InfoObject-Typ, mit dem sich der Server vorrangig befasst. Der Wert dieser Metrik ändert sich nicht.
Durchschnittliche Verarbeitungszeit (ms)	Die durchschnittliche Zeit in Millisekunden, die der Server für die Verarbeitung der letzten 500 von ihm empfangenen Anforderungen benötigt hat. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Maximale Verarbeitungszeit (ms)	Die maximale Zeit in Millisekunden, die der Server für die Verarbeitung einer der letzten 500 Anforderungen benötigt hat. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Minimale Verarbeitungszeit (ms)	Die minimale Zeit in Millisekunden, die der Server für die Verarbeitung einer der letzten 500 Anforderungen benötigt hat. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Anzahl der Anforderungen in der Warteschlange	Die Anzahl der Anforderungen, die auf die Verarbeitung warten oder gerade verarbeitet werden. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Objekt-Dll-Name	Der Name des Verarbeitungs-Plug-ins für den Server. Der Wert dieser Metrik ändert sich nicht.
Cache-Größe	Die Datenmenge in Kilobyte, der der Server derzeit auf der Festplatte zwischengespeichert hat.
Anzahl der offenen Verbindungen	Die Anzahl der Verbindungen, die zurzeit zwischen dem Server und den Clients offen sind.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
Übertragene Daten (KB)	Die Gesamtmenge von Daten in Kilobyte, die seit dem Start des Servers an die Clients übertragen wurde.

In der folgenden Tabelle sind die Servermetriken beschrieben, die auf dem Bildschirm *Metriken* für Crystal Reports 2013 Report Application Server angezeigt werden.

Tabelle 118: Crystal-Reports-2013-Report-Application-Server-Metriken

Metrik	Beschreibung
metric_currentdoccount Hinweis Diese Metrik wird als “document_s_” auf der Seite "Überwachung" in der CMC angezeigt.	Die Anzahl der Dokumente, die derzeit vom Server verarbeitet werden.
metric_totaldoccount Hinweis Diese Metrik wird als “document_s_” auf der Seite "Überwachung" in der CMC angezeigt.	Die Anzahl der Dokumente, die vom Server seit seinem Start verarbeitet wurden.
metric_currentagentthreadcount Hinweis Diese Metrik wird als “agent thread_s_” auf der Seite "Überwachung" in der CMC angezeigt.	Die Anzahl der Threads, die derzeit vom Server verarbeitet werden.
metric_totalagentthreadcount Hinweis Diese Metrik wird als “agent thread_s_” auf der Seite "Überwachung" in der CMC angezeigt.	Die Anzahl der Threads, die vom Server seit seinem Start verarbeitet wurden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

31.1.10 Web Intelligence Server-Metriken

Tabelle 119: Web-Intelligence-Verarbeitungsdienst-Metriken

Metrik	Beschreibung
Cache-Größe (KB)	Die aktuelle Datenmenge in Kilobyte, die im Cache gespeichert ist.
Maximale Anzahl von Dokumenten im Cache	Die Anzahl der Dokumente, die seit dem Serverstart aus dem Cache gelöscht wurden, da sie zu alt waren.
Anzahl an Cache-Höchstmarkierungen	Gibt an, wie oft das Cache auf dem Server seit dessen Start die zulässige maximale Größe erreicht hat.
CPU-Auslastung (%)	Der Prozentsatz der CPU-Gesamtzeit des Servers seit seinem Start.
CPU-Gesamtzeit (Sekunden)	Die CPU-Gesamtzeit in Sekunden des Servers seit seinem Start.
Anzahl an hohen Arbeitsspeicherschwellenwerten	Gibt an, wie häufig der hohe Arbeitsspeicherschwellenwert auf dem Server seit dessen Start erreicht wurde.
Anzahl an maximalen Arbeitsspeicherschwellenwerten	Gibt an, wie häufig der maximale Arbeitsspeicherschwellenwert auf dem Server seit dessen Start erreicht wurde.
Größe des virtuellen Speichers (MB)	Gesamtmenge des Speichers in Megabyte, die dem Server zugewiesen wurde.
Aktuelle Anzahl an Client-Aufrufen	Die aktuelle Anzahl von CORBA-Aufrufen, die vom Server verarbeitet werden.
Anzahl der Remote-Erweiterung-Fehler	Die Anzahl der fehlgeschlagenen Versuche des Servers, eine Verbindung mit einem Remote-Erweiterungsdienst herzustellen, der von einem Adaptive Processing Server gehostet wird.
Aktuelle Anzahl an Aufgaben	Die aktuelle Anzahl von Aufgaben, die auf dem Server ausgeführt werden.
Gesamtzahl an Client-Aufrufen	Die Gesamtzahl von CORBA-Aufrufen, die der Server seit seinem Start empfangen hat.
Gesamtzahl an Aufgaben	Die Gesamtzahl von Aufgaben, die auf dem Server seit seinem Start ausgeführt wurden.
Leerlaufzeit (Sekunden)	Die Zeit in Sekunden, die seit der letzten, vom Server von einem Client empfangenen Anforderung vergangen ist.
Aktuelle Anzahl der aktiven Sitzungen	Die aktuelle Anzahl der Sitzungen, die Anforderungen von Clients akzeptieren können.
Anzahl der aus dem Cache geöffneten Dokumente	Die Anzahl der Dokumente, für die das letzte Anforderungsergebnis direkt aus dem Cache gelesen wurde.
Anzahl der Dokumente	Die Anzahl der Dokumente, die derzeit auf dem Server offen sind.
Aktuelle Anzahl an Sitzungen	Die aktuelle Anzahl von Sitzungen, die auf dem Server erstellt wurden.
Anzahl des Dokument-Austauschs	Die Anzahl der Dokumente, für die ein Bereinigungs-Thread Austauschanforderungen geplant hat.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
Anzahl an ausgetauschten Dokumenten	Die Anzahl der Dokumente, die durch Austauschanforderungen getauscht wurden.
Anzahl der Zeitüberschreitungen bei Sitzung	Die Anzahl der Sitzungen mit Zeitüberschreitungen seit dem Start des Servers.
Gesamtzahl an Sitzungen	Die Anzahl der auf dem Server seit seinem Start erstellten Sitzungen.
Anzahl der Benutzer	Die Gesamtzahl der mit dem Server verbundenen Benutzer.
Anzahl der aktiven Threads	Die Anzahl der Threads, die Anforderungen bedienen, die vom Server empfangen wurden (Asynchronismus-Threadpool).
Gesamtanzahl der Threads	Die Gesamtanzahl der Threads, die erstellt wurden, seit der Server gestartet wurde (Asynchronismus-Threadpool).

