PUBLIC (ÖFFENTLICH)

SAP BusinessObjects Business Intelligence

Dokumentversion: 4.3 Support Package 4 – 2023-12-07

Business-Intelligence-CMC-Hilfe

© 2024 SAP SE oder ein SAP-Konzernunternehmen Alle Rechte vorbehalten.

THE BEST RUN SAP

Inhalt

1 Central Management Console. 15

1.1 Central Management Console. 15

1.2 Anmelden bei der CMC. 15

1.3 Navigieren in der CMC. 16

1.4 Festlegen der CMC-Einstellungen. 17

2 Systemkonfigurationsassistent. 18

2.1 Einführung in den Systemkonfigurationsassistenten. 18

2.2 Angeben der von Ihnen verwendeten Produkte. 18

2.3 Auswählen von Implementierungsvorlagen. 20

2.4 Festlegen von Datenordnerspeicherorten. 22

2.5 Überprüfen von Änderungen. 24

2.6 Protokolldateien und Antwortdateien. 24

Verwenden von Antwortdateien. 25

3 Verwalten von Benutzern und Gruppen. 29

3.1 Verwalten von Enterprise-Konten und allgemeinen Konten. 29

So erstellen Sie ein Benutzerkonto. 29

So ändern Sie ein Benutzerkonto. 30

Löschen eines Benutzerkontos. 31

Erstellen von neuen Gruppen. 31

So ändern Sie die Eigenschaften einer Gruppe. 32

So zeigen Sie Gruppenmitglieder an. 32

Hinzufügen von Untergruppen. 33

Festlegen von Gruppenmitgliedschaften. 33

Hinzufügen von Benutzern oder Benutzergruppen in Massenvorgängen. 34

So löschen Sie eine Gruppe. 34

So aktivieren Sie das Guest-Konto. 35

Hinzufügen der Registerkarte "Anpassung" zu einem Benutzer oder einer Gruppe. 35

Hinzufügen von Benutzern zu Gruppen. 36

Ändern der Kennworteinstellungen. 37

Aktivieren der vertrauenswürdigen Authentifizierung. 39

Gewähren von Zugriff für Benutzer und Gruppen. 40

Steuern des Zugriffs auf Posteingänge von Benutzern. 41

Festlegen der BI-Launchpad-Einstellungen für Benutzergruppen in der CMC 41

Festlegen der Einstellungen für das fiorisierte BI-Launchpad für Benutzergruppen in der CMC 43

3.2 Verwalten von Aliasen. . . . 45
Erstellen von Benutzern und Hinzufügen eines Drittthersteller-Alias. . . . 45
Erstellen eines neuen Alias für einen vorhandenen Benutzer. . . . 46
So weisen Sie einen Alias eines anderen Benutzers zu. . . . 47
So löschen Sie einen Alias. . . . 47
So deaktivieren Sie einen Alias. . . . 48

4 Festlegen von Rechten. . . . 49
4.1 Verwalten von Sicherheitseinstellungen für Objekte in der CMC. . . . 49
Rechte für einen Prinzipal auf einem Objekt anzeigen. . . . 49
So weisen Sie einer Zugriffskontrollliste für ein Objekt Prinzipale hinzu. . . . 50
Ändern der Sicherheit für einen Prinzipal auf einem Objekt. . . . 50
Festlegen von Rechten für einen Ordner der obersten Ebene in der BI-Plattform. . . . 51
Überprüfen von Sicherheitseinstellungen für ein Subjekt. . . . 52
4.2 Arbeiten mit Zugriffsberechtigungen. . . . 54
Auswählen zwischen den Zugriffsberechtigungen *Ansicht* und *Ansicht auf Abruf*. . . . 56
Kopieren von vorhandenen Zugriffsberechtigungen. . . . 57
Erstellen von Zugriffsberechtigungen. . . . 57
Umbenennen von Zugriffsberechtigungen. . . . 58
So löschen Sie eine Zugriffsberechtigung. . . . 58
So ändern Sie Rechte in einer Zugriffsberechtigung. . . . 58
Verfolgen der Beziehung zwischen Zugriffsberechtigungen und Objekten. . . . 59
Standortübergreifende Verwaltung von Zugriffsberechtigungen. . . . 60
4.3 Auflösen der Übernahme. . . . 61
So deaktivieren Sie die Übernahme. . . . 62

5 Authentifizierung. . . . 64
5.1 Übersicht. . . . 64
Authentifizierungsoptionen in der BI-Plattform. . . . 64
5.2 Enterprise-Authentifizierung. . . . 64
Enterprise-Authentifizierung. . . . 64
Einstellungen der Enterprise-Authentifizierung. . . . 65
5.3 LDAP-Authentifizierung. . . . 68
LDAP-Authentifizierung. . . . 68
Konfigurieren der SSL-Einstellungen für die LDAP-Serverauthentifizierung oder gegenseitige Authentifizierung . . . 72
Konfigurieren des LDAP-Plugins für SiteMinder . . . 77
Zuordnen von LDAP-Gruppen. . . . 78
5.4 Windows-AD-Authentifizierung. . . . 80
Windows AD-Authentifizierung. . . . 80
Sicherheits-Plugin für Windows AD. . . . 80
Konfigurieren der Windows AD-Authentifizierung . . . 81

Zuordnen von Windows AD-Gruppen. 85
5.5 SAP-Authentifizierung. 86
SAP-Authentifizierung. 86
Verbinden mit SAP-Berechtigungssystemen. 87
Einstellen von SAP-Authentifizierungsoptionen. 89
Importieren von SAP-Rollen. 93
Workflow für die Integration in Secure Network Communication 97
5.6 Oracle-EBS-Authentifizierung. 99
Oracle-EBS-Authentifizierung. 99
Aktivieren der Oracle-EBS-Authentifizierung. 99
Zuordnen von Oracle-E-Business Suite-Rollen zur BI-Plattform. 101
Aktualisieren von Oracle EBS-Rollen und -Benutzern. 104
5.7 JD-Edwards-Enterprise-One-Authentifizierung. 106
JD Edwards EnterpriseOne-Authentifizierung. 106
Aktivieren der JD Edwards EnterpriseOne-Authentifizierung. 106
Zuordnen von JD-Edwards-EnterpriseOne-Rollen zur BI-Plattform. 107
5.8 PeopleSoft-Enterprise-Authentifizierung. 112
PeopleSoft Enterprise-Authentifizierung. 112
Aktivieren der PeopleSoft Enterprise-Authentifizierung. 113
Zuordnen von PeopleSoft-Rollen zur BI-Plattform. 114
5.9 Siebel-Authentifizierung. 119
Siebel-Authentifizierung. 119
Aktivieren der Siebel-Authentifizierung. 119
Zuordnen von Rollen zur BI-Plattform. 120
5.10 X.509-Authentifizierung. 125
X.509-Authentifizierung für BI-Launchpad. 125
X.509-Authentifizierung für Webdienste. 133
X.509-Authentifizierung für die CMC. 136
5.11 OpenID-Connect-Authentifizierung. 138
OpenID-Connect-Authentifizierung aktivieren. 139

6 Verwalten von Benutzerattributen. 140
6.1 Verwalten von Attributen für Systembenutzer 140
6.2 Priorisierung von Benutzerattributen über mehrere Authentifizierungsoptionen hinweg. 141
6.3 Hinzufügen von neuen Benutzerattributen. 141
6.4 Benutzerdefinierte Benutzerattribute bearbeiten. 143

7 Multitenancy. 144
7.1 Verwalten von Tenants in der CMC. 144
Festlegen von Tenant-Eigenschaften 144
Zuweisen von Zugriffsrechten zu einer Tenant-Benutzergruppe 146
Verwalten von Benutzergruppen für einen Tenant. 147

Löschen von Tenants. 149

8 Verwalten der Lizenz. 150

8.1 Verwalten von Lizenzschlüsseln. 150

Anzeigen von Lizenzinformationen. 150

Hinzufügen von Lizenzschlüsseln. 150

So zeigen Sie die aktuelle Kontoaktivität an. 151

9 Verwalten von Servern. 152

9.1 Arbeiten mit dem Verwaltungsbereich "Server" in der CMC. 152

9.2 So lassen Sie den Status eines Servers anzeigen. 155

9.3 Starten, Stoppen oder Neustarten von Servern über die CMC. 155

9.4 Automatisches Starten von Servern. 156

9.5 Aktivieren und deaktivieren von Servern über die CMC. 156

9.6 Hinzufügen von Servern. 157

9.7 So klonen Sie einen Server. 157

9.8 Löschen von Servern. 158

9.9 Benutzerdefinierte Kopfinformationen hinzufügen. 158

9.10 Nichtexklusive Servergruppen erstellen. 159

9.11 Hinzufügen von Untergruppen zu Servergruppen. 160

9.12 So fügen Sie eine Servergruppe zu einer anderen hinzu. 160

9.13 Rechteverwaltung für Servergruppen. 161

9.14 Gruppenzugehörigkeit eines Servers ändern. 165

9.15 Ändern der Eigenschaften eines Servers. 166

9.16 So legen Sie eine Konfigurationsvorlage fest. 166

9.17 So wenden Sie eine Konfigurationsvorlage auf einen Server an. 167

9.18 Wiederherstellen der Systemstandardwerte. 168

9.19 So zeigen Sie die Servermetrik an. 168

9.20 So zeigen Sie die Systemmetrik an. 169

9.21 So aktivieren oder deaktivieren Sie Ziele für einen Job Server. 169

9.22 Anzeigen von Serverplatzhaltern. 169

9.23 Anzeigen und Bearbeiten der Platzhalter eines Knotens. 170

9.24 Festlegen der Zieleigenschaften für einen Job Server. 170

Eigenschaften für Posteingangsziele. 171

Eigenschaften für E-Mail-Ziele. 172

Eigenschaften für FTP-Ziele. 173

Eigenschaften für SFTP-Ziele. 174

Eigenschaften für Dateisystemziele. 175

9.25 Konfigurieren von Adaptive Processing Servern für Produktionssysteme. 176

10 Verwalten von Web Application Container Servern (WACS). 178

10.1 Web Application Container Server (WACS). 178

10.2 Hinzufügen oder Entfernen zusätzlicher WACS in einer Implementierung. 178
Installieren von WACS. 179
Hinzufügen eines neuen Web Application Container Servers. 180
Klonen eines Web Application Container Servers 180
Löschen von WACS-Servern aus der Implementierung. 181
10.3 Hinzufügen oder Entfernen von Diensten auf dem WACS. 182
Hinzufügen einer Webanwendung oder eines Webdiensts zu einem WACS. 182
Entfernen einer Webanwendung oder eines Webdiensts von einem WACS. 182
10.4 Konfigurieren von WACS für AD Kerberos. 183
10.5 Konfigurieren der WACS AD Kerberos-Einzelanmeldung. 184
10.6 Konfigurieren von HTTPS/SSL. 184
10.7 WACS und Ihre IT-Umgebung. 186
Verwenden eines WACS mit einem Reverse Proxy. 186
Konfigurieren des WACS auf einem mehrfach vernetzten Rechner. 187
10.8 Fehlerbehebung. 188
So zeigen Sie die Servermetrik an. 188
Status eines WACS anzeigen lassen. 188
Auflösen von Portkonflikten. 188
Ändern der Anzahl gleichzeitiger Anforderungen. 189
Verhindern von Anmeldungen beim WACS über HTTP. 190

11 Verwalten von Anwendungen. 191
11.1 Übersicht. 191
11.2 Allgemeine Einstellungen. 192
Festlegen von Benutzerrechten für Anwendungen. 192
Protokollierungsebene der Ablaufverfolgung der Webanwendung in der CMC einstellen. 192
11.3 Anwendungseinstellungen. 193
Verwalten des CMC-Registerkartenzugriffs. 193
Verwalten der BI-Launchpad-Einstellungen. 201
Verwalten von Web-Intelligence-Einstellungen. 203
Verwalten von Einstellungen für Crystal Reports. 206
Verwalten von Central Management Console-Einstellungen. 206
Verwalten der Einstellungen der BI-Kommentaranwendung. 210
Verwalten der Papierkorbeinstellungen. 212
Verwalten von Warnmeldungseinstellungen. 215
Verwalten von Widget-Einstellungen. 217
Verwalten von Einstellungen für SAP BusinessObjects Mobile. 217
Verwalten des Push-Benachrichtigungsdienstes in SAP BusinessObjects Mobile. 221
Verwalten der Einstellungen für die Plattformsuche. 222
Konfigurieren der BEx-Webintegration. 229
Konfigurieren von SAP-HANA-Einzelanmeldung. 235
Verwalten der SAP-Lumira-Einstellungen. 239

Verwalten von Einstellungen für die Zusammenarbeit. 240
Verwalten der Einstellungen von Diskussionsforen. 244
Berechtigungsserver-Konfiguration. 247
Konfiguration der Informationsklassifizierung. 251

12 Verwalten von Datenquellen und Verbindungen. 253
12.1 Verwalten von Verbindungen. 253
So löschen Sie eine Universumsverbindung. 253
12.2 Verwalten von Universen. 254
So löschen Sie Universen. 254