31.1.11 Dashboard-Servermetriken

Tabelle 120: Dashboards-Processing-Server-Metriken

Metrik	Beschreibung
Offene Aufträge	Eine Tabelle, in der die Aufträge aufgelistet sind, die derzeit auf dem Server ausgeführt werden. Diese Tabelle enthält die ID und den Namen des Dokuments, den Namen des Benutzers, der den Auftrag ausführt, das Datum des letzten Zugriffs auf das Dokument und die Dauer der Ausführung des Auftrags.
Anzahl der verarbeiteten Anforderungen	Die Gesamtzahl der Anforderungen, die der Server seit seinem Start verarbeitet hat.
Anzahl der offenen Aufträge	Die Anzahl von Aufträgen, die der Server und seine untergeordneten Prozesse zurzeit verarbeiten.
Objekttyp	Der InfoObject-Typ, mit dem sich der Server vorrangig befasst. Der Wert dieser Metrik ändert sich nicht.
Durchschnittliche Verarbeitungszeit (ms)	Die durchschnittliche Zeit in Millisekunden, die der Server für die Verarbeitung der letzten 500 von ihm empfangenen Anforderungen benötigt hat. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Maximale Verarbeitungszeit (ms)	Die maximale Zeit in Millisekunden, die der Server für die Verarbeitung einer der letzten 500 Anforderungen benötigt hat. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Minimale Verarbeitungszeit (ms)	Die minimale Zeit in Millisekunden, die der Server für die Verarbeitung einer der letzten 500 Anforderungen benötigt hat. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
Anzahl der Anforderungen in der Warteschlange	Die Anzahl der Anforderungen, die auf die Verarbeitung warten oder gerade verarbeitet werden. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Objekt-Dll-Name	Der Name des Verarbeitungs-Plug-ins für den Server. Der Wert dieser Metrik ändert sich nicht.
Anzahl der offenen Verbindungen	Die Anzahl der Verbindungen, die zurzeit zwischen dem Server und den Clients offen sind.
Anforderungsfehlerrate	Die Anzahl der Anforderungen, die der Server nicht verarbeiten konnte, als Prozentsatz der letzten 500 von ihm empfangenen Anforderungen.
Übertragene Daten (KB)	Die Gesamtmenge von Daten in Kilobyte, die seit dem Start des Servers an die Clients übertragen wurde.
Anzahl der fehlgeschlagenen Anforderungen	Die Anzahl der Anforderungen, die der Server seit seinem Start nicht abschließen konnte.
Maximale Anzahl untergeordneter Prozesse	Die maximale Anzahl gleichzeitiger untergeordneter Prozesse, die auf dem Server zulässig sind.

Tabelle 121: Cache Server-Metriken

Metrik	Beschreibung
Cache-Trefferquote (%)	Der Prozentsatz der letzten 500 Anforderungen, die mit zwischengespeicherten Daten verarbeitet wurden.
Verbundene Verarbeitungsserver	Eine Tabelle, in der die Dashboards Processing Server in Ihrer Implementierung aufgelistet sind. Die Tabelle enthält den Namen des Servers und die Anzahl der Verbindungen, die zurzeit zum Server offen sind.
Anzahl der verarbeiteten Anforderungen	Die Gesamtzahl der Anforderungen, die der Server seit seinem Start verarbeitet hat.
Objekttyp	Der InfoObject-Typ, mit dem sich der Server vorrangig befasst. Der Wert dieser Metrik ändert sich nicht.
Durchschnittliche Verarbeitungszeit (ms)	Die durchschnittliche Zeit in Millisekunden, die der Server für die Verarbeitung der letzten 500 von ihm empfangenen Anforderungen benötigt hat. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Maximale Verarbeitungszeit (ms)	Die maximale Zeit in Millisekunden, die der Server für die Verarbeitung einer der letzten 500 Anforderungen benötigt hat. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Minimale Verarbeitungszeit (ms)	Die minimale Zeit in Millisekunden, die der Server für die Verarbeitung einer der letzten 500 Anforderungen benötigt hat. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Metrik	Beschreibung
Anzahl der Anforderungen in der Warteschlange	Die Anzahl der Anforderungen, die auf die Verarbeitung warten oder gerade verarbeitet werden. Wenn diese Zahl durchgängig hoch ist und weiter steigt, kann es sinnvoll sein, zusätzliche Server auf anderen Rechnern zu erstellen.
Objekt-Dll-Name	Der Name des Verarbeitungs-Plug-ins für den Server. Der Wert dieser Metrik ändert sich nicht.
Cache-Größe (KB)	Die Datenmenge in Kilobyte, der der Server derzeit auf der Festplatte zwischengespeichert hat.
Anzahl der offenen Verbindungen	Anzahl der Verbindungen zu Clients, die derzeit offen sind.
Übertragene Daten (KB)	Die Gesamtmenge von Daten in Kilobyte, die seit dem Start des Servers an die Clients übertragen wurde.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

32 Anhang "Server- und Knotenplatzhalter"

32.1 Server- und Knotenplatzhalter

Mit Ausnahme von *%SERVER_FRIENDLY_NAME%* und *%SERVER_NAME%* gelten diese Platzhalter für alle Server auf demselben Knoten.

Tabelle 122: Platzhalter

Platzhalter	Beschreibung	Standardwerte
%AuditingDatabaseConnection%	Die vom CMS verwendete Audit-Datenbankverbindung.	Dieser Wert wird während der Installation festgelegt.
%AuditingDatabaseDriver%	Der Typ des Datenbanktreibers für die Verbindung zur Audit-Datenbank.	Unter Windows lautet der Standardwert sqlserverauditdbss.
%BINDIR%	Der Ordner, in dem die 64-Bit-Binärdateien von SAP BusinessObjects Business Intelligence gespeichert sind.	Unter Windows `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. Unter UNIX `<INSTALLVERZ>/sap_bobj/enterprise_xi40/<Plattform>/`
%BINDIR32%	Der Ordner, in dem die 32-Bit-Binärdateien von SAP BusinessObjects Business Intelligence gespeichert sind.	Unter Windows `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Unter UNIX `<INSTALLVERZ>/sap_bobj/enterprise_xi40/<Plattform>/`
%CACHESERVER_EXE%	Der Name der ausführbaren Datei für den Crystal Reports Cache Server.	Unter Windows: `crcache.exe`. Unter Unix: `boe_crcached.bin`
%CMS_EXE%	Der Name der ausführbaren Datei für den Central Management Server.	Unter Windows: `cms.exe`. Unter UNIX: `boe_cmsd`.
%CONNECTIONSERVER32_EXE%	Der Name der ausführbaren Datei für den 32-Bit-Connection Server.	Unter Windows: `ConnectionServer32.exe`. Unter UNIX: `ConnectionServer32`.
%CONNECTIONSERVER_DIR%	Der Stammordner des Connection Server.	Unter Windows `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer`. Unter UNIX `<INSTALLVERZ>/sap_bobj/enterprise_xi40/dataAccess/connectionServer`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Platzhalter	Beschreibung	Standardwerte
%CONNECTIONSERVER_EXE%	Der Name der ausführbaren Datei für den 64-Bit-Connection Server.	Unter Windows: `ConnectionServer.exe`. Unter UNIX: `ConnectionServer`.
%CR2013_BINDIR%	Das Verzeichnis, in dem sich die Server-Binärdateien von Crystal Reports 2013 befinden.	Unter Windows **<INSTALLVERZ>**`\SAP BusinessObjectsEnterprise XI 4.0\win32_x86`. Unter UNIX sieht das Verzeichnis in etwa so aus: **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`.
%CR2013_DefaultWorkingDir%	Das Standardarbeitsverzeichnis für Crystal-Reports-2013-Server.	Unter Windows **<INSTALLVERZ>**`\SAP BusinessObjectsEnterprise XI 4.0\win32_x86`. Unter UNIX sieht das Verzeichnis in etwa so aus: **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`.
%CRYSTALRAS_EXE%	Der Name der ausführbaren Datei für den Report Application Server.	Unter Windows: `crystalras.exe`. Unter UNIX: `boe_crystalrasd`.
%CR_ODBCINI%	Name und Pfad, in dem die Datei `.odbc.ini` gespeichert ist.	Unter UNIX **<INSTALLVERZ>**`/bobje/odbc.ini`. Unter Windows ist dies eine leere Zeichenfolge.
%CommonJavaBundlesDir%	Der Ordner, indem die gemeinsamen OSGI-Bündel gespeichert sind.	Unter Windows **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\java\lib\bundles`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/java/lib/bundles`.
%CommonJavaLibDir%	Der Ordner, in dem die gemeinsamen Java-Bibliotheken gespeichert sind.	Unter Windows **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\java\lib`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/java/lib`.
%DLLEXT%	Die Standarderweiterung einer `.dll`- oder `.so`-Datei.	Unter Windows: `.dll`. Unter UNIX: `.so`.
%DLLPATH%	Der Name der Umgebungsvariablen auf dem Rechner, auf dem SAP BusinessObjects Business Intelligence installiert ist. Diese Umgebungsvariable gibt die Verzeichnisse an, die	Unter Windows: “Path”. Unter UNIX: “LD_LIBRARY_PATH”.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Platzhalter	Beschreibung	Standardwerte
	der Interpreter nach ausführbaren Dateien durchsucht.	
%DLLPATH32%	Auf 32-Bit-Solaris-Systemen: Der Name der Umgebungsvariablen auf dem Rechner, auf dem SAP BusinessObjects Business Intelligence installiert ist. Diese Umgebungsvariable gibt die Verzeichnisse an, die der Interpreter nach ausführbaren Dateien durchsucht.	Auf Solaris-Rechnern: “LD_LIBRARY_PATH_32”. Dieser Platzhalter ist unter anderen Betriebssystemen eine leere Zeichenfolge.
%DLLPATH64%	Auf 64-Bit-Solaris-Systemen: Der Name der Umgebungsvariablen auf dem Rechner, auf dem SAP BusinessObjects Business Intelligence installiert ist. Diese Umgebungsvariable gibt die Verzeichnisse an, die der Interpreter nach ausführbaren Dateien durchsucht.	Auf Solaris-Rechnern: “LD_LIBRARY_PATH_64”. Dieser Platzhalter ist unter anderen Betriebssystemen eine leere Zeichenfolge.
%DLLPREFIX%	Das Standardpräfix einer `.dll`- oder `.so`-Datei.	Unter UNIX: “lib”. Dieser Platzhalter ist unter Windows-Betriebssystemen eine leere Zeichenfolge.
%DLLPRELOAD%	Der Name der LD_PRELOAD-Umgebungsvariablen für die Plattform.	Unter UNIX: *LD_PRELOAD*. Dieser Platzhalter ist unter Windows-Betriebssystemen eine leere Zeichenfolge.
%DLLPRELOAD32%	Der Name der LD_PRELOAD-Umgebungsvariablen auf 32-Bit-AIX-Systemen.	Unter AIX: *LDR_PRELOAD*. Dieser Platzhalter ist auf anderen Rechnern eine leere Zeichenfolge.
%DLLPRELOAD64%	Der Name der LD_PRELOAD-Umgebungsvariablen auf 64-Bit-AIX-Systemen.	Unter AIX: *LDR_PRELOAD64*. Dieser Platzhalter ist auf anderen Rechnern eine leere Zeichenfolge.
%DP%	Das Pfadtrennzeichen.	Unter Windows: “;”. Unter UNIX: “:”.
%DefaultAuditingDir%	Das Verzeichnis, in das temporäre Audit-Dateien geschrieben werden. Damit die optimale Leistung gewährleistet werden kann, sollte sich der Speicherort auf dem lokalen Laufwerk des Servers befinden.	Unter Windows `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\Auditing`. Unter UNIX `<INSTALLVERZ>/sap_bobj/data/Auditing/`.
%DefaultDataDir%	Das temporäre Verzeichnis, das vom Job Server verwendet wird.	Unter Windows `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\Data`. Unter UNIX `<INSTALLVERZ>/sap_bobj/data/`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Platzhalter	Beschreibung	Standardwerte
%DefaultInputFRSDir%	Der Stammordner des Input File Repository Servers.	Unter Windows **<INSTALLVERZ>** `\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/data/frsinput`.
%DefaultLoggingDir%	Der Verzeichnispfad, in dem die Protokolldateien gespeichert sind.	Unter Windows **<INSTALLVERZ>** `\SAP BusinessObjects Enterprise XI 4.0\logging`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/logging`.
%DefaultOutputFRSDir%	Der Stammordner des Output File Repository Servers.	Unter Windows **<INSTALLVERZ>** `\SAP BusinessObjects Enterprise XI 4.0\FileStore\Output`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/data/frsoutput`.
%DefaultWorkingDir%	Das Arbeitsverzeichnis für 64-Bit-Server	Unter Windows **<INSTALLVERZ>** `\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/`**<Plattform>**.
%DefaultWorkingDir32%	Das Arbeitsverzeichnis für 32-Bit-Server.	Unter Windows **<INSTALLVERZ>** `\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/`**<Plattform>**.
%EPM_LD_PRELOAD_ONCE%	Der Name der LD_PRELOAD_ONCE-Umgebungsvariablen für die Plattform.	$LD_PRELOAD_ONCE$
%EVENTSERVER_EXE%	Der Name der ausführbaren Datei für den Event Server.	Unter Windows: `EventServer.exe`. Unter UNIX: `boe_eventsd`.
%EXEEXT%	Die Standarderweiterung von ausführbaren Dateien.	Unter Windows: `.exe`. Dieser Platzhalter ist unter UNIX nicht verfügbar.
%EXEPATH%	Der Name der Umgebungsvariablen auf dem Rechner, auf dem SAP BusinessObjects Business Intelligence installiert ist. Diese Umgebungsvariable gibt die Verzeichnisse an, die der Interpreter nach ausführbaren Dateien durchsucht.	Unter Windows: “Path”. Unter UNIX: “PATH”.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Platzhalter	Beschreibung	Standardwerte
%EnterpriseDir%	Der Speicherort, an dem die 64-Bit-Plattform SAP BusinessObjects Business Intelligence installiert ist.	Unter Windows **<INSTALLVERZ>** `\SAP BusinessObjects Enterprise XI 4.0\`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/`.
%EnterpriseDir32%	Der Speicherort, an dem die 32-Bit-Plattform SAP BusinessObjects Business Intelligence installiert ist.	Unter Windows **<INSTALLVERZ>** `\SAP BusinessObjects Enterprise XI 4.0\`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/`.
%ExternalJavaLibDir%	Der Ordner, in dem die externen Java-Bibliotheken von Drittanbietern gespeichert sind.	Unter Windows **<INSTALLVERZ>** `\SAP BusinessObjects Enterprise XI 4.0\java\lib\external`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/java/lib/external`.
%FILESERVER_EXE%	Der Name der ausführbaren Datei für den File Server.	Unter Windows: `fileserver.exe`. Unter UNIX: `boe_filesd`.