13 Verwalten von Hotbackups. 256
13.1 Hotbackups. 256
Aktivieren von Hotbackups. 257

14 Ordner. 258
14.1 Ordner 258
Erstellen von Ordnern. 258
Löschen von Ordnern. 258
Kopieren oder Verschieben von Ordnern. 259
Beschränken von Berichtinstanzen auf Ordnerebene. 259
Beschränkung von Dokumenten in Posteingängen. 260

15 Kategorien. 262
15.1 Arbeiten mit Kategorien. 262
Erstellen einer Kategorie. 262
Löschen einer Kategorie. 262
Verschieben einer Kategorie. 262
Hinzufügen von Objekten zu Kategorien. 263
Entfernen oder Löschen von Objekten aus einer Kategorie. 263
Anzeigen der persönlichen Kategorien eines Benutzers. 264
Hinzufügen von mehreren Objekten zu einer Kategorie. 264

16 Objektverwaltung. 265
16.1 Standardeinstellungen. 265
16.2 Hinzufügen von Objekten in der CMC. 267
16.3 Kopieren von Objekten. 268
16.4 So verschieben Sie ein Objekt. 268
16.5 Erstellen von Objektverknüpfungen. 268
16.6 Löschen von Objekten. 269
16.7 So suchen Sie nach einem Objekt bzw. nach Objekten. 269
16.8 Senden von Objekten oder Instanzen an ein Ziel. 270
16.9 Ändern der Eigenschaften von Objekten. 271

16.10 So überprüfen Sie die Beziehungen eines Objekts. 271
16.11 Erstellen eines neuen Hyperlinks. 272

17 Berichte. 273
17.1 Auswählen der Regenerierungsoptionen für einen Bericht. 273
17.2 Auswählen von Berichtanzeigeoptionen für einen Crystal-Reports-Bericht. 273
17.3 Auswählen der Standardserver zum Verarbeiten eines Objekts. 273
17.4 Ändern der Datenbankeinstellungen in Crystal-Reports-Berichten. 274
17.5 Aktualisieren der Standardparameterwerte für einen Crystal-Reports-Bericht. 275
17.6 Aktualisieren der Eingabeaufforderungen für ein Web-Intelligence-Dokument. 275
17.7 Verwenden von Filtern. 276
17.8 Auswählen eines Druckers für Crystal-Reports-Berichte. 277
17.9 Auswählen von Seitenlayoutoptionen für Crystal Reports-Berichte und PDF-Objekte. 278
17.10 Zuweisen einer Verarbeitungserweiterung zu einem Bericht. 278
17.11 Anzeigen einer Miniaturansicht der ersten Seite eines Crystal-Reports-Berichts. 279
17.12 Hinzufügen von Berichten in das BI-Repository und Hinzufügen von Hyperlinks. 279
17.13 Anzeigen von Universen für Web-Intelligence-Dokumente. 280
17.14 Warnmeldungen zu einem Crystal-Reports-Bericht anzeigen. 280

18 Programmobjekte. 281
18.1 Festlegen von Befehlszeilenargumenten. 281
18.2 Festlegen eines Arbeitsverzeichnisses für ein Programmobjekt. 281
18.3 Ändern des Standardarbeitsverzeichnisses für Programmobjekte. 281
18.4 Angeben des Pfads zu externen oder Hilfsdateien. 282
18.5 Laden von externen oder Hilfsdateien auf den File Repository Server. 282
18.6 Hinzufügen einer Umgebungsvariablen. 283
18.7 Festlegen der erforderlichen Parameter für Java-Programme. 283
18.8 Ermöglichen des Zugriffs durch Java-Programme auf andere Dateien. 284
18.9 Festlegen des Benutzerkontos für ein Programmobjekt. 284

19 Objektpakete. 285
19.1 Erstellen von Objektpaketen. 285
19.2 Hinzufügen neuer Objekte zu einem Objektpaket. 285
19.3 Festlegen von Komponentenfehleroptionen für ein Objektpaket. 285

20 Zeitgesteuerte Verarbeitung. 287
20.1 Objekt zeitgesteuert verarbeiten. 287
Wiederholungsmuster. 288
Ausführungsoptionen für Wiederholungsmuster. 289
20.2 Zeitgesteuerte Verarbeitung eines Objekts mit dem Enterprise-Standardspeicherort als Ziel. 291
20.3 Zeitgesteuertes Verarbeiten eines Objektes für einen Dateispeicherort. 291
20.4 Zeitgesteuertes Verarbeiten von Objekten für einen FTP-Server 292
20.5 Zeitgesteuertes Verarbeiten von Objekten für einen SFTP-Server. 293

20.6 Zeitgesteuertes Verarbeiten eines Objekts für E-Mails. . . . 294
Einrichten von SMTP über SSL. . . . 295
20.7 Zeitgesteuertes Senden von Objekten an BI-Posteingänge von Benutzern. . . . 295
20.8 Aktivieren oder Deaktivieren von Zielen für einen Job Server. . . . 296
20.9 Zeitgesteuerte Verarbeitung von Objekten auf der Grundlage von Ereignissen. . . . 297
20.10 Zeitgesteuerte Verarbeitung von Objekten zum Auslösen eines Ereignisses. . . . 297
20.11 Konfigurieren von Erfolgs- oder Fehlerbenachrichtigungen für eine Instanz. . . . 298
20.12 Einstellen einer Warnungsbenachrichtigung. . . . 299
20.13 Auswahl eines Ausgabeformats.. . . . 299
20.14 Wählen eines Cache-Formats für Web-Intelligence-Dokumente. . . . 300
20.15 Zeitgesteuerte Verarbeitung eines Berichtsobjekts für einzelne Benutzer. . . . 301
20.16 Auswählen eines Servers oder einer Servergruppe für die zeitgesteuerte Verarbeitung von Objekten. . . . 301
20.17 Verwalten von Instanzen für ein Objekt. . . . 302
20.18 Instanzen-Manager. . . . 303
20.19 Anzeigen einer Instanz. . . . 303
20.20 Anhalten einer Instanz. . . . 304
20.21 Fortsetzen einer angehaltenen Instanz. . . . 304
20.22 Löschen von Instanzen. . . . 304
20.23 Beschränkungen für Instanzen festlegen. . . . 304
20.24 Sofortiges Ausführen mehrerer Objekte. . . . 305
20.25 Auswählen von Sprachen für Berichtsinstanzen 306

21 Kalender. . . . 307
21.1 Erstellen eines Kalenders. . . . 307
21.2 Termine zum Kalender hinzufügen. . . . 307
21.3 Löschen eines Kalenders. . . . 308

22 Ereignisse. . . . 309
22.1 Ereignisse. . . . 309
Benutzerbenachrichtigungen. . . . 310
22.2 Ereignisse und zeitgesteuerte Verarbeitung. . . . 313
Erstellen eines dateibasierten Ereignisses. . . . 315
Erstellen eines Zeitsteuerungsereignisses. . . . 315
Erstellen eines benutzerdefinierten Ereignisses. . . . 316
Auslösen eines benutzerdefinierten Ereignisses. . . . 316

23 Warnmeldungen. . . . 317
23.1 Suchen von Warnungsquellobjekten in der CMC. . . . 317
23.2 Aktivieren der Warnmeldungsfunktion für ein Ereignis. . . . 317
23.3 Abonnieren einer Warnmeldung. . . . 318
23.4 Abonnement einer Warnmeldung aufheben. . . . 319
23.5 Abonnieren einer Warnmeldung für andere Benutzer. . . . 319

23.6 Aufheben des Abonnements einer Warnung für andere Benutzer. 320
23.7 Ausschließen von Benutzern von einer Warnungmeldung. 320
23.8 Verwalten von Warnmeldungseinstellungen für eine Warnungsquelle. 321

24 Profile. 323
24.1 Erstellen eines Profils. 323
24.2 Angeben eines globalen Profilziels für ein Profil. 323
24.3 Angeben eines Profilwerts für einen Benutzer oder eine Gruppe. 323
24.4 Verwenden von Variablen als Profilwerte. 324

25 BI-Admin-Studio. 326
25.1 Admin-Cockpit. 327
Admin-Cockpit. 327
BI für Server. 328
BI-Informationen zu Dokumentinstanzen. 329
BI: Benutzer und Sitzungen. 330
BI für die Nutzung von Daten. 330
BI für Anwendungen. 331
25.2 Überwachung. 331
Dashboard. 332
Diagramme. 335
Diagnosen. 336
Kontrollmodule. 348
Metriken. 356
Warnmeldungen. 358
Erstellen von Berichten für Überwachungsdaten. 359
25.3 Grafischer Vergleich. 360
Vergleich von Objekten oder Dateien mittels des Grafischen Vergleichs. 360
Vergleichen von Objekten oder Dateien mithilfe des Versionsverwaltungssystems. 362
Zeitgesteuerte Verarbeitung des Vergleichs. 362

26 Auditing. 364
26.1 Übersicht. 364
26.2 Seite CMC-Auditing. 370
Auditing-Status. 371
Konfigurieren von Audit-Ereignissen. 372
Konfigurationseinstellungen des Audit-Datenspeichers (ADS). 376

27 Plattformsuche. 379
27.1 Plattformsuche. 379
Konfigurieren von Anwendungseigenschaften in der CMC. 379
Liste der Indizierungsfehler. 386
Festlegen der Sicherheitsberechtigungen für Benutzer. 386

Zeitgesteuertes Verarbeiten eines Objekts. 389

28 Arbeiten mit Föderation. 391

28.1 Föderation. 391

28.2 Begriffe in Föderation. 392

28.3 Verwalten von Sicherheitsrechten. 394

Für die ursprüngliche Website erforderliche Rechte. 394

Für die Zielwebsite erforderliche Rechte. 395

Föderation-spezifische Rechte. 396

Replizieren der Sicherheit eines Objekts. 397

Replizieren der Sicherheit durch Zugriffsberechtigungen. 398

28.4 Optionen für Replikationstypen und Replikationsmodi. 398

Einseitige Replikation 399

Beidseitige Replikation 399

"Von ursprünglicher Website aus aktualisieren" oder "Von Ziel aus aktualisieren". 400

28.5 Replizieren von Dritthersteller-Benutzern und -Gruppen. 401

28.6 Replizieren von Universen und Universumsverbindungen. 403

28.7 Verwalten von Remoteverbindungen. 404

Erstellen von Remoteverbindungen. 404

Ändern von Remoteverbindungen. 406

28.8 Verwalten von Replikationsaufträgen. 406

Erstellen von Replikationsaufträgen. 407

Zeitgesteuertes Verarbeiten eines Replikationsauftrags. 409

Ändern von Replikationsaufträgen. 409

Anzeigen eines Protokolls nach einem Replikationsauftrag. 410

28.9 Verwalten der Objektbereinigung. 410

Verwenden der Objektbereinigung. 411

28.10 Erkennen und Auflösen von Konflikten. 411

Konfliktauflösung bei der einseitigen Replikation. 412

Konfliktauflösung bei der beidseitigen Replikation. 414

28.11 Verwenden von Web Services in Föderation. 417

Sitzungsvariablen 418

Zwischenspeichern von Dateien 418

Benutzerdefinierte Implementierung 419

28.12 Remote-Zeitsteuerung und lokale Ausführung von Instanzen. 420

Remote-Zeitsteuerung. 420

Lokal ausgeführte Instanzen. 421

Instanzenfreigabe. 422

28.13 Importieren und Höherstufen replizierter Inhalte. 423

Importieren replizierter Inhalte. 423

Importieren replizierter Inhalte und Fortsetzen der Replikation 424

Höherstufen von Inhalten aus einer Testumgebung. 424

Neuverweisen auf eine Zielwebsite. . . . 425
28.14 Optimale Vorgehensweisen. . . . 425
Einschränkungen der aktuellen Version. . . . 429
Behandeln von Fehlermeldungen. . . . 430

29 Verwalten von Replikationslisten. . . . 435
29.1 Verwalten von Replikationslisten. . . . 435
Erstellen von Replikationslisten. . . . 436
Ändern von Replikationslisten. . . . 437