%HOARD_PATH%	Der Speicherort des Speichermanagers.	Er ist standardmäßig leer.
%HOARD_PRELOAD%	Gibt an, ob der Speichermanager vorab geladen werden soll.	Er ist standardmäßig leer.
%INSTALLROOTDIR%	Der Ordner, in dem die 64-Bit-Plattform SAP BusinessObjects Business Intelligence installiert ist.	Dieser Wert wird während der Installation festgelegt.
%INSTALLROOTDIR32%	Der Ordner, an dem die 32-Bit-Plattform SAP BusinessObjects Business Intelligence installiert ist.	Dieser Wert wird während der Installation festgelegt.
%IntroscopeAgentEnableInstrumentation%	Gibt an, ob die Instrumentation für Java-Server, die den Introscope Agent Enterprise Manager verwenden, aktiviert ist.	Die möglichen Werte TRUE oder FALSE richten sich danach, ob der Introscope Agent Enterprise Manager bei der Installation von SAP BusinessObjects Business Intelligence aktiviert war.
%IntroscopeAgentEnterpriseManagerHost%	Der Hostname des Introscope Agent Enterprise Managers, an den die Instrumentationsdaten gesendet werden.	Dieser Wert wird während der Installation festgelegt.
%IntroscopeAgentEnterpriseManagerPort%	Der Port des Introscope Agent Enterprise Managers, an den die In-	Dieser Wert wird während der Installation festgelegt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Platzhalter	Beschreibung	Standardwerte
	strumentationsdaten gesendet werden.	
%IntroscopeAgentEnterpriseManagerTransport%	Der Transport, der zum Senden der Instrumentationsdaten an den Introscope Agent Enterprise Manager verwendet wird. Zulässige Werte sind: • TCP • HTTP • HTTPS • SSL	TCP
%IntroscopeAgentEnterpriseManagerTransportHTTP%	Die Klasse, der zum Senden der Instrumentationsdaten an den Introscope Agent Enterprise Manager über HTTP verwendet wird.	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportHTTPS%	Die Klasse, der zum Senden der Instrumentationsdaten an den Introscope Agent Enterprise Manager über HTTPS verwendet wird.	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportSSL%	Die Klasse, der zum Senden der Instrumentationsdaten an den Introscope Agent Enterprise Manager über SSL verwendet wird.	com.wily.isengard.postofficehub.link.net.SSLSocketFactory
%IntroscopeAgentEnterpriseManagerTransportTCP%	Die Klasse, der zum Senden der Instrumentationsdaten an den Introscope Agent Enterprise Manager über TCP verwendet wird.	com.wily.isengard.postofficehub.link.net.DefaultSocketFactory
%IntroscopeDir%	Der Ordner, in dem der Introscope Agent Enterprise Manager installiert ist.	Unter Windows `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\java\wily`. Unter UNIX `<INSTALLVERZ>/sap_bobj/enterprise_xi40/java/wily`.
%JAVAW_EXE%	Der Name der ausführbaren Datei für die Java Virtual Machine, die nicht über ein Konsolenfenster verfügt.	Unter Windows: `javaw.exe`. Unter UNIX: `java`.
%JAVA_EXE%	Der Name der ausführbaren Datei für die Java Virtual Machine.	Unter Windows: `java.exe`. Unter UNIX: `java`.
%JOBSERVERCHILD_EXE%	Der Name der ausführbaren Datei,für das untergeordnete Element des Adaptive Job Servers.	Unter Windows: `JobServerChild.exe`. Unter UNIX: `boe_jobcd`.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Platzhalter	Beschreibung	Standardwerte
%JOBSERVER_EXE%	Der Name der ausführbaren Datei für den Adaptive Job Server.	Unter Windows: `JobServer.exe`. Unter UNIX: `boe_jobsd`.
%JdkBinDir%	Der Ordner, in dem die JDK-Binärdateien gespeichert sind.	Unter Windows **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/`**<PLATTFORM>**`/sapjvm/bin`.
%JreBinDir%	Der Ordner, in dem die JRE-Binärdateien gespeichert sind.	Unter Windows **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/`**<PLATTFORM>**`/sapjvm/jre/bin`.
%JVM_ARCH_ENVIRONMENT%	Gibt an, ob der Rechner auf einer 32-Bit- oder einer 64-Bit-JVM ausgeführt wird.	Für 32-Bit-UNIX-Rechner lautet der Standardwert “-d32”. Für 64-Bit-Rechner lautet der Standardwert “-d64”. Auf Windows-Rechnern ist dies eine leere Zeichenfolge.
%JVM_HEADLESS_MODE%	Das Befehlzeilenargument, das angibt, ob JVM im Headless-Modus arbeitet.	Unter Windows: -Djava.awt.headless=false. Unter UNIX: -Djava.awt.headless=true
%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%	Andere Befehlszeilenparameter, die das Verhalten der JVM festlegen, wenn diese Fehler wegen ungenügendem Arbeitsspeicher antrifft.	"-XX:+HeapDumpOnOutOfMemoryError" "-XX:HeapDumpPath=%DefaultLoggingDir%" "-XX:+ExitVMOnOutOfMemoryError"
%JVM_SHARED_MEMORY_SEGMENT%	Befehlszeilenparameter, die JVM-Erweiterungen aktivieren und die Instanznummer der JVM festlegen.	Dieser Platzhalter ist standardmäßig leer.
%LANGUAGEPACKSDIR%	Der Ordner, in dem die Sprachpakete der Implementierung installiert sind.	Unter Windows **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\Languages`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/Languages/`.
%LANGUAGEPACKSDIR32%	Ordner, in dem die Sprachpakete der Implementierung auf 32-Bit-Systemen installiert sind.	. Unter Windows **<INSTALLVERZ>**`\SAP BusinessObjects Enterprise XI 4.0\Languages`. Unter UNIX **<INSTALLVERZ>**`/sap_bobj/enterprise_xi40/Languages/`.
%LSTDir%	Ordner, in dem die LST-Konfigurationsdateien gespeichert sind.	Unter Windows **<INSTALLVERZ>**`\SAP BusinessObjects Enter-`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Platzhalter	Beschreibung	Standardwerte
		prise XI 4.0\conf\lst. Unter UNIX **<INSTALLVERZ>**/sap_bobj/enterprise_xi40/conf/lst.
%MDAS_JVM_OS_STACK_SIZE%	Gibt die JVM-Stapelgröße für den mehrdimensionalen Analysedienst an.	Dieser Platzhalter ist standardmäßig leer.
%NCSInstrumentLevelThreshold%	Die Schwellenwertebene der Ablaufverfolgungsprotokollierung für die NCS-Bibliothek.	Der Standardwert lautet 0.
%PAGESERVER_EXE%	Der Name der ausführbaren Datei für den Crystal Reports 2013 Processing Server.	Unter Windows: crproc.exe. Unter UNIX: boe_crprocd.bin.
%PJSContainerDir%	Der Ordner, in dem sich die APS-Container-JARS befinden.	Unter Windows **<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container. Unter UNIX **<INSTALLVERZ>**/sap_bobj/enterprise_xi40/java/pjs/container.
%PJSServicesDir%	Der Ordner, in dem sich die APS-Service-JARS befinden.	Unter Windows **<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services. Unter UNIX **<INSTALLVERZ>**/sap_bobj/enterprise_xi40/java/pjs/services.
%Platform%	Das Betriebssystem des Rechners, auf dem die SAP-BI-Plattform ausgeführt wird.	Das Betriebssystem des Rechners, auf dem die SAP-BI-Plattform ausgeführt wird.
%Platform32%	Das Betriebssystem des Rechners, auf dem die 32-Bit-SAP-BI-Plattform ausgeführt wird.	Das Betriebssystem des Rechners, auf dem die SAP-BI-Plattform ausgeführt wird.
%RasBinDir%	Der Stammordner des Report Application Servers.	Unter Windows **<INSTALLVERZ>**\SAP BusinessObjects Enterprise XI 4.0\win32_x86. Unter UNIX **<INSTALLVERZ>**/sap_bobj/enterprise_xi40/**<PLATTFORM>**/
%SERVER_FRIENDLY_NAME%	Der vollständige Name des Servers.	Der vollständige Name des Servers.
%SERVER_NAME%	Der vollständige Name des Servers.	Der vollständige Name des Servers.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Platzhalter	Beschreibung	Standardwerte
%SMDAgentHost%	Der Hostname des SMD Agents, an den die Instrumentrationsdaten gesendet werden.	Dieser Wert wird während der Installation festgelegt.
%SMDAgentPort%	Der SMD Agent-Port, an den die Instrumentationsdaten gesendet werden.	Dieser Wert wird während der Installation festgelegt.
%TRACE_CONFIGFILE_INI%	Name und Pfad der Datei `BO_Trace.ini`.	Unter Windows **`<INSTALLVERZ>`**`\SAP BusinessObjects Enterprise XI 4.0\conf\BO_trace.ini`. Unter UNIX **`<INSTALLVERZ>`**`/sap_bobj/enterprise_xi40/conf/BO-trace.ini`.
%WarFilesDir%	Der Speicherort der Webanwendungsdateien.	Unter Windows **`<INSTALLVERZ>`**`\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps`. Unter UNIX **`<INSTALLVERZ>`**`/sap_bobj/enterprise_xi40/warfiles/webapps`.
%WEBI_LD_PRELOAD%	Der Name der LD_PRELOAD-Umgebungsvariablen für die Plattform.	$LD_PRELOAD$
%WEBISERVER_EXE%	Der Name der ausführbaren Datei für den Web Intelligence Processing Server.	Unter Windows: `wireportserver.exe`. Unter UNIX: `WIReportServer`.
%WEBI_LD_PRELOAD_ONCE%	Der Name der LD_PRELOAD_ONCE-Umgebungsvariablen für die Plattform.	$LD_PRELOAD_ONCE$
%XCCACHE_EXE%	Der Name der ausführbaren Datei für den Dashboards Cache Server.	Unter Windows: `xccache.exe`. Unter UNIX: `boe_xccached`
%XCPROC_EXE%	Der Name der ausführbaren Datei für den Dashboards Processing Server.	Unter Windows: `xcproc.exe`. Unter UNIX: `boe_xcprocd`.

Hinweis

Die folgenden Platzhalter können auf Knotenebene bearbeitet werden. Die Beschreibungen und Standardwerte sind der oben stehenden Tabelle zu entnehmen. Platzhalter, die nicht in der Liste aufgeführt sind, sind schreibgeschützt.

- **%DefaultAuditingDir%**
- **%DefaultDataDir%**
- **%DefaultLoggingDir%**
- **%IntroscopeAgentEnableInstrumentation%**
- **%IntroscopeAgentEnterpriseManagerHost%**

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

- **%IntroscopeAgentEnterpriseManagerPort%**
- **%IntroscopeAgentEnterpriseManagerTransport%**
- **%NCSInstrumentLevelThreshold%**
- **%SMDAgentHost%**
- **%SMDAgentPort%**

Weitere Informationen

Anzeigen und Bearbeiten der Platzhalter eines Knotens [Seite 436]

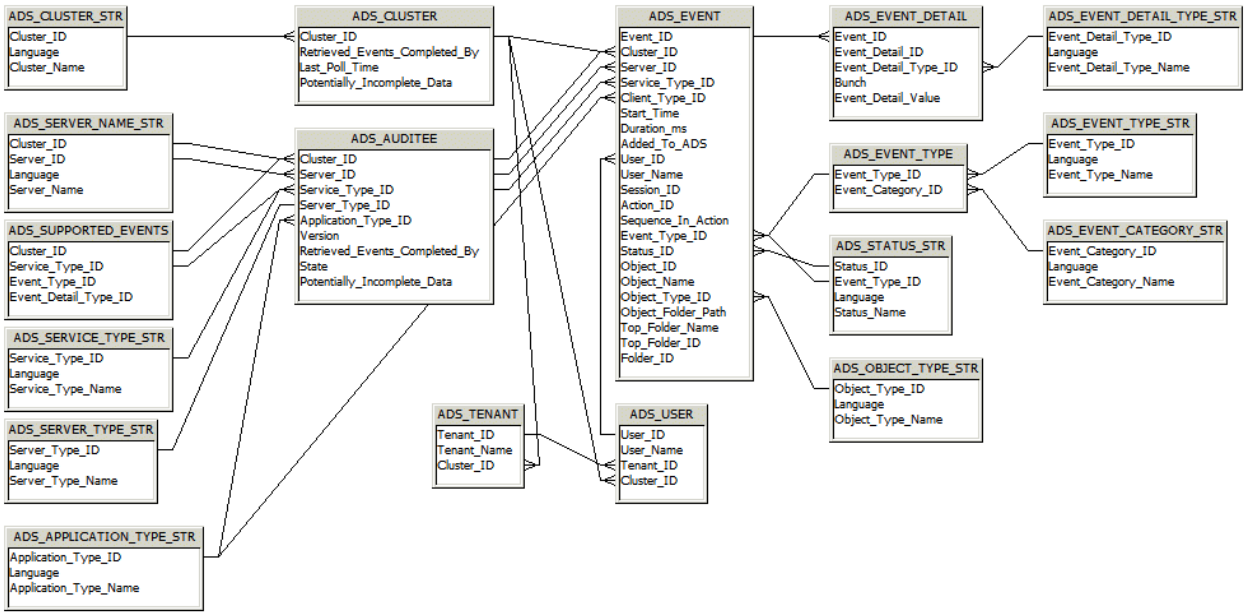
© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

33 ADS-Schema (Audit-Datenspeicher)

33.1 Übersicht

Dieser Anhang dient als Referenz für alle Berichtsdesigner, die auf Überwachungs-Datenspeicher-Tabellen zugreifen und Berichte erstellen. Das folgende Diagramm und die Tabellen erläutern Ihnen die Tabellen, in denen die Überwachungsdaten aufgezeichnet werden, und den Bezug der Tabellen untereinander.

33.2 Schemadiagramm



33.3 ADS-Tabellen (Audit-Datenspeicher)

ADS_APPLICATION_TYPE_STR-Tabelle

In dieser Tabelle ist ein mehrsprachiges Lexikon der Clientanwendungstypnamen enthalten.

Spaltenname	Typ	Beschreibung
Application_Type_ID	Zeichen (64)	Anwendungstyp-CUID der Anwendung
Language	Zeichen (10)	Code für die Sprache, in der der Anwendungstyp aufgezeichnet ist, beispielsweise `<EN>` oder `<DE>`

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Spaltenname	Typ	Beschreibung
Application_Type_Name	Zeichen (255)	Name des Anwendungstyps in Textform, beispielsweise Crystal Reports oder Web Intelligence

ADS_AUDITEE-Tabelle

In dieser Tabelle werden Eigenschafteninformationen für alle Server von auditierten Objekten aufgezeichnet, die zur Implementierung gehören.

Spaltenname	Typ	Beschreibung
Cluster_ID	Zeichen (64)	GUID des Clusters, zu dem das auditierte Objekt gehört
Server_ID	Zeichen (64)	CUID des Servers, durch den das Ereignis ausgelöst wurde. Wenn das Ereignis durch einen Client ausgelöst wurde, wird die CUID des Adaptive Processing Servers aufgezeichnet, der das Ereignis verarbeitet hat.
Service_Type_ID	Zeichen (64)	Diensttyp-CUID des Diensts, durch den das Ereignis ausgelöst wurde. Für Ereignisse, die durch einen Client ausgelöst wurden, wird eine Anwendungstyp-CUID aufgezeichnet.
Server_Type_ID	Zeichen (64)	Servertyp-CUID des Servers, durch den das Ereignis ausgelöst wurde
Application_Type_ID	Zeichen (64)	Anwendungstyp-CUID des Clients, durch den das Ereignis ausgelöst wurde. Bei Serverereignissen wird die ID des Diensttyps aufgezeichnet.
Version	Zeichen (64)	Version des Servers oder Clients, durch den das Ereignis zum Zeitpunkt der Aufzeichnung ausgelöst wurde
Retrieved_Events_Completed_By	DatumUhrzeit	Letzter Zeitpunkt, an dem der Auditor-CMS die temporären Dateien dieses auditierten Objekts abgefragt hat. Dies zeigt an, dass alle Ereignisse von diesem auditierten Objekt, die vor diesem Zeitpunkt abgeschlossen wurden, im ADS vorhanden sind.
State	Ganzzahl	Zustand ("Wird ausgeführt", "Wird nicht ausgeführt", "Gelöscht"), in dem sich das auditierte Objekt befunden hat
Potentially_Incomplete_Data	Ganzzahl	Zeigt an, ob dieses auditierte Objekt unter Umständen Ereignisse aufweist, die nicht in den ADS übertragen wurden