30 Veröffentlichungen. . . . 439
30.1 Entwurfsaufgaben. . . . 439
Veröffentlichung in der CMC erstellen. . . . 439
Veröffentlichung zum Bearbeiten öffnen. . . . 439
Allgemeine Eigenschaften für eine Veröffentlichung definieren. . . . 440
Quelldokumente hinzufügen. . . . 440
Auswählen von Enterprise-Empfängern. . . . 441
Auswählen dynamischer Empfänger. . . . 442
Ziel für eine Veröffentlichung auswählen. . . . 443
Wiederholungsmuster auswählen. . . . 445
Personalisierte Platzhalter für Veröffentlichungsquelldokumente auswählen. . . . 447
Personalisierte Platzhalter für E-Mail-Felder auswählen. . . . 448
Inhalte aus dynamischen Quelldokumenten in eine E-Mail einbetten. . . . 448
Veröffentlichungserweiterung in der CMC hinzufügen. . . . 449
E-Mail-Benachrichtigung für einen Veröffentlichungsauftrag in der CMC aktivieren. . . . 450
Audit-Benachrichtigung für einen Veröffentlichungsauftrag in der CMC aktivieren. . . . 451
Ereignisse zum Auslösen einer Veröffentlichung auswählen. . . . 452
Servergruppe für eine Veröffentlichung auswählen. . . . 453
Profilauflösungsmethode in der CMC auswählen. . . . 453
Berichtsbursting-Methode in der CMC auswählen. . . . 453
30.2 Crystal-Reports-Berichte – Entwurfsaufgaben. . . . 454
Crystal-Reports-Berichte mithilfe von Parameterwerten personalisieren. . . . 454
Crystal Reports-Berichte durch Filtern von Feldern personalisieren. . . . 454
Veröffentlichungsformat für einen Crystal-Reports-Bericht auswählen. . . . 455
(Optional) Druckoptionen für Crystal-Reports-Berichte in Veröffentlichungen auswählen. . . . 462
(Optional) Versandregel für Empfänger für einen Crystal-Reports-Bericht in einer Veröffentlichung auswählen. . . . 463
(Optional) Globale Versandregel für eine Veröffentlichung auswählen. . . . 464
(Optional) Zusammengeführte PDF-Dateien aus Crystal-Reports-Berichten formatieren. . . . 464
Datenbank-Anmeldedaten für einen Crystal-Reports-Bericht in einer Veröffentlichung konfigurieren. . . . 466
30.3 Web-Intelligence-Dokumente – Entwurfsaufgaben. . . . 467

Veröffentlichungsformat für ein Web-Intelligence-Dokument auswählen. 467
Web-Intelligence-Dokument mit einem globalen Profilziel personalisieren. 467
Web-Intelligence-Dokumente durch Filtern von Feldern personalisieren. 468
Bearbeiten von Parameter- oder Eingabeaufforderungswerten für ein Objekt. 469
30.4 Aufgaben nach dem Entwurf. 470
Veröffentlichung testen. 470
Veröffentlichung zeitgesteuert verarbeiten. 470
Abonnieren von Veröffentlichungen bzw. Aufheben eines Abonnements. 472
Abonnieren einer Veröffentlichungsinstanz oder Aufheben eines Abonnements. 473
Veröffentlichungsinstanz neu verteilen. 473
Fehlgeschlagene Veröffentlichung wiederholen. 474

31 Rechte (Anhang). 475
31.1 Informationen über den Anhang zu Berechtigungen. 475
31.2 Allgemeine Rechte. 475
Zielrechte. 479
31.3 Rechte für bestimmte Objekttypen. 480
Ordnerrechte. 480
Kategorien. 480
Crystal-Reports-Berichte. 481
Web-Intelligence-Dokumente. 481
Benutzer und Gruppen. 482
Zugriffsberechtigungen. 484
Universumsrechte (.unv). 484
Universumsrechte (.unx). 486
Zugriffsberechtigungen für Universumsobjekte. 487
Verbindungsrechte. 488
Anwendungen. 490

32 Servereigenschaften (Anhang). 499
32.1 Über Servereigenschaften (Anhang). 499
Allgemeine Servereigenschaften. 499
Kerndienste-Eigenschaften. 501
Eigenschaften von Konnektivitätsdiensten. 513
Eigenschaften von Crystal-Reports-Diensten. 518
Analysis Services-Eigenschaften. 526
Eigenschaften des Datenföderations-Diensts. 527
Eigenschaften der Web-Intelligence-Dienste. 528

33 Servermetrik (Anhang). 537
33.1 Info zu Servermetriken (Anhang). 537
Allgemeine Servermetriken. 537

Central Management Server-Metriken. 539
Connection Server-Metriken. 543
Event Server-Metriken. 543
File Repository Server-Metriken. 543
Adaptive Processing Server-Metriken. 544
Web Application Container Server-Metriken. 549
Adaptive Job Server-Metriken. 549
Crystal-Reports-Server-Metriken. 551
Web Intelligence Server-Metriken. 554

34 Server-Platzhalter. 556
34.1 Server- und Knotenplatzhalter. 556

35 Verwalten kryptografischer Schlüssel. 566
35.1 Verwalten von Kryptografieschlüsseln in der CMC. 566
Status von Kryptografieschlüsseln. 566
Anzeigen der einem Kryptografieschlüssel zugeordneten Objekte. 568
35.2 Erstellen eines neuen Kryptografieschlüssels. 568
35.3 Löschen eines Kryptografieschlüssels aus dem System. 568
35.4 Sperren eines Kryptografieschlüssels. 569
35.5 Kryptografieschlüssel als gefährdet markieren. 569

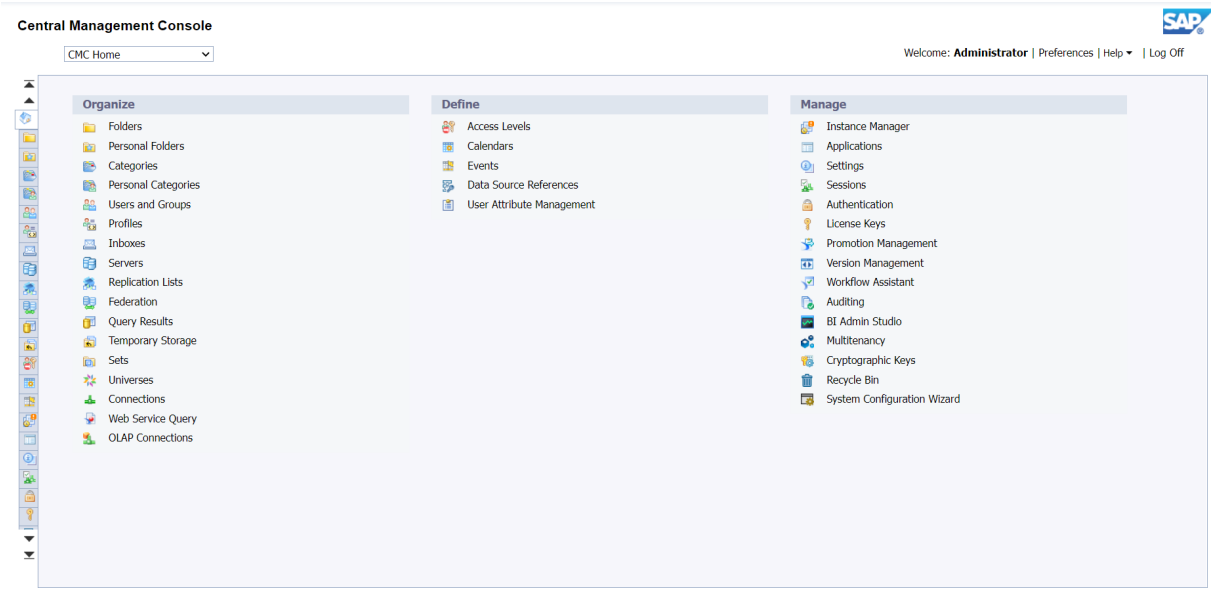
36 Hochstufverwaltung. 571
36.1 Hochstufverwaltung. 571
Herzlich willkommen bei der Hochstufverwaltung. 571
Erste Schritte mit der Hochstufverwaltung. 574
Verwenden der Hochstufverwaltung. 584
Hochstufen des vollständigen Repository-Inhalts mithilfe der Hochstufverwaltung. 605
Schritte zur vollständigen Systemhochstufung. 608
Verwenden der Befehlszeilenoption. 612
Verwenden des erweiterten Change and Transport System. 639
Verwendung des Hochstufverwaltungs-Assistenten. 651
36.2 Versionsverwaltung. 664
Mehrere Versionen von BI-Ressourcen verwalten. 664
Apache Subversion als Versionsverwaltungssystem verwenden. 666
Vergleichen von verschiedenen Versionen desselben Auftrags. 667
Aktualisieren von Subversion-Inhalten. 667

1 Central Management Console

1.1 Central Management Console

Die Central Management Console (CMC) ist ein webbasiertes Tool, mit dem fast alle administrativen Routineaufgaben ausgeführt werden können, darunter die Verwaltung von Benutzern, Inhalten und Servern.

Alle Benutzer mit gültigen Anmeldedaten für die Business Intelligence (BI) Plattform können sich bei der CMC anmelden und Einstellungen vornehmen. Benutzer, die nicht Mitglied der Administratorengruppe sind, können die Verwaltungsaufgaben jedoch erst ausführen, nachdem ihnen die entsprechenden Zugriffsrechte für eine Aufgabe erteilt wurden.



Der Zugriff auf die CMC kann auf zwei Arten erfolgen — aus Ihrem Browser oder durch die Auswahl von *Programme* > *SAP Business Intelligence* > *SAP BusinessObjects BI Plattform 4* > *SAP BusinessObjects BI Plattform Central Management Console* in Windows.

1.2 Anmelden bei der CMC

Sie können sich nur bei einer Sitzung der Central Management Console (CMC) anmelden. (Sie können nicht mehrere Sitzungen der CMC in separaten Browserregisterkarten oder -fenstern ausführen.)

1. Geben Sie die URL zur CMC in einen Browser ein.

   Die Standard-URL lautet `http://<Webserver>:8080/BOE/CMC/`. In Ihrer Implementierung ist möglicherweise eine benutzerdefinierte URL konfiguriert.

Ersetzen Sie `<Webserver>` durch den Namen des Webserverrechners. Wenn das virtuelle Standardverzeichnis auf dem Webserver geändert wurde, geben Sie die entsprechende URL ein. Ändern Sie ggf. die Standardportnummer in die Nummer, die während der Installation bereitgestellt wurde.

2. Geben Sie den Namen des Central Management Server (CMS) in das Feld *System* ein.
3. Falls sich ein Administrator Ihres Unternehmens zum ersten Mal an der CMC anmeldet, geben Sie **`Administrator`** als Benutzername und das Standardkennwort ein, das während der Installation erstellt wurde.

   Geben Sie nach der ersten Anmeldung Ihren Benutzernamen und Ihr Kennwort ein.

   Wenn Sie die LDAP-Authentifizierung verwenden, können Sie sich über ein Konto anmelden, das der Administratorgruppe zugeordnet wurde.
4. Wählen Sie in der Liste *Authentifizierung* den Eintrag *Enterprise* aus.

   In der Liste werden auch Windows AD, LDAP und andere Authentifizierungmethoden angezeigt. Benutzerkonten und Gruppen von Drittherstellern müssen jedoch der BI-Plattform zugeordnet werden, bevor Sie sie verwenden können.
5. Klicken Sie auf *Anmelden*.

Die CMC wird gestartet, und das Fenster *CMC-Starseite* wird angezeigt.

> **Hinweis**
>
> Die Benutzersitzung wird freigegeben, sobald der Benutzer den Browser schließt.

Wählen Sie zukünftig unter Windows *Start* > *Alle Programme* > *SAP Business Intelligence* > *SAP BusinessObjects BI 4* > *Central Management Console von SAP BusinessObjects Business Intelligence*, um die CMC zu starten. Wenn Ihre CMC auf einem Web Application Container Server (WACS) gehostet wird, wählen Sie *Start* > *Alle Programme* > *SAP Business Intelligence* > *SAP BusinessObjects BI 4* > *WACS-Centrale-Management-Console von SAP BusinessObjects BI*.

1.3 Navigieren in der CMC

Zur Navigation in der Central Management Console (CMC) stehen zwei Möglichkeiten zur Verfügung.

- Klicken Sie auf die Symbole links vom Fenster, oder klicken Sie auf die Links unter *Organisieren*, *Definieren* oder *Verwalten*.
- Wählen Sie die Optionen in der Liste *CMC-Startseite* oben links im Fenster.

Wenn Sie in der *Strukturansicht* durch Auswahlen navigieren, in denen viele untergeordnete Objekte enthalten sind, werden möglicherweise nicht alle untergeordneten Objekte angezeigt. Verwenden Sie die paginierte Objektliste, um untergeordnete Objekte zu suchen.

1.4 Festlegen der CMC-Einstellungen

Im Bereich *Einstellungen* der Central Management Console (CMC) können Sie die Administrationsansicht der BI-Plattform anpassen. In der CMC vorgenommene Einstellungen wirken sich auf das Verhalten von Objekten in der CMC und im BI-Launchpad aus.

Die CMC-Einstellungen werden standardmäßig auf die Plattform und das Launchpad angewendet. Die Benutzer können jedoch persönliche Einstellungen im BI-Launchpad festlegen, mit denen die CMC-Einstellungen überschrieben werden (und zwar so lange, bis die BI-Plattform mit einer neuen Softwareversion oder einem Patch aktualisiert wird). Bei allen Plattform-Aktualisierungen werden alle Einstellungen auf die Standard-CMC-Einstellungen zurückgesetzt.

Wenn ein Benutzer zwei oder mehr Benutzergruppen in der BI-Plattform angehört, zeigt das BI-Launchpad nur die Einstellungen einer Gruppe an.