ADS_CLUSTER-Tabelle

In dieser Tabelle werden Informationen zu allen Clustern aufgezeichnet, die auditierte Objekte enthalten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Spaltenname	Typ	Beschreibung
Cluster_ID	Zeichen (64)	GUID des Clusters.
Retrieved_Events_Completed_By	DatumUhrzeit	Zeigt an, wie aktuell die Audit-Informationen in der Datenbank für den jeweiligen Cluster sind. Zeichnet den ältesten abgerufenen Audit-Zeitstempel für alle gerade ausgeführten Server von auditierten Objekten auf. Dies gibt an, dass sich alle Ereingisse, die vor diesem Zeitpunkt abgeschlossen wurden, im ADS befinden.
Last_Poll_Time	DatumUhrzeit	Letzter Zeitpunkt, an dem der Auditor-CMS die auditierten Objekte im jeweiligen Cluster abgefragt hat
Potentially_Incomplete_Data	Ganzzahl	Kennzeichnet potenziell unvollständige Audit-Informationen im Cluster: "0" = alle Server haben die Daten normal übertragen, "1" = für mindestens einen ausgeführten oder nicht ausgeführten Server im Cluster wurde das Kennzeichen **Potentially Incomplete Data** (Potenziell unvollständige Daten) festgelegt, was bedeutet, dass Ereignisse für ein auditiertes Objekt nicht an den ADS übertragen wurden.

ADS_CLUSTER_STR-Tabelle

In dieser Tabelle sind die verschiedenen Cluster in der Implementierung zur Referenz aufgezeichnet.

Spaltenname	Typ	Beschreibung
Cluster_ID	Zeichen (64)	Eine eindeutige ID des Clusters
Language	Zeichen (10)	Code für die Spracheinstellung des Clusters, beispielsweise `<EN>` oder `<DE>`
Cluster_Name	Zeichen (255)	Name des Clusters.

ADS_EVENT-Tabelle

In dieser Tabelle werden die grundlegenden Eigenschaften für jedes Ereignis aufgezeichnet. Sie ist das zentrale Bindeglied für andere Tabellen im Schema.

Spaltenname	Typ	Beschreibung
Event_ID	Zeichen (64)	Eine eindeutige ID, die für das Ereignis generiert wird
Cluster_ID	Zeichen (64)	GUID des Clusters des auditierten Objekts. Dies wird aufgezeichnet, da mehrere Cluster denselben ADS verwenden können.
Server_ID	Zeichen (64)	CUID des Servers, durch den das Ereignis ausgelöst wurde.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Spaltenname	Typ	Beschreibung
Service_Type_ID	Zeichen (64)	• CUID des Diensttyps, durch den das Ereignis ausgelöst wurde. Dienste auf einem Server zeichnen ihre Servertyp-CUID auf. • Clientanwendungen (z.B. BI-Launchpad oder Web Intelligence) zeichnen ihre Anwendungstyp-CUID auf.
Client_Type_ID	Zeichen (64)	Zeichnet die Clienttyp-ID des Clients auf, der die Sitzung eingerichtet hat
Start_Time	DatumUhrzeit	Datum und Uhrzeit (UTC) des Starts des Ereignisvorgangs (einschließlich Millisekunden).
Duration_ms	Ganzzahl	Dauer des Vorgangs in Millisekunden
Added_to_ADS	DatumUhrzeit	Datum und Uhrzeit (UTC) der Aufzeichnung des Ereignisses im ADS.
User_ID	Zeichen (64)	CUID des Benutzers, der die Aktion ausgeführt hat
User_Name	Zeichen (255)	Name, der der ID des Benutzers zugeordnet ist, der die Aktion ausgeführt hat. Wird in der Standardsprache des Auditor-CMS aufgezeichnet.
Session_ID	Zeichen (64)	GUID der Sitzung, in der das Ereignis ausgelöst wurde. Wenn keine Sitzung zugeordnet ist, ist das Feld 0.
Action_ID	Zeichen (64)	ID der Benutzeraktion, die das Ereignis ausgelöst hat. Wird zum Gruppieren von Ereignissen verwendet, die aus einer einzelnen Benutzeraktion hervorgehen.
Sequence_In_Action	Ganzzahl	Bei Multiserverereignissen (oder Client- und Multiserverereignissen) der Server oder die Clientanwendung in der Sequenz, die bzw. der das Ereignis ausgelöst hat. Die Sequenz-ID ist in allen Workflows der zeitgesteuerten Verarbeitung immer 0.
Event_Type_ID	Ganzzahl	Typ des Ereignisses (zum Beispiel "Anzeigen" oder "Speichern")
Status_ID	Ganzzahl	Status des Vorgangs (zum Beispiel "0" = erfolgreich, "1" = fehlgeschlagen)
Object_ID	Zeichen (64)	CUID des Objekts, für das der Vorgang ausgeführt wurde
Object_Name	Zeichen (255)	Name des Objekts, für das der Vorgang ausgeführt wurde. Wird in der Standardsprache des Auditor-CMS aufgezeichnet.
Object_Type_ID	Zeichen (64)	CUID des Objekttyps, für den der Vorgang ausgeführt wurde
Object_Folder_Path	Zeichen (255)	Vollständiger Ordnerpfad (zum Beispiel `Land/Region/Stadt`) des Objekts, für das der Vorgang ausgeführt wurde. Wird in der Standardsprache des Auditor-CMS aufgezeichnet. Falls der Ordnerpfad nicht bestimmt werden kann, wird dieser Wert auf 0 gesetzt.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Spaltenname	Typ	Beschreibung
Folder_ID	Zeichen (64)	CUID des Ordners für das Objekt, für das der Vorgang ausgeführt wurde
Top_Folder_Name	Zeichen (255)	Name der Ordners auf oberster Ebene für das Objekt. Wenn sich das Objekt beispielsweise in `Land/Region/Stadt` befindet, wird `Land` aufgezeichnet.
Top_Folder_ID	Zeichen (64)	CUID des Ordners auf oberster Ebene, in dem das Objekt gespeichert ist. Wenn sich das Objekt beispielsweise in `Land/Region/Stadt` befindet, wird die CUID des Ordners `Land` aufgezeichnet.

ADS_EVENT_CATEGORY_STR-Tabelle

In dieser Tabelle ist ein mehrsprachiges Lexikon der Ereigniskategorienamen enthalten.

Spaltenname	Typ	Beschreibung
Event_Category_ID	Ganzzahl	Ereigniskategorie-ID
Language	Zeichen (10)	Code für die Sprache, in der der Ereigniskategoriename aufgezeichnet ist, beispielsweise **<EN>** oder **<DE>**
Event_Category_Name	Zeichen (255)	Name der Ereigniskategorie

ADS_EVENT_DELETES

Nicht verwenden bzw. keine Berichte auf der Grundlage dieser Tabelle erstellen. Sie wird intern vom System verwendet und kann in künftigen Releases entfernt werden.

ADS_EVENT_DETAIL-Tabelle

In dieser Tabelle werden die Eigenschaften der Ereignisdetails aufgezeichnet.

Spaltenname	Typ	Beschreibung
Event_Detail_ID	Ganzzahl	GUID des Ereignisdetails
Event_ID	Zeichen (64)	Übergeordnete Ereignis-GUID
Event_Detail_Type_ID	Ganzzahl	Typ des Ereignisdetails
Bunch	Ganzzahl	Wenn das Detail Teil einer Serie ist, werden damit die Details verbunden.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Spaltenname	Typ	Beschreibung
		Wenn ein Bericht beispielsweise Eingabeaufforderungen für den Bundesstaat und das Land enthält, kann ein Benutzer "USA" bei der Eingabeaufforderung "Land" und "Kalifornien" sowie "Nevada" bei der Eingabeaufforderung "Bundesstaat" eingeben. Dadurch würden Ereignisdetails mit zwei Bunches erzeugt werden. Bunch 1 würde aus Folgendem bestehen: • Name der Eingabeaufforderung: Land • Wert der Eingabeaufforderung: USA Bunch 2 würde aus Folgendem bestehen: • Name der Eingabeaufforderung: Bundesland • Wert der Eingabeaufforderung: Kalifornien • Wert der Eingabeaufforderung: Nevada
Event_Detail_Value	Zeichen (Langtext)	Wert des Ereignisdetails

ADS_EVENT_DETAIL_TYPE_STR-Tabelle

In dieser Tabelle ist ein mehrsprachiges Lexikon der Namen für Ereignisdetailtypen enthalten.

Spaltenname	Typ	Beschreibung
Event_Detail_ID	Ganzzahl	Ereignisdetailtyp-ID des Ereignisdetails
Language	Zeichen (10)	Code für die Sprache, in der der Ereignisdetailname aufgezeichnet ist, beispielsweise `<EN>` oder `<DE>`
Event_Detail_Type_Name	Zeichen (255)	Textname des Ereignisdetailtyps

ADS_EVENT_TYPE-Tabelle

In dieser Tabelle sind die verschiedenen Ereigniskategorien zur Referenz aufgezeichnet.

Spaltenname	Typ	Beschreibung
Event_Type_ID	Ganzzahl	Eindeutiger Identifikator des Ereignistyps
Event_Category_ID	Ganzzahl	Ereigniskategorie. Beispielsweise "Allgemein", "Web Intelligence" oder "LifeCycle-Management".

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

ADS_EVENT_TYPE_STR-Tabelle

In dieser Tabelle ist ein mehrsprachiges Lexikon der Ereignistypnamen enthalten.

Spaltenname	Typ	Beschreibung
Event_Type_ID	Ganzzahl	Ereignistyp-ID des Ereignisses
Language	Zeichen (10)	Code für die Sprache, in der der Ereigniskategoriename aufgezeichnet ist, beispielsweise `<EN>` oder `<DE>`
Event_Type_Name	Zeichen (255)	Name des Ereignistyps in Textform, beispielsweise "Anzeigen" oder "Anmelden"

ADS_OBJECT_TYPE_STR-Tabelle

In dieser Tabelle ist ein mehrsprachiges Lexikon der Ereignisobjektnamen enthalten.

Spaltenname	Typ	Beschreibung
Object_Type_ID	Zeichen (64)	Objekttyp-CUID des Objekts
Language	Zeichen (10)	Code für die Sprache, in der der Objekttypname aufgezeichnet ist, beispielsweise `<EN>` oder `<DE>`
Object_Type_Name	Zeichen (255)	Name des Objekttyps

ADS_SERVER_NAME_STR-Tabelle

In dieser Tabelle ist ein mehrsprachiges Lexikon der Servernamen enthalten. Die Werte werden bei Umbenennung der Server aktualisiert.

Spaltenname	Typ	Beschreibung
Cluster_ID	Zeichen (64)	GUID des Clusters, zu dem der Server gehört
Server_ID	Zeichen (64)	CUID des Servers
Language	Zeichen (10)	Code für die Sprache des Servernamens, beispielsweise `<EN>` oder `<DE>`
Server_Name	Zeichen (255)	Name des Servers

ADS_SERVICE_TYPE_STR-Tabelle

In dieser Tabelle ist ein mehrsprachiges Lexikon der Diensttypnamen enthalten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Spaltenname	Typ	Beschreibung
Service_Type_ID	Zeichen (64)	Diensttyp- oder Dienstkategorie-CUID des Diensts
Language	Zeichen (10)	Code für die Sprache, in der der Diensttypname aufgezeichnet ist, beispielsweise **<EN>** oder **<DE>**
Service_Type_Name	Zeichen (255)	Name des Diensttyps

ADS_STATUS_STR-Tabelle

In dieser Tabelle ist ein mehrsprachiges Lexikon der Ereignisstatusnamen enthalten.

Spaltenname	Typ	Beschreibung
Status_ID	Ganzzahl	Numerische Darstellung des Betriebsstatus
Event_Type_ID	Ganzzahl	ID des Ereignistyps des Ereignisses. Beispielsweise 1002 für "Anzeigen".
Language	Zeichen (10)	Code für die Sprache, in der der Ereignisstatus aufgezeichnet ist, beispielsweise **<EN>** oder **<DE>**
Status_Name	Zeichen (255)	Eine Beschreibung des Ereignisstatus in Textform, beispielsweise "Erfolgreich" oder "Fehlgeschlagen"

ADS_SUPPORTED_EVENTS-Tabelle

In dieser Tabelle wird eine Liste der unterstützten Ereignisse und zugehörigen Ereignisdetails für jeden Dienst- oder Clientanwendungstyp aufgezeichnet.

Spaltenname	Typ	Beschreibung
Cluster_ID	Zeichen (64)	GUID des Clusters, zu dem der Dienst gehört
Service_Type_ID	Zeichen (64)	Diensttyp-CUID des Diensts, durch den das Ereignis ausgelöst wurde. Wenn das Ereignis von einer Clientanwendung ausgelöst wurde, wird eine Anwendungstyp-CUID aufgezeichnet.
Event_Type_ID	Ganzzahl	ID für den Typ des aufgezeichneten Ereignisses (beispielsweise ID von "Speichern")
Event_Detail_Type_ID	Ganzzahl	CUID, die den Typ des Ereignisdetails identifiziert, das für das jeweilige Ereignis erfasst wurde (beispielsweise "Dateipfad")

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Tabelle ADS_TENANT

In dieser Tabelle wird die Beziehung zwischen Tenant-Namen und -IDs aufgezeichnet.

Spaltenname	Typ	Beschreibung
Cluster_ID	Zeichen (64)	GUID des Clusters.
Tenant_ID	Zeichen (64)	CUID des Tenants.
Tenant_Name	Zeichen (255)	Name des Tenants.

Tabelle ADS_USER

In dieser Tabelle wird die Beziehung zwischen Benutzern und Tenants aufgezeichnet.