1. Melden Sie sich bei der CMC an, und klicken Sie oben rechts im CMC-Fenster auf *Einstellungen*.
2. Legen Sie im Dialogfeld *Einstellungen* die Optionen wie gewünscht fest, und klicken Sie auf *Speichern und schließen*.

2 Systemkonfigurationsassistent

2.1 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.

2.2 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 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.

> **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.

2.3 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 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,

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.

2.4 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 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

2.5 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 24]

2.6 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.

Weitere Informationen

Verwenden von Antwortdateien [Seite 25]

2.6.1 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`

- `-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
# ******************************************************
# ***************** 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:

- 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.

3 Verwalten von Benutzern und Gruppen

3.1 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.

3.1.1 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.
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 gemäß den für die Enterprise-Authentifizierung definierten Kennwortkriterien 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.

> **Hinweis**
>
> Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mit einer Namenslizenz erstellt wurden, ist auf 10 Sitzungen beschränkt. Wenn ein Namenslizenzbenutzer versucht, eine 11. gleichzeitige Anmeldesitzung herzustellen, zeigt das System eine entsprechende Fehlermeldung an. Um eine weitere Anmeldesitzung öffnen zu können, muss eine der bestehenden Sitzungen geschlossen werden.
>
> Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mittels einer Prozessorlizenz oder einer Lizenz für Öffentliche Dokumente erstellt wurde, unterliegt jedoch keiner Einschränkung.

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.

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

3.1.2 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.

   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 46]

3.1.3 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 Drittsteller-System eingerichtet wurde und einer Drittsteller-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 für die Löschbestätigung wird angezeigt, welches Sie darüber informiert, dass es sich beim Benutzer um den Eigentümer eines oder mehrerer Objekte handelt.
4. Wählen Sie *OK*.
   Das Benutzerkonto wird gelöscht.

Weitere Informationen

So ändern Sie ein Benutzerkonto [Seite 30]
So deaktivieren Sie einen Alias [Seite 48]

3.1.4 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.

3.1.5 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*.

3.1.6 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*.
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.

3.1.7 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 33]

3.1.8 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.
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.

3.1.9 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.
- 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.

> **Hinweis**
>
> Nur Benutzer, die der Standardadministratorengruppe angehören, können Benutzer in Massenvorgängen hinzufügen. Diese Funktion wird für delegierte Administratoren nicht unterstützt.

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*.

3.1.10 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.

3.1.11 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*.

3.1.12 Hinzufügen der Registerkarte "Anpassung" zu einem Benutzer oder einer Gruppe

Sie benötigen das Recht „Objekte bearbeiten“, um eine Benutzergruppe zu bearbeiten.

Sie können der CMC die Registerkarte *Anpassung* für eine Anwendung (wie Web Intelligence) oder BI-Launchpad) für eine bestimmte Benutzergruppe hinzufügen.

1. Wechseln Sie zum Verwaltungsbereich *Benutzer und Gruppen* der CMC.
2. Klicken Sie im Navigationsbereich auf *Gruppenliste*, und klicken Sie mit der rechten Maustaste auf eine Benutzergruppe und wählen *Anpassung*.
3. Klicken Sie im Dialogfeld *Anpassung* unter *Anpassung* im Navigationsbereich auf die Anwendung, für die die Registerkarte hinzugefügt werden soll.

4. Klicken Sie auf *Speichern und schließen*.

3.1.13 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:

- 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 33]

3.1.13.1 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*.

3.1.13.2 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.
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*.

3.1.14 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.

3.1.14.1 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*.

> **Hinweis**
>
> Wenn Sie das Kennwort eines Benutzers ändern, wird dieser von allen laufenden Sitzungen abgemeldet und auf die Startseite weitergeleitet, um sich erneut anzumelden.

3.1.14.2 Allgemeine Kennworteinstellungen ändern

> **Hinweis**
>
> Inaktive Benutzerkonten werden nicht automatisch deaktiviert.

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.

   Kennworteinstellungen

Kennworteinstellung	Standardwert	Minimum	Empfohlener Höchstwert
Mindestens N Zeichen	8 Zeichen	6 Zeichen	255 Zeichen
Darf N Zeichen nicht überschreiten	255 Zeichen	13 Zeichen	255 Zeichen
Kennwort muss alle N Tage geändert werden.	30 Tage	2 Tage	100 Tage
Die letzten N Kennwörter dürfen nicht wiederverwendet werden	3 Kennwörter	1 Kennwort	100 Kennwörter
Mindestens N Minuten bis zur Änderung des Kennworts warten	0 Minuten	0 Minuten	100 Minuten

Kennworteinstellung	Standardwert	Minimum	Empfohlener Höchstwert
Konto nach N fehlgeschlagenen Anmeldeversuchen deaktivieren	10 Fehlschläge	1 Fehlschläge	100 Fehlschläge
Zähler für fehlgeschlagene Anmeldungen nach N Minuten zurücksetzen	5 Minuten	1 Minute	100 Minuten
Konto nach N Minuten wieder aktivieren	5 Minuten	0 Minuten	100 Minuten

> **Hinweis**
>
> Wenn Sie eine Aktualisierung von einer niedrigeren Version von SAP BusinessObjects Business Intelligence Platform auf eine höhere Version oder eine Erweiterungsinstallation durchführen wollen, setzen Sie *Konto nach N fehlgeschlagenen Anmeldeversuchen deaktivieren* auf den Standardwert.

> **Hinweis**
>
> Die oben genannten Regeln gelten nur für Enterprise-Benutzer und nicht für andere Authentifizierungstypen Dritter.

4. Klicken Sie auf *Aktualisieren*.

3.1.15 Aktivieren der vertrauenswürdigen Authentifizierung

> **Hinweis**
>
> Die vertrauenswürdige Authentifizierung wird nur für BI-Launchpad unterstützt und ist für die CMC nicht verfügbar.

Die Benutzer ziehen es vor, sich einmal beim System anzumelden, ohne Kennwörter mehrere Male während einer Sitzung eingeben zu müssen. Die vertrauenswürdige Authentifizierung stellt eine Einzelanmeldungslösung für die Integration Ihrer BI-Plattform-Authentifizierungslösung in Authentifizierungslösungen anderer Hersteller dar. Anwendungen, die eine Vertrauensstellung beim CMS haben, können die vertrauenswürdige Authentifizierung verwenden, damit sich Benutzer ohne Angabe ihrer Kennwörter anmelden können.

Zum Aktivieren der vertrauenswürdigen Authentifizierung müssen sowohl der Server als auch der Client konfiguriert werden.

3.1.15.1 Konfigurieren des Servers für die Verwendung der vertrauenswürdigen Authentifizierung

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
2. Doppelklicken Sie auf *Enterprise*.
   Das Dialogfeld *Enterprise* wird angezeigt.
3. Wählen Sie *Vertrauenswürdige Authentifizierung ist aktiviert*.
4. Erstellen Sie einen gemeinsamen geheimen Schlüssel für die Benutzer.

   > **Hinweis**
   >
   > Anhand des gemeinsamen geheimen Schlüssels erstellen der Client und der CMS ein Kennwort für die vertrauenswürdige Authentifizierung. Mithilfe dieses Kennwort wird Vertrauen hergestellt.

5. Geben Sie einen Timeout-Wert für vertrauenswürdige Authentifizierungsanforderungen ein.

   > **Hinweis**
   >
   > Der Timeout-Wert legt fest, wie lange der CMS auf den IEnterpriseSession.logon()-Aufruf von der Clientanwendung wartet.

6. Klicken Sie auf *Aktualisieren*.

3.1.15.2 Konfigurieren des Clients für die Verwendung der vertrauenswürdigen Authentifizierung

1. Erstellen Sie eine gültige Konfigurationsdatei auf dem Clientrechner.

   Für die Konfigurationsdatei gelten die folgenden Bedingungen:

   - Der Name der Datei muss `TrustedPrincipal.conf` lauten.
   - Die Datei muss im Verzeichnis `businessobjects_root/win32_x86/` gespeichert werden.
   - Die Datei muss die Anweisung `SharedSecret=<secretPassword>` enthalten, wobei `<secretPassword>` das Kennwort für die vertrauenswürdige Authentifizierung ist.

2. Verwenden Sie den Sitzungsmanager, um einen vertrauenswürdigen Prinzipal zu erstellen sich beim CMS anzumelden:

```
ISessionMgr sessionMgr = CrystalEnterprise.getSessionMgr();
ITrustedPrincipal trustedPrincipal =
sessionMgr.createTrustedPrincipal("userName", "cmsName");
IEnterpriseSession enterpriseSession = sessionMgr.logon(trustedPrincipal);
```

3.1.16 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.

Weitere Informationen

So weisen Sie einer Zugriffskontrollliste für ein Objekt Prinzipale hinzu [Seite 50]

3.1.17 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

Verwalten von Sicherheitseinstellungen für Objekte in der CMC [Seite 49]

3.1.18 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:

- 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.

3.1.18.1 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:
   - 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*.

3.1.19 Festlegen der Einstellungen für das fiorisierte BI-Launchpad für Benutzergruppen in der CMC

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

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

Benutzer können ihre eigenen Einstellungen im fiorisierten BI-Launchpad definieren, und diese Einstellungen übersteuern die Standardwerte. Sie können jederzeit zu den Standardeinstellungen zurückkehren. Weitere Informationen finden Sie im Abschnitt *Festlegen der Seiteneinstellungen* im *Benutzerhandbuch für das fiorisierte Business-Intelligence-Launchpad*.

Wenn der Administrator jedoch die Standardeinstellungen des fiorisierten BI-Launchpads in der CMC ändert, haben die Standardwerte Vorrang vor den benutzerdefinierten Werten.

3.1.19.1 Festlegen der Einstellungen für das fiorisierte BI-Launchpad für eine Benutzergruppe

1. Wechseln Sie zum Bereich *Benutzer- und Gruppenmanagement* der CMC.
2. Wählen Sie unter *Gruppenliste* die Benutzergruppe aus, für die Sie die Einstellungen des fiorisierten BI-Launchpads ändern möchten.

3. Klicken Sie mit der rechten Maustaste, und wählen Sie *Einstellungen für das fiorisierte BI-Launchpad*.
4. Deaktivieren Sie das Kontrollkästchen *Keine Einstellungen definiert*.
5. Zur Anpassung der Registerkarte *Startseite* führen Sie eine der folgenden Aktionen aus, um auf der Registerkarte die gewünschte Startseite zu wählen:

Optionen für die Startseite	Aktion
Standard-Startseite des fiorisierten BI-Launchpads anzeigen	Wählen Sie *Standard-Startseite*.
Eine bestimmte Startseite anzeigen	Wählen Sie *Startseite auswählen* und anschließend: 1. Wählen Sie im Feld *Landing Page* eine Landing Page aus. • *Meine Startseite* • *Zeitgesteuerte Verarbeitung* • *Posteingang* • *Ordner* • *Papierkorb* 2. Wählen Sie im Feld *Dokumente auflisten als Kachelansicht (Standard)* oder *Listenansicht*. 3. Wählen Sie im Feld *Landing Filter* einen Landing Filter aus. • *Alles anzeigen* • *Meine Dokumente* • *Alle Kategorien* • *Meine Favoriten* • *Meine zuletzt angezeigten* • *Meine zuletzt ausgeführten* Wählen Sie aus *Meine Ordner*, *Öffentliche Ordner*, *Persönliche Kategorien* und *Öffentliche Kategorien* ein Objekt aus, das Sie standardmäßig als Landing Page anzeigen möchten.
Einen bestimmten Bericht als Startseite anzeigen	Wählen Sie *Bericht auswählen*, und klicken Sie dann auf *Dokumente durchsuchen*, um ein Dokument aus *Meine Ordner* oder *Öffentliche Ordner* auszuwählen.
Eine Kategorie als Startseite anzeigen	Wählen Sie *Kategorie auswählen*, und klicken Sie dann auf *Kategorien durchsuchen*, um eine Kategorie aus *Persönliche Kategorien* oder *Öffentliche Kategorien* auszuwählen.

6. Wählen Sie im Feld *Wählen Sie die auf der Registerkarte "Dokumente" anzuzeigende Spalte aus* die Spalteneigenschaften aus:
   - *Typ*
   - *Letzte Ausführung*
   - *Instanzen*

- *Beschreibung*
- *Angelegt von*
- *Zuletzt aktualisiert*
- *Erstellt am*
- *Speicherort (Kategorien)*
- *Meine Favoriten (Startseite)*
- *Status (zeitgesteuert)*
- *Zeit der Instanz (zeitgesteuert)*
- *Ordnerpfad*

> ⓘ Hinweis
>
> Die Spalten *Typ*, *Beschreibung*, *Zuletzt aktualisiert*, *Meine Favoriten (Startseite)*, *Status (zeitgesteuert)* und *Zeit der Instanz (zeitgesteuert)* sind standardmäßig ausgewählt. Sie können die Auswahl der Spalten, die Sie anzeigen möchten, ändern.

7. Wählen Sie *Speichern und schließen*.

Damit die vom Administrator definierten Einstellungen auf der Oberfläche angezeigt werden, müssen sich Benutzer am fiorisierten BI-Launchpad anmelden, *Einstellungen* > *Kontoeinstellungen* > *Seiteneinstellungen* wählen und die Option *Administratoreinstellungen verwenden* aktivieren.

3.2 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.

3.2.1 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`**.
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.

3.2.2 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.

3.2.3 So weisen Sie einen Alias eines anderen Benutzers zu

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

> ⓘ 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 `UMSCHALTTASTE` + `Klicken` oder `STRG` + `Klicken`.

7. Klicken Sie auf *OK*.

3.2.4 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.

3.2.5 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 47]

4 Festlegen von Rechten

4.1 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:

- 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

4.1.1 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
     Von Zugriffsberechtigung
     Objekttyp
     Der Name des Rechts

- Sortieren Sie die Liste der angezeigten Rechte aufsteigend oder absteigend nach den folgenden Kriterien:

  Zusammenstellung
  Typ
  Name des Rechts
  Status des Rechts (Gewährt, Verweigert oder Nicht angegeben)

Zusätzlich können Sie auf einen der Links in der Spalte *Quelle* klicken, um die Quelle der übernommenen Rechte anzuzeigen.

4.1.2 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.
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 50]

4.1.3 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 50]

4.1.4 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 50]
Ändern der Sicherheit für einen Prinzipal auf einem Objekt [Seite 50]

4.1.5 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
  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.

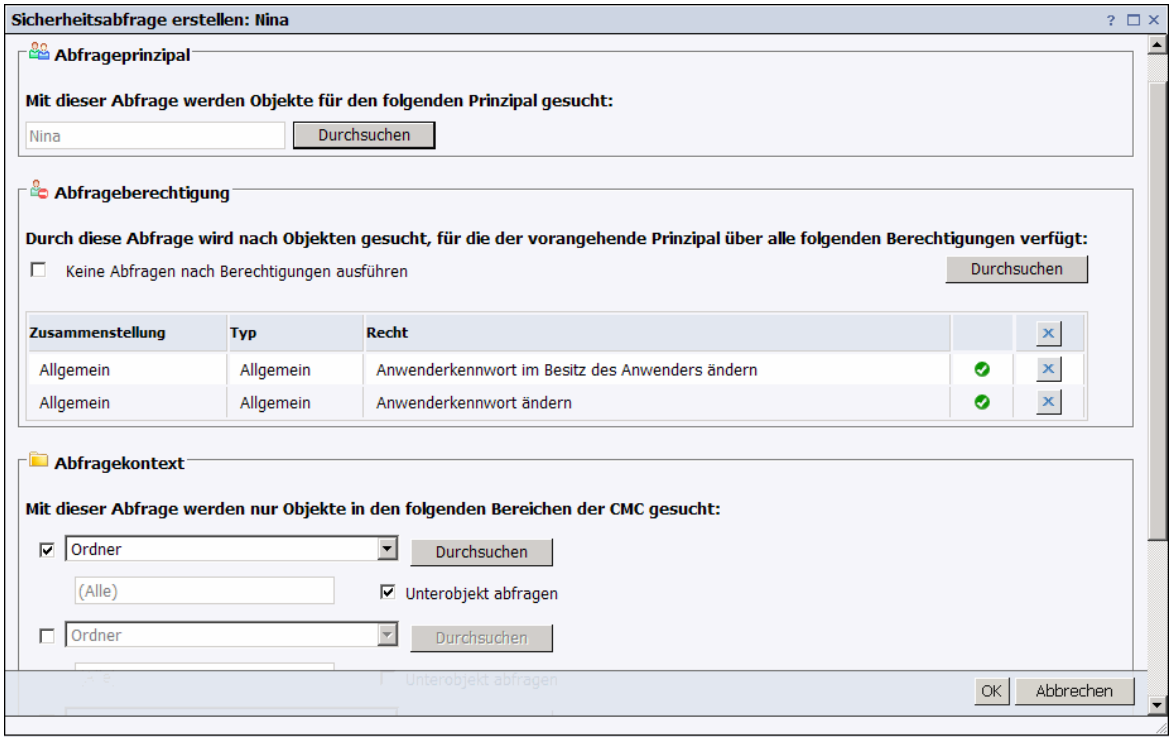
Wenn Sie eine Sicherheitsabfrage ausführen, werden die Ergebnisse im Bereich *Abfrageergebnisse* angezeigt, der sich im *Strukturbereich* unterhalb von *Sicherheitsabfragen* befindet. Wenn Sie eine Sicherheitsabfrage optimieren möchten, können Sie eine zweite Abfrage in den Ergebnissen der ersten Abfrage 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.

4.1.5.1 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*.



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.

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.

4.2 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.

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.	*Ansichts*recht 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.

Aufgabe für Zugriffsberechtigung	Erforderliche Rechte
Erstellen einer Zugriffsberechtigung	*Hinzufüge*recht für den Ordner *Zugriffsberechtigungen* der obersten Ebene
Anzeigen genau abgestimmter Rechte in einer Zugriffsberechtigung	*Ansichts*recht für die Zugriffsberechtigung
Zuweisen einer Zugriffsberechtigung zu einem Subjekt, das einem Objekt zugewiesen ist	*Ansichts*recht für die Zugriffsberechtigung

Aufgabe für Zugriffsberechtigung	Erforderliche Rechte
	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 *Bearbeitungs*recht für die Zugriffsberechtigung
Löschen einer Zugriffsberechtigung	*Ansichts*- und *Lösch*recht für die Zugriffsberechtigung
Klonen einer Zugriffsberechtigung	*Ansichts*recht für die Zugriffsberechtigung *Kopier*recht für die Zugriffsberechtigung *Hinzufüge*recht für den Ordner *Zugriffsberechtigungen* der obersten Ebene

4.2.1 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.

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.

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.2.5 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.

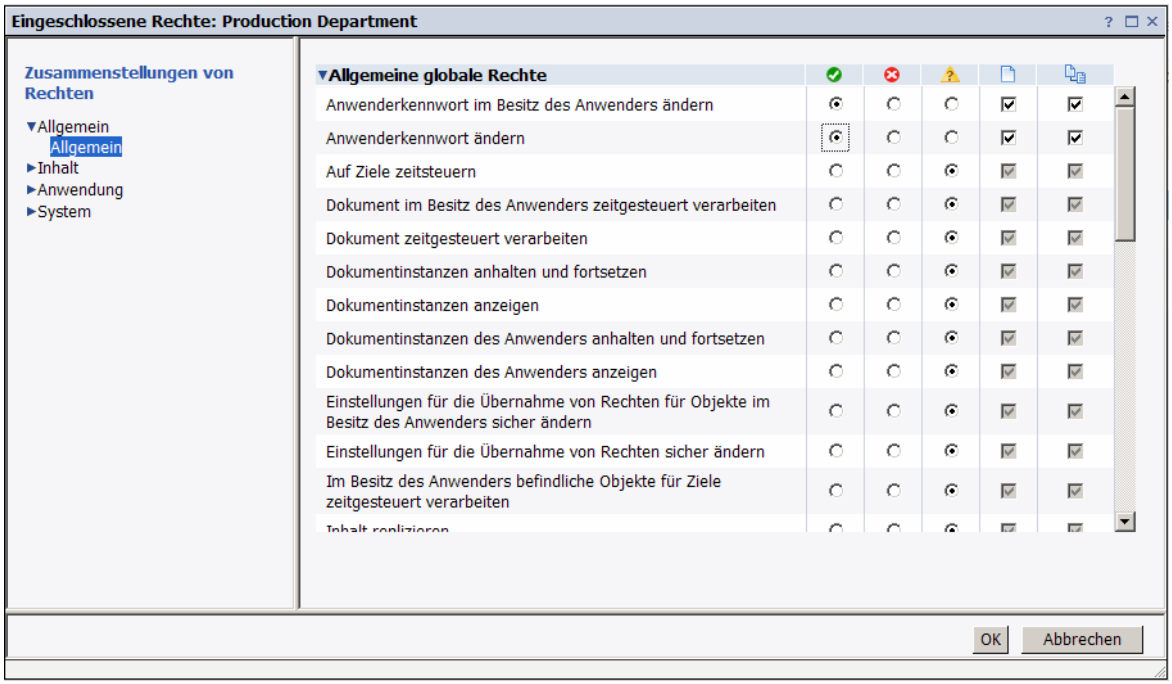
   Es wird ein Dialogfeld mit Informationen über die Objekte angezeigt, auf die sich diese Zugriffsberechtigung auswirkt. Wenn Sie die Zugriffsberechtigung nicht löschen möchten, klicken Sie auf *Abbrechen*, um das Dialogfeld zu schließen.
3. Klicken Sie auf *Löschen*.
   Die Zugriffsberechtigung wird gelöscht, und Sie kehren zum Bereich *Zugriffsberechtigungen* zurück.

4.2.6 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.

4.2.7 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 *Ansichts*rechte 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.

4.2.8 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.

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.

Weitere Informationen

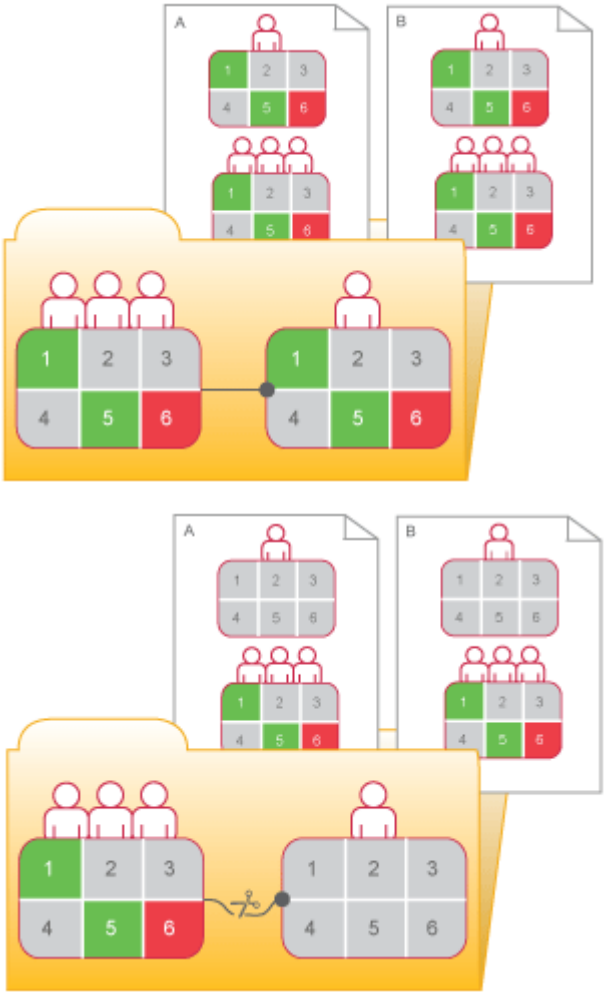
Föderation [Seite 391]
Verfolgen der Beziehung zwischen Zugriffsberechtigungen und Objekten [Seite 59]

4.3 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.



Auflösen der Übernahme

4.3.1 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*.

5 Authentifizierung

5.1 Übersicht

5.1.1 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.

5.2 Enterprise-Authentifizierung

5.2.1 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 Plattform die Benutzer- und Gruppeninformationen in der eigenen Datenbank. 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.

Weitere Informationen

Einstellungen der Enterprise-Authentifizierung [Seite 65]
Ändern der Enterprise-Einstellungen [Seite 66]
Allgemeine Kennworteinstellungen ändern [Seite 67]

5.2.2 Einstellungen der Enterprise-Authentifizierung

Einstellungen	Optionen	Beschreibung
Kennwortbeschränkungen	*Kennwörter mit Groß- und Kleinschreibung erzwingen*	Mit dieser Option wird sichergestellt, dass das Kennwort mindestens einen Groß- und einen Kleinbuchstaben enthält. **Hinweis** Diese Option ist standardmäßig aktiviert. Sie kann bei Bedarf vom Administrator deaktiviert werden.
	Ziffer(n) im Kennwort erzwingen	Mit dieser Option wird sichergestellt, dass Kennwörter mindestens eine Ziffer enthalten.
	Sonderzeichen im Kennwort erzwingen	Mit dieser Option wird sichergestellt, dass Kennwörter mindestens ein Sonderzeichen enthalten.
	Muss mindestens N Zeichen enthalten, wobei N folgendes ist	Mit dieser Option wird sichergestellt, dass Kennwörter mindestens N Zeichen lang sind.
	Darf N Zeichen nicht überschreiten, wobei N Folgendes ist:	Mit dieser Option wird sichergestellt, dass Kennwörter N Zeichen nicht überschreiten dürfen.
	Darf keine der folgenden Zeichenfolgen enthalten	Diese Option stellt sicher, dass das Kennwort keine eingeschränkten Zeichenfolgen enthält. Der Standardwert hierfür lautet wie folgt: Kennwort 12345678 Administrator.
Benutzerbeschränkungen	*Kennwort muss alle N Tage geändert werden.*	Diese Option stellt sicher, dass Kennwörter durch regelmäßige Erneuerung nicht zum Problem werden.

Einstellungen	Optionen	Beschreibung
	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.
	Kennwort muss nach N Tage(n) der Inaktivität geändert werden	Diese Option stellt sicher, dass sich das Kennwort nach N Tagen der Inaktivität ändert.
	Initiales Kennwort muss nach N Tage(n) geändert werden	Diese Option stellt sicher, dass sich das Initialkennwort nach N Tagen ändert.
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
OpenID-Connect-Authentifizierung	*OpenID-Connect-Authentifizierung wurde aktiviert*	Um die *OpenID-Connect-Authentifizierung* zu aktivieren, aktivieren Sie das Kontrollkästchen *OpenID-Connect-Authentifizierung wurde aktiviert*. Bei der Authentifizierung über OpenID Connect wird in der BI-Plattform eine interne Enterprise-Sitzung erstellt.

5.2.2.1 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.

5.2.2.2 Allgemeine Kennworteinstellungen ändern

> **Hinweis**
>
> Konten, die längere Zeit nicht verwendet werden, werden nicht automatisch deaktiviert. Administratoren müssen inaktive Konten automatisch löschen.

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	Standardwert	Minimum	Empfohlener Höchstwert
Darf keine der folgenden Zeichenfolgen enthalten	Kennwort 12345678 Administrator	1 Zeichen	25550 Zeichen
Mindestens N Zeichen	8 Zeichen	6 Zeichen	255 Zeichen
Darf N Zeichen nicht überschreiten	255 Zeichen	13 Zeichen	255 Zeichen
Kennwort muss alle N Tage geändert werden.	30 Tage	2 Tage	100 Tage
Die letzten N Kennwörter dürfen nicht wiederverwendet werden	3 Kennwörter	1 Kennwort	100 Kennwörter
Mindestens N Minuten bis zur Änderung des Kennworts warten	0 Minuten	0 Minuten	100 Minuten
Kennwort muss nach N Tage(n) der Inaktivität geändert werden	20 Tage	2 Tage	365 Tage
Initiales Kennwort muss nach N Tage(n) geändert werden	7 Tage	2 Tage	15 Tage

Kennworteinstellung	Standardwert	Minimum	Empfohlener Höchstwert
Konto nach N fehlgeschlagenen Anmeldeversuchen deaktivieren	10 Fehlschläge	1 Fehlschläge	100 Fehlschläge
Zähler für fehlgeschlagene Anmeldungen nach N Minuten zurücksetzen	5 Minuten	1 Minute	100 Minuten
Konto nach N Minuten wieder aktivieren	5 Minuten	0 Minuten	100 Minuten

4. Klicken Sie auf *Aktualisieren*.

5.3 LDAP-Authentifizierung

5.3.1 LDAP-Authentifizierung

Die BI-Plattform unterstützt die LDAP-Authentifizierung für Benutzer- und Gruppenkonten. Bevor sich Benutzer mit ihrem LDAP-Benutzernamen und -Kennwort im 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 Enterprise-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.

Der Assistent für die LDAP-Konfiguration wird bereitgestellt, um die Administratoren bei den folgenden Aufgaben zu unterstützen:

- Konfigurieren des LDAP-Hosts
- Vorbereiten des LDAP-Servers für SSL (wenn erforderlich)
- Konfigurieren des LDAP-Plugins für SiteMInder (wenn erforderlich)

Mit der SAP-Authentifizierungsanwendung wird konfiguriert, wie sich Benutzer in der BI-Plattform authentifizieren.

> **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.

Weitere Informationen

LDAP-Hosts konfigurieren [Seite 69]
Zuordnen von LDAP-Gruppen [Seite 78]
Konfigurieren der SSL-Einstellungen für die LDAP-Serverauthentifizierung oder gegenseitige Authentifizierung [Seite 72]
Konfigurieren des LDAP-Plugins für SiteMinder [Seite 77]

5.3.1.1 LDAP-Hosts konfigurieren

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.

   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 Ihr LDAP-Server anonyme Bindungen zulässt, lassen Sie diesen Bereich leer. BI-Plattform-Server und -Clients stellen die Bindung zum primären Host über eine anonyme Anmeldung her.

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 (kein SSO)*
    - *SiteMinder*
14. Klicken Sie auf *Weiter*, und wählen Sie die Art der Zuordnung von Aliasen und Benutzern zu BI-Plattform-Konten aus.

    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 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.

  > **Hinweis**
  >
  > Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mit einer Namenslizenz erstellt wurden, ist auf 10 Sitzungen beschränkt. Wenn ein Namenslizenzbenutzer versucht, eine 11. gleichzeitige Anmeldesitzung herzustellen, zeigt das System eine entsprechende Fehlermeldung an. Um eine weitere Anmeldesitzung öffnen zu können, muss eine der bestehenden Sitzungen geschlossen werden.
  >
  > Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mittels einer Prozessorlizenz oder einer Lizenz für Öffentliche Dokumente erstellt wurde, unterliegt jedoch keiner Einschränkung.

- *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.

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.

> **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 72]
Konfigurieren des LDAP-Plugins für SiteMinder [Seite 77]

5.3.2 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 anschließend 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.

Bei Windows-Systemen erfolgt die standardmäßige SSL-Kommunikation über TLS 1.2. Informationen zu Linux-Systemen finden Sie im SAP-Hinweis 2623529.

Weitere Informationen

LDAP-Hosts konfigurieren [Seite 69]

5.3.2.1 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.
	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 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>`

Ressource	Diese Aktion vor Beginn dieser Aufgabe durchführen
	`-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 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

Ressource	Diese Aktion vor Beginn dieser Aufgabe durchführen

	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*
     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*.

   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 77]

5.3.3 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

LDAP-Hosts konfigurieren [Seite 69]

5.3.3.1 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.

5.3.4 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.

5.3.4.1 LDAP-Gruppen mithilfe der BI-Plattform zuordnen

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 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 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.

     > **Hinweis**
     >
     > Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mit einer Namenslizenz erstellt wurden, ist auf 10 Sitzungen beschränkt. Wenn ein Namenslizenzbenutzer versucht, eine 11. gleichzeitige Anmeldesitzung herzustellen, zeigt das System eine entsprechende Fehlermeldung an. Um eine weitere Anmeldesitzung öffnen zu können, muss eine der bestehenden Sitzungen geschlossen werden.
     >
     > Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mittels einer Prozessorlizenz oder einer Lizenz für Öffentliche Dokumente erstellt wurde, unterliegt jedoch keiner Einschränkung.

   - *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 das System können 100 Zugriffslizenzen beispielsweise 250, 500 oder auch 700 Benutzer unterstützen.
7. Klicken Sie auf *Aktualisieren*.

5.3.4.2 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*.

5.4 Windows-AD-Authentifizierung

5.4.1 Windows AD-Authentifizierung

Die BI-Plattform unterstützt die Windows-AD-Authentifizierung für Benutzer- und Gruppenkonten. Bevor sich Benutzer mit ihrem Windows-AD-Benutzernamen und -Kennwort am System anmelden können, müssen Sie ihre Konten der BI-Plattform zuordnen.

Grundlegender Arbeitsablauf bei der Windows AD-Authentifizierung

Um die AD-Authentifizierung mit der BI-Plattform einzurichten, muss der folgende Ablauf eingehalten werden:

1. Aktivieren Sie das Windows AD-Sicherheits-Plugin, und ordnen Sie Benutzer und Gruppen zu.
2. Wählen Sie eine Authentifizierungsmethode:
   - Windows AD mit Kerberos
   - Windows AD mit NTLM
3. Legen Sie die Einzelanmeldung für BI-Plattform-Anwendungen fest. Dieser optionale Schritt kann mithilfe folgender Methoden erleichtert werden:
   - Windows AD mit Kerberos
   - Windows AD mit NTLM
   - Windows AD mit SiteMinder

5.4.2 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, 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.

  > **Hinweis**
  >
  > Die Konfiguration wurde nur mit SUSE Linux Enterprise 11 ausgeführt und getestet.

- Das Windows-AD-Plugin für die BI-Plattform unterstützt Domänen innerhalb mehrerer Forests.

5.4.3 Konfigurieren der Windows AD-Authentifizierung

Unabhängig vom verwendeten Protokoll (Kerberos oder NTLM) führen Sie die folgenden Schritte aus, um AD-Benutzern die Authentifizierung zu ermöglichen. Diese Schritte beinhalten Anleitungen zum Zuordnen von Windows AD-Benutzern und -Gruppen und zum zeitgesteuerten Verarbeiten von Aktualisierungen. Der unten stehende Ablauf enthält keine Schritte zum Konfigurieren von Windows AD mit SiteMinder.

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* ausgewählt ist.
4. Klicken Sie im Bereich *Eigenschaften der Windows AD-Konfiguration* auf den Link neben *AD-Verwaltungsname*.

   > **Hinweis**
   >
   > Bevor das Windows AD-Plugin nicht konfiguriert wurde, werden anstelle dieses Links zwei Anführungszeichen angezeigt. Nachdem die Konfiguration gespeichert wurde, enthält der Link die AD-Verwaltungsnamen.

5. Geben Sie Namen und Kennwort eines aktivierten Domänenbenutzerkontos ein. Die BI-Plattform verwendet dieses Konto, um Informationen von AD abzufragen.

   Bei den Anmeldedaten für die Administration können die folgenden Formate verwendet werden:

   - NT-Name (`Domänenname\Benutzername`)
   - UPN (`Benutzer@DNS_Domänenname`)

   Inhalte aus AD werden von der BI-Plattform nie geändert, hinzugefügt oder gelöscht. Die Informationen werden lediglich gelesen, sodass nur eine entsprechende Leseberechtigung erforderlich ist.

   > **Hinweis**
   >
   > Die AD-Authentifizierung wird nicht fortgesetzt, wenn das zum Lesen des AD-Verzeichnisses verwendete AD-Konto ungültig wird (beispielsweise, wenn das Kontokennwort geändert wird bzw. abläuft oder das Konto deaktiviert wird).

6. Geben Sie im Feld *Standard-AD-Domäne* die entsprechenden Informationen ein.

   > **Hinweis**
   >
   > - Gruppen der Standarddomäne können ohne Angabe des Domänennamenpräfixes zugeordnet werden.
   > - 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 bei der BI-Plattform anmelden.

7. Geben Sie im Bereich *Zugeordnete AD-Mitgliedsgruppen* im Feld *AD-Gruppe hinzufügen (Domäne\Gruppe)* die entsprechenden Informationen ein.

   Gruppen können mithilfe der folgenden Formate zugeordnet werden:

   - 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, können Sie dafür nur das NT-Namensformat (\\Servername\Gruppenname) verwenden. Windows AD unterstützt keine lokalen Benutzer. Dies bedeutet, dass lokale Benutzer, die einer zugeordneten lokalen Gruppe angehören, der BI-Plattform nicht zugeordnet werden. Daher können sie nicht auf das System zugreifen.

8. Klicken Sie auf *Hinzufügen*.

Die Gruppe wird zu der Liste hinzugefügt.

9. Wählen Sie unter *Authentifizierungsoptionen* eine der folgenden Optionen aus:
   - NTLM-Authentifizierung verwenden
   - Kerberos-Authentifizierung verwenden

   Wenn Sie Kerberos auswählen, müssen Sie den "Cachesicherheitskontext" auswählen, sofern Sie planen, die Einzelanmeldung bei der Datenbank zu konfigurieren. In die Konfiguration der Kerberos-Authentifizierung sind Ressourcen involviert, die über die CMC hinausgehen. Ausführliche Informationen über das Einrichten der Windows AD-Authentifizierung mit Kerberos finden Sie im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.

   > **Hinweis**
   >
   > Um die BI-Plattform für die Kerberos- und Windows-AD-Authentifizierung 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. 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 SPN und `DNS.COM` dem vollständig qualifizierten Domänennamen in Großbuchstaben entspricht.

10. Wenn Sie die Einzelanmeldung für Windows AD-Benutzer und -Gruppen einrichten möchten, wählen Sie *Einzelanmeldung für ausgewählten Authentifizierungsmodus aktivieren*.
11. Wählen Sie die Option im Bereich *Synchronisierung der Anmeldedaten*, um die Datenquellanmeldedaten des Windows AD-Benutzers zum Zeitpunkt der Anmeldung zu aktivieren und zu aktualisieren. Dadurch werden die Datenquelle und die aktuellen Anmeldedaten des Benutzers synchronisiert.
12. Geben Sie im Bereich *Optionen für AD-Aliase* an, wie neue Aliase zur BI-Plattform hinzugefügt und aktualisiert werden.
    a. Wählen Sie unter *Optionen für neuen Alias* aus, wie neue Aliase Enterprise-Konten zugeordnet werden. Wählen Sie eine der folgenden Optionen:
       - *Jeden neuen AD-Alias einem vorhandenen Benutzerkonto mit demselben Namen zuweisen*
         Verwenden Sie diese Option, wenn Sie wissen, dass einige Benutzer über ein bereits vorhandenes Enterprise-Konto mit demselben Namen verfügen. Vorhandenen Benutzern werden also 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 unter *Aktualisierungsoptionen für Aliase* aus, wie Aliasaktualisierungen für die Enterprise-Konten verwaltet werden. Wählen Sie eine der folgenden Optionen:
       - *Neue Aliase bei der Aliasaktualisierung erstellen*
         Aktivieren Sie diese Option, 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-Konto 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*
         Aktivieren Sie diese Option, wenn das zuzuordnende AD-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 unter *Optionen für neue Benutzer* an, wie neue Benutzer erstellt werden, indem Sie eine der folgenden Optionen auswählen:

- *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 das System können 100 Zugriffslizenzen beispielsweise 250, 500 oder auch 700 Benutzer unterstützen.

13. Um die zeitgesteuerte Verarbeitung der Aktualisierung von AD-Aliasen zu konfigurieren, klicken Sie auf *Aktualisierungen von AD-Aliasen zeitgesteuert verarbeiten*.
    a. Wählen Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* ein Wiederholungsintervall aus der Dropdown-Liste *Objekt ausführen* aus.
    b. Legen Sie weitere Zeitsteuerungsoptionen und -parameter nach Bedarf fest.
    c. Klicken Sie auf *Zeitgesteuert verarbeiten*.
    Bei der Aliasaktualisierung wird auch das Gruppendiagramm aktualisiert.
14. Im Bereich *Optionen für die Attributbindung* können Sie die folgenden optionalen Einstellungen auswählen:
    - *Vollständigen Namen und E-Mail-Adresse importieren*
      Falls aktiviert, werden die vollständigen Namen des AD-Benutzerkontos mit den Beschreibungen importiert und mit dem Benutzerobjekt in der BI-Plattform gespeichert.
    - *AD-Attributbindung soll Priorität vor LDAP-Attributbindung haben*
      Falls aktiviert, haben AD-Attribute in Szenarios, in denen sowohl Windows AD als auch LDAP aktiviert ist, Priorität.
15. Sie können Aktualisierungen von AD-Gruppendiagrammen im Bereich *Optionen für AD-Gruppendiagramm* konfigurieren.
    a. Klicken Sie auf *Aktualisierungen des AD-Gruppendiagramms zeitgesteuert verarbeiten*.
    Das Dialogfeld *Zeitgesteuerte Verarbeitung* wird angezeigt.
    b. Wählen Sie ein Wiederholungsintervall aus der Dropdown-Liste *Objekt ausführen*.
    c. Legen Sie weitere Optionen und Parameter für die zeitgesteuerte 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. Sie können die nächste zeitgesteuerte Aktualisierung für die AD-Gruppenkonten unter *Optionen für AD-Gruppendiagramm* anzeigen lassen.
16. Verwenden Sie die Einstellungen im Bereich *AD-Aktualisierung auf Abruf* um anzugeben, was aktualisiert werden soll. Sie können eine der folgenden Optionen auswählen:
    - *AD-Gruppen jetzt aktualisieren*

Aktivieren Sie diese Option, wenn Sie das Gruppendiagramm aktualisieren möchten. Die Aktualisierung wird erst ausgeführt, nachdem Sie auf *Aktualisieren* geklickt haben.

> **Hinweis**
>
> Diese Option wirkt sich auf alle zeitgesteuerten Aktualisierungen von Gruppendiagrammen aus. Die nächste zeitgesteuerte Aktualisierung von Gruppendiagrammen ist unter *Optionen für AD-Gruppendiagramm* aufgeführt.

- *AD-Gruppen und -Aliase jetzt aktualisieren*
  Aktivieren Sie diese Option, wenn Sie das Gruppendiagramm und Benutzeraliase aktualisieren möchten. Die Aktualisierungen werden erst ausgeführt, nachdem Sie auf *Aktualisieren* geklickt haben.

> **Hinweis**
>
> Diese Option wirkt sich auf alle zeitgesteuerten Gruppendiagramme oder Aktualisierungen aus. Die nächsten zeitgesteuerten Aktualisierungen sind unter *Optionen für AD-Gruppendiagramm* und *Optionen für AD-Aliase* aufgeführt.

- *AD-Gruppen und -Aliase jetzt nicht aktualisieren*
  Wenn Sie auf *Aktualisieren* klicken, werden die Gruppe noch die Benutzeraliase aktualisiert.

> **Hinweis**
>
> Diese Option wirkt sich auf alle zeitgesteuerten Gruppen- oder Aliasaktualisierungen aus. Die nächsten zeitgesteuerten Aktualisierungen sind unter *AD-Gruppenoptionen* und *Optionen für AD-Aliase* aufgeführt.

17. Klicken Sie auf *Aktualisieren*.
18. Klicken Sie auf *OK*.

5.4.4 Zuordnen von Windows AD-Gruppen

Bevor Sie Gruppen importieren, sollten Sie die Windows AD-Authentifizierung aktivieren.

Die Windows AD-Authentifizierungsanwendung wird zum Konfigurieren der Authentifizierung und Zuordnen von Windows AD-Gruppen verwendet. Ordnen Sie die Windows AD-Gruppen mithilfe der folgenden Schritte zu.

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* ausgewählt ist.
4. Klicken Sie im Bereich *Eigenschaften der Windows AD-Konfiguration* auf den Link neben *AD-Verwaltungsname*.
5. Geben Sie Namen und Kennwort eines aktivierten Domänenbenutzerkontos ein. Das System verwendet dieses Konto, um Informationen von AD abzufragen.

   Bei den Anmeldedaten für die Administration können die folgenden Formate verwendet werden:

   - NT-Name (`Domänenname\Benutzername`)
   - UPN (`Benutzer@DNS_Domänenname`)

Inhalte aus AD werden von der BI-Plattform nie geändert, hinzugefügt oder gelöscht. Die Informationen werden lediglich gelesen, sodass nur eine entsprechende Leseberechtigung erforderlich ist.

> **Hinweis**
>
> Die AD-Authentifizierung wird nicht fortgesetzt, wenn das zum Lesen des AD-Verzeichnisses verwendete AD-Konto ungültig wird (beispielsweise, wenn das Kontokennwort geändert wird bzw. abläuft oder das Konto deaktiviert wird).

6. Geben Sie im Feld *Standard-AD-Domäne* die entsprechenden Informationen ein.

> **Hinweis**
>
> - Gruppen der Standarddomäne können ohne Angabe des Domänennamenpräfixes zugeordnet werden.
> - 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 bei der BI-Plattform anmelden.

7. Geben Sie im Bereich *Zugeordnete AD-Mitgliedsgruppen* im Feld *AD-Gruppe hinzufügen (Domäne\Gruppe)* die entsprechenden Informationen ein.

   Gruppen können mithilfe der folgenden Formate zugeordnet werden:

   - Security Account Manager-Kontoname (SAM), der auch als NT-Name bezeichnet wird (`Domänenname\Gruppenname`)
   - DN (`cn=GroupName, ....., dc=DomainName, dc=com`)

> **Hinweis**
>
> Wenn Sie eine lokale Gruppe zuordnen möchten, können Sie dafür nur das NT-Namensformat (\\Servername\Gruppenname) verwenden. Windows AD unterstützt keine lokalen Benutzer. Dies bedeutet, dass lokale Benutzer, die einer zugeordneten lokalen Gruppe angehören, der BI-Plattform nicht zugeordnet werden. Daher können sie nicht auf das System zugreifen.

8. Klicken Sie auf *Hinzufügen*.
9. Geben Sie im Bereich *Zugeordnete AD-Mitgliedsgruppen* im Feld *AD-Gruppe suchen (Domäne\Gruppe)* die entsprechenden Informationen ein.

   Die Liste wird nach der gewünschten Gruppe durchsucht. Über *Anzeigen* können Sie außerdem eine vollständige Liste der AD-Gruppen in einem separaten Dialogfeld anzeigen.
10. Klicken Sie auf *Aktualisieren*.
11. Wählen Sie *OK*.

5.5 SAP-Authentifizierung

5.5.1 SAP-Authentifizierung

Die SAP-Authentifizierung ermöglicht es SAP-Benutzern, sich mit ihrem SAP-Benutzernamen und -Kennwort bei der BI-Plattform anzumelden, ohne dass das Kennwort im BI-Plattform-System gespeichert werden

muss. Außerdem bietet Ihnen die SAP-Authentifizierung die Möglichkeit, Informationen über Benutzerrollen in SAP beizubehalten und diese Rolleninformationen in der BI-Plattform zu verwenden, um Rechte für Administrationsaufgaben oder den Zugriff auf Inhalte zuzuweisen.

Mit der SAP-Authentifizierungsanwendung erfolgt sowohl die Konfiguration der Art und Weise, wie sich Benutzer in der BI-Plattform authentifizieren, als auch der Import und die Aktualisierung von Rollen aus dem SAP-System.

Die Anwendung ist in vier Registerkarten unterteilt, die in der folgenden Tabelle beschrieben werden.

Registerkarte	Beschreibung
Berechtigungssysteme	Einstellungen für die Identifizierung des SAP-Systems, das in die BI-Plattform integriert wird.
Rollenimport	Einstellungen für die Identifizierung der Rollen, die in die BI-Plattform importiert werden sollen.
SNC-Einstellungen	Einstellungen für die Konfiguration der Secure Network Communication (SNC) zwischen dem SAP-Zielsystem und der BI-Plattform.
Optionen	Einstellung für die Aktivierung der SAP-Authentifizierung. Diese Registerkarte enthält außerdem Einstellungen für: • Verbindungsoptionen • Importieren von Benutzern in das BI-Plattform-System • das Importieren von Schlüsseldateien zum Einrichten des SAP-Einzelanmeldungsdiensts (Single Sign-On, SSO)
Benutzeraktualisierung	Einstellungen für die zeitgesteuerte Verarbeitung und die Ausführung von Aktualisierungen für importierte SAP-Rollen.

Weitere Informationen

Verbinden mit SAP-Berechtigungssystemen [Seite 87]
Einstellen von SAP-Authentifizierungsoptionen [Seite 89]
Importieren von SAP-Rollen [Seite 93]
Aktualisieren von SAP-Rollen und -Benutzern [Seite 95]
Konfigurieren der SNC-Einstellungen in der Central Management Console [Seite 98]

5.5.2 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.

5.5.2.1 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.

   > ⓘ 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).

5.5.2.2 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.

5.5.3 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

5.5.3.1 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*.

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 [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.

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 Verbindung	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 Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mit einer Namenslizenz erstellt wurden, ist auf 10 Sitzungen beschränkt. Wenn ein Namenslizenzbenutzer versucht, eine 11. gleichzeitige Anmeldesitzung herzustellen, zeigt das

Einstellung	Beschreibung
	System eine entsprechende Fehlermeldung an. Um eine weitere Anmeldesitzung öffnen zu können, muss eine der bestehenden Sitzungen geschlossen werden. Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mittels einer Prozessorlizenz oder einer Lizenz für Öffentliche Dokumente erstellt wurde, unterliegt jedoch keiner Einschränkung. **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. 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.

Einstellung	Beschreibung
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*.

5.5.3.2 Ändern des Stamms im Inhaltsordner

1. Wechseln Sie zum Verwaltungsbereich *Authentifizierung* der CMC.
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/`).

5.5.4 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~Clientnummer@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.

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.

5.5.4.1 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*.

5.5.4.2 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.
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.

5.5.4.3 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.

5.5.4.3.1 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*.

   > → 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.

Wiederholungsmuster	Beschreibung
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.

> → Tipp
>
> Um die nächste zeitgesteuert verarbeitete Aktualisierung abzubrechen, klicken Sie im Bereich *Nur Rollen aktualisieren* oder *Rollen und Aliase aktualisieren* auf *Geplante Aktualisierungen abbrechen*.

5.5.5 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 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 93]

5.5.5.1 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 Webanwendungsserver 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.

   Das SNC-Namensformat hängt von der SNC-Bibliothek ab. Bei Verwendung der SAP-Kryptografiebibliothek wird der definierte Name entsprechend den 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.
9. Klicken Sie auf *Speichern*.

Weitere Informationen

Verbinden mit SAP-Berechtigungssystemen [Seite 87]

5.6 Oracle-EBS-Authentifizierung

5.6.1 Oracle-EBS-Authentifizierung

Die Oracle-EBS-Authentifizierung ermöglicht es Benutzern, sich mit ihren EBS-Benutzernamen und -Kennwörtern bei der BI-Plattform anzumelden, ohne dass die Kennwörter im System gespeichert werden müssen.

Mit der Oracle-EBS-Authentifizierungsanwendung wird die Art und Weise konfiguriert, wie sich Benutzer in der BI-Plattform authentifizieren und Rollen aus dem EBS-System importieren.

Die Anwendung ist in vier Registerkarten unterteilt, die in der folgenden Tabelle beschrieben werden.

Registerkarte	Beschreibung
Optionen	Einstellung für die Aktivierung der Oracle EBS-Authentifizierung und Optionen, die den Umgang mit neuen Aliasen, Aliasaktualisierungen und neuen Benutzern definieren.
Systeme	Einstellungen für Oracle-EBS-Systembenutzer und -Dienste, auf die über die BI-Plattform zugegriffen werden soll.
Zuständigkeiten	Einstellungen für den Import von Rollen in die BI-Plattform.
Benutzeraktualisierung	Einstellungen für die zeitgesteuerte Verarbeitung und die Ausführung von Aktualisierungen für importierte Oracle EBS-Rollen.

Weitere Informationen

Aktivieren der Oracle E-Business Suite-Authentifizierung [Seite 100]
Oracle-E-Business-Suite-Rollen zuordnen [Seite 101]
Zeitgesteuertes Verarbeiten für Oracle EBS-Rollen [Seite 104]

5.6.2 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.

5.6.2.1 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*.
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

Oracle-E-Business-Suite-Rollen zuordnen [Seite 101]

5.6.3 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.

5.6.3.1 Oracle-E-Business-Suite-Rollen zuordnen

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.

     > **Hinweis**
     >
     > Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mit einer Namenslizenz erstellt wurden, ist auf 10 Sitzungen beschränkt. Wenn ein Namenslizenzbenutzer versucht, eine 11. gleichzeitige Anmeldesitzung herzustellen, zeigt das System eine entsprechende Fehlermeldung an. Um eine weitere Anmeldesitzung öffnen zu können, muss eine der bestehenden Sitzungen geschlossen werden.
     >
     > Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mittels einer Prozessorlizenz oder einer Lizenz für Öffentliche Dokumente erstellt wurde, unterliegt jedoch keiner Einschränkung.

   - *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*.
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.

5.6.3.2 Hinzufügen von Benutzern zu zugewiesenen Rollen

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.

5.6.3.3 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.

5.6.3.3.1 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.

5.6.4 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.

5.6.4.1 Zeitgesteuertes Verarbeiten für Oracle EBS-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 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.
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.

5.7 JD-Edwards-Enterprise-One-Authentifizierung

5.7.1 JD Edwards EnterpriseOne-Authentifizierung

Mit der Authentifizierung von JD Edwards EnterpriseOne können Benutzer sich mit ihren JD-Edwards-Benutzernamen und -Kennwörtern bei derBI-Plattform anmelden, ohne dass die Kennwörter in der BI-Plattform gespeichert werden müssen.

Mit der JD-Edwards-Authentifizierungsanwendung erfolgt sowohl die Konfiguration der Art und Weise, wie sich Benutzer in der BI-Plattform authentifizieren, als auch der Import von Rollen aus dem JD-Edwards-System.

Die Anwendung ist in vier Registerkarten unterteilt, die in der folgenden Tabelle beschrieben werden.

Registerkarte	Beschreibung
Optionen	Einstellung für die Aktivierung der JD Edwards EnterpriseOne-Authentifizierung und Optionen, die den Umgang mit neuen Aliasen, Aliasaktualisierungen und neuen Benutzern definieren.
Systeme	Einstellungen für Systembenutzer und Dienste von JD Edwards EnterpriseOne, auf die über die BI-Plattform zugegriffen werden soll.
Zuständigkeiten	Einstellungen für den Import von Rollen in die BI-Plattform.
Benutzeraktualisierung	Einstellungen für die zeitgesteuerte Verarbeitung und die Ausführung von Aktualisierungen für importierte JD Edwards EnterpriseOne-Rollen.

Weitere Informationen

Aktivieren der JD Edwards EnterpriseOne-Authentifizierung [Seite 106]
Zuordnen von JD-Edwards-EnterpriseOne-Rollen zur BI-Plattform [Seite 107]
Zeitgesteuertes Verarbeiten von Benutzeraktualisierungen [Seite 110]

5.7.2 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.

5.7.2.1 JD Edwards-Authentifizierung in der BI-Plattform aktivieren

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.
11. Geben Sie einen Namen für die Umgebung ein, und klicken Sie auf *Hinzufügen*.
12. Klicken Sie auf *Aktualisieren*, um die Änderungen zu speichern.

5.7.3 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.

5.7.3.1 JD Edwards EnterpriseOne-Rolle zuordnen

1. Melden Sie sich als Administrator bei der Central Management Console an.
2. Klicken Sie im Bereich *Verwaltung* 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*
     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.
   - *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.

     > **Hinweis**
     >
     > Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mit einer Namenslizenz erstellt wurden, ist auf 10 Sitzungen beschränkt. Wenn ein Namenslizenzbenutzer

> versucht, eine 11. gleichzeitige Anmeldesitzung herzustellen, zeigt das System eine entsprechende Fehlermeldung an. Um eine weitere Anmeldesitzung öffnen zu können, muss eine der bestehenden Sitzungen geschlossen werden.
>
> Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mittels einer Prozessorlizenz oder einer Lizenz für Öffentliche Dokumente erstellt wurde, unterliegt jedoch keiner Einschränkung.

- *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.

5.7.3.2 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.

5.7.3.3 Aufheben der Zuordnung von Rollen

Um zu verhindern, dass sich Benutzer an der BI-Plattform anmelden, können Sie die Zuordnung der Rollen, denen sie angehören, aufheben.

5.7.3.3.1 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.

5.7.3.4 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.

5.7.3.4.1 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.
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.

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.

5.8 PeopleSoft-Enterprise-Authentifizierung

5.8.1 PeopleSoft Enterprise-Authentifizierung

Die PeopleSoft-Enterprise-Authentifizierung ermöglicht es Benutzern, sich mit ihrem PeopleSoft-Benutzernamen und -Kennwort bei der BI-Plattform anzumelden, ohne dass die Kennwörter in der BI-Plattform gespeichert werden müssen.

Mit der PeopleSoft-Enterprise-Authentifizierungsanwendung erfolgt sowohl die Konfiguration der Art und Weise, wie sich Benutzer in der BI-Plattform authentifizieren, als auch der Import von Rollen aus dem PeopleSoft-System.

Die Anwendung ist in vier Registerkarten unterteilt, die in der folgenden Tabelle beschrieben werden.

Registerkarte	Beschreibung
Optionen	Einstellung für die Aktivierung der PeopleSoft Enterprise-Authentifizierung und Optionen, die den Umgang mit neuen Aliasen, Aliasaktualisierungen und neuen Benutzern definieren.
Systeme	Einstellungen für PeopleSoft-Enterprise-Systembenutzer und -Dienste, auf die über die BI-Plattform zugegriffen werden soll.
Zuständigkeiten	Einstellungen für den Import von Rollen in die BI-Plattform.
Benutzeraktualisierung	Einstellungen für die zeitgesteuerte Verarbeitung und die Ausführung von Aktualisierungen für importierte PeopleSoft Enterprise-Rollen.

Weitere Informationen

Aktivieren der PeopleSoft Enterprise-Authentifizierung [Seite 113]
Zuordnen von PeopleSoft-Rollen zur BI-Plattform [Seite 114]
Zeitgesteuertes Verarbeiten von Benutzeraktualisierungen [Seite 110]

5.8.2 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.

5.8.2.1 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.

   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.

5.8.3 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.

5.8.3.1 PeopleSoft-Rollen zu BI-Plattform zuordnen

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.
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.

> **Hinweis**
>
> Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mit einer Namenslizenz erstellt wurden, ist auf 10 Sitzungen beschränkt. Wenn ein Namenslizenzbenutzer versucht, eine 11. gleichzeitige Anmeldesitzung herzustellen, zeigt das System eine entsprechende Fehlermeldung an. Um eine weitere Anmeldesitzung öffnen zu können, muss eine der bestehenden Sitzungen geschlossen werden.
>
> Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mittels einer Prozessorlizenz oder einer Lizenz für Öffentliche Dokumente erstellt wurde, unterliegt jedoch keiner Einschränkung.

- *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.

5.8.3.2 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.

5.8.3.3 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.

5.8.3.4 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.

5.8.3.4.1 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.
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.

5.9 Siebel-Authentifizierung

5.9.1 Siebel-Authentifizierung

Mit der Siebel-Authentifizierung können Benutzer sich mit ihren Siebel-Benutzernamen und -Kennwörtern bei der BI-Plattform anmelden, ohne dass das Kennwort in der BI-Plattform gespeichert werden muss.

Mit der Siebel-Authentifizierungsanwendung erfolgt sowohl die Konfiguration der Art und Weise, wie sich Benutzer bei der BI-Plattform authentifizieren, als auch der Import von Rollen aus dem Siebel-System.

Die Anwendung ist in vier Registerkarten unterteilt, die in der folgenden Tabelle beschrieben werden.

Registerkarte	Beschreibung
Optionen	Einstellung für die Aktivierung der Siebel-Authentifizierung und Optionen, die den Umgang mit neuen Aliasen, Aliasaktualisierungen und neuen Benutzern definieren.
Systeme	Einstellungen für Siebel-Systembenutzer und -Dienste, auf die über die BI-Plattform zugegriffen werden soll.
Zuständigkeiten	Einstellungen für den Import von Rollen in die BI-Plattform.
Benutzeraktualisierung	Einstellungen für die zeitgesteuerte Verarbeitung und die Ausführung von Aktualisierungen für importierte Siebel-Rollen.

Weitere Informationen

Aktivieren der Siebel-Authentifizierung [Seite 119]
Zuordnen von Rollen zur BI-Plattform [Seite 120]
Zeitgesteuertes Verarbeiten von Benutzeraktualisierungen [Seite 110]

5.9.2 Aktivieren der Siebel-Authentifizierung

Damit Siebel-Informationen von der BI-Plattform verwendet werden können, benötigt diese Informationen zur Authentifizierung im Siebel-System.

5.9.2.1 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*.
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.

5.9.3 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.

5.9.3.1 Siebel-eBusiness-Rolle zu BI-Plattform zuordnen

1. Melden Sie sich als Administrator bei der Central Management Console an.
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 gegebenenfalls 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 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.

     > **Hinweis**
     >
     > Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mit einer Namenslizenz erstellt wurden, ist auf 10 Sitzungen beschränkt. Wenn ein Namenslizenzbenutzer versucht, eine 11. gleichzeitige Anmeldesitzung herzustellen, zeigt das System eine entsprechende Fehlermeldung an. Um eine weitere Anmeldesitzung öffnen zu können, muss eine der bestehenden Sitzungen geschlossen werden.
     >
     > Die Anzahl der gleichzeitigen Anmeldesitzungen für Namenslizenzbenutzer, die mittels einer Prozessorlizenz oder einer Lizenz für Öffentliche Dokumente erstellt wurde, unterliegt jedoch keiner Einschränkung.

- *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.

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 >.

> **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.

5.9.3.2 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.

5.9.3.3 Aufheben der Zuordnung von Rollen

Um zu verhindern, dass sich Benutzer an der BI-Plattform anmelden, können Sie die Zuordnung der Rollen, denen sie angehören, aufheben.

5.9.3.3.1 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.
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.

5.9.3.4 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.

5.9.3.4.1 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.

Wiederholungsmuster	Beschreibung
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.

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.

5.10 X.509-Authentifizierung

5.10.1 X.509-Authentifizierung für BI-Launchpad

5.10.1.1 Erstellen und Konfigurieren von Zertifikaten und Keystores

> **Hinweis**
>
> In der BI-Plattform sollte ein Benutzer vorhanden sein, um den Single Sign-On über X.509-Authentifizierung zu ermöglichen.

> **Hinweis**
>
> Laden Sie das OpenSSL-Toolkit herunter, und installieren Sie es, um die unten stehenden Schritte durchzuführen.

> **Hinweis**
>
> Führen Sie die unten genannten Schritte durch, wenn Sie ein CA-Zertifikat erstellen und selbst signieren möchten.

> **Hinweis**
>
> Wenn Sie über ein vertrauenswürdiges CA-Zertifikat verfügen, erhalten Sie unter Mit vertrauenswürdigem CA-Zertifikat [Seite 127] weitere Informationen zum Erstellen und Konfigurieren von Zertifikaten und Keystores.

1. Führen Sie den folgenden Befehl aus, um einen Schlüssel als Zertifizierungsstelle (ca.key) und eine Zertifizierungsanforderungs-Datei (ca.csr) zu erstellen. `Openssl.exe req -newkey rsa:2048 -nodes -out c:\ssl\ca.csr -keyout c:\ssl\ca.key`
2. Führen Sie den folgenden Befehl aus, um das signierte Zertifikat "ca.pem" zu erstellen: `Openssl.exe x509 -req -trustout -signkey c:\ssl\ca.key -days 365 -in c:\ssl\ca.csr -out c:\ssl\ca.pem`
3. Erstellen Sie das Serverschlüsselpaar, das Zertifikat und den Keystore.
   a. Erstellen Sie eine Datei, in der die Seriennummern des CA-Zertifikats hinterlegt sind, indem Sie folgenden Befehl ausführen: `Echo 02 >c:\ssl\ca.srl`
   b. Navigieren Sie zu `C:\Program Files\Java\jre7\bin`, und erstellen Sie mit