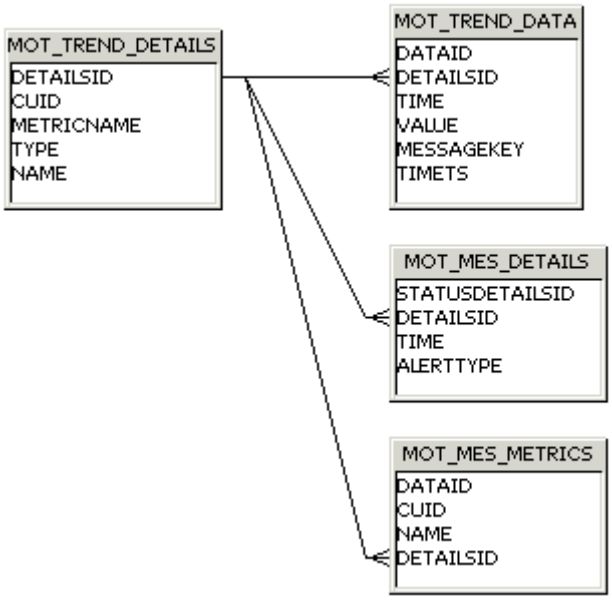
Spaltenname	Typ	Beschreibung
Cluster_ID	Zeichen (64)	GUID des Clusters.
User_ID	Zeichen (64)	CUID des Benutzers.
User_Name	Zeichen (255)	Der Name des Anwenders.
Tenant_ID	Zeichen (64)	CUID des Tenants.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

34 Überwachungsdatenbankschema (Anhang)

34.1 Trenddatenbankschema

Das folgende Trenddatenbankdiagramm und die Tabellen erläutern Ihnen die Tabellen, in denen die Metrik-, Diagnose- und Kontrollmoduldaten aufgezeichnet werden und den Bezug der Tabellen untereinander.



MOT_TREND_DETAILS

In dieser Tabelle werden Informationen zu verwalteten Einheiten, Diagnosen und Kontrollmodule aufgezeichnet. Zum Beispiel die CUID und die Metriknamen.

Spaltenname	Typ	Schlüssel	Beschreibung
DetailsId	INTEGER	Primärschlüssel Automatisch generiert	
CUID	VARCHAR(64)	–	CUID des InfoObjects, das die Metrik zur Verfügung stellt oder mit der Metrik verknüpft ist
MetricName	VARCHAR(255)	–	Name der Metrik
Typ	VARCHAR(32)	–	"Abonnement", "ManagedEntityStatus" oder "Diagnose"
Name	VARCHAR(255)	–	Name des Kontrollmoduls, wenn der Typ "ManagedEntityStatus" entspricht. Andernfalls entspricht es

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Spaltenname	Typ	Schlüssel	Beschreibung
			standardmäßig derselben Zeichenfolge wie im Typ, jedoch nur in Großbuchstaben, z.B.: "DIAGNOSE" oder "ABONNEMENT".

MOT_TREND_DATA

In dieser Tabelle werden die Trenddaten von Metriken, Kontrollmodule und Diagnosen aufgezeichnet. Zum Beispiel Wert und Uhrzeit der Metrik.

Spaltenname	Typ	Schlüssel	Beschreibung
DataId	INTEGER	Primärschlüssel Automatisch generiert	
DetailsId	INTEGER	Fremdschlüssel (aus MOT_TREND_DETAILS)	
Time oder TimeT	BIGINT oder NUMBER oder FIXED Unix-Epoch-Datum	–	Uhrzeit, zu der die Daten gesammelt wurden
Wert	FLOAT oder DOUBLE oder NUMBER	–	Wert der Metrik/des Abonnements
MessageKey	VARCHAR(32)	–	Fehlermeldungsschlüssel oder Null, wenn erfolgreich. Für ein Kontrollmodul kann er auch "watchEnabled" oder "watchDisabled" sein. Es handelt sich hierbei um einen "Schlüssel", weil er letztendlich zum Abrufen lokalisierter Meldungen vor dem Anzeigen der Benutzeroberfläche verwendet wird.
Ts	DATETIME oder TIMESTAMP	–	Uhrzeit, zu der Daten in die Datenbank geschrieben wurden

MOT_MES_DETAILS

In dieser Tabelle werden Informationen zu Abonnement-Nichteinhaltungen und Warnmeldungsversand aufgezeichnet. Zum Beispiel die Uhrzeit der Nichteinhaltung und des Warnmeldungsversands.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Spaltenname	Typ	Schlüssel	Beschreibung
StatusDetailsId	INTEGER	Primärschlüssel Automatisch generiert	
DetailsId	INTEGER	Fremdschlüssel (aus MOT_TREND_DETAILS)	
Zeit	BIGINT oder NUMBER Unix-Epoch-Datum	–	Uhrzeit, zu der die Daten gesammelt wurden
AlertType	SMALLINT oder NUMBER	–	Bereitstellungstyp der Abonnementbenachrichtigung (z.B. E-Mail)

MOT_MES_METRICS

In dieser Tabelle sind Informationen zu Kontrollmodulen und Metriken enthalten, die zu den Kontrollmodulgleichungen gehören. Jede zum Kontrollmodul gehörende Metrik verfügt über einen Eintrag in dieser Tabelle.

Spaltenname	Typ	Schlüssel	Beschreibung
DataId	INTEGER	Primärschlüssel Automatisch generiert	
DetailsId	INTEGER	Fremdschlüssel (aus MOT_TREND_DETAILS)	
CUID	VARCHAR(64)	–	CUID des Kontrollmoduls
Name	VARCHAR(255)	–	Name des Kontrollmoduls

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

35 Systemkopie-Arbeitsblatt (Anhang)

35.1 Systemkopie-Arbeitsblatt

Eigenschaft	Wert
Cluster-Schlüssel	
Namen der Knoten	
Rechnername und BI-Plattform-Installationsordner jedes Rechners in der Implementierung.	
Das Administratorkennwort der BI-Plattform	
CMS-Datenbankverbindungen, die Benutzernamen und Kennwörter, die zu diesen Verbindungen gehören, für jeden Rechner in der Implementierung	
Audit-Datenbankverbindungen, die Benutzernamen und Kennwörter, die zu diesen Verbindungen gehören, für jeden Rechner in der Implementierung	
Für jeden Rechner in der Implementierung Details von allen anderen Datenbankclientverbindungen für jeden Rechner im Quellsystem, der von Universen und Berichten verwendet wird	
Für jeden Rechner in der Implementierung die Datenbankclienttypen und -versionen	
Die Version, das Support Package und die Patch-Ebene	
Dateispeicherorte der einzelnen Input FRS und Output FRS in der Implementierung.	
Der Speicherort des Hochstufverwaltungs-Datenbankordners und des Subversion-Ordners, falls Promotion Management kopiert werden soll.	
Der Ordner der Überwachungsdatenbank, falls die Überwachungsdatenbank kopiert werden soll	
Der Pfad zum Ordner der semantischen Ebene	

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

www.sap.com/contactsap

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.
Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch die SAP AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.
Die von SAP AG oder deren Vertriebsfirmen angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehersteller enthalten. Produkte können länderspezifische Unterschiede aufweisen.
Die vorliegenden Unterlagen werden von der SAP AG und ihren Konzernunternehmen („SAP-Konzern") bereitgestellt und dienen ausschließlich zu Informationszwecken. Der SAP-Konzern übernimmt keinerlei Haftung oder Gewährleistung für Fehler oder Unvollständigkeiten in dieser Publikation. Der SAP-Konzern steht lediglich für Produkte und Dienstleistungen nach der Maßgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt ist. Aus den in dieser Publikation enthaltenen Informationen ergibt sich keine weiterführende Haftung.
SAP und andere in diesem Dokument erwähnte Produkte und Dienstleistungen von SAP sowie die dazugehörigen Logos sind Marken oder eingetragene Marken der SAP AG in Deutschland und anderen Ländern.
Zusätzliche Informationen zur Marke und Vermerke finden Sie auf der Seite http://www.sap.com/corporate-de/legal/copyright/index.epx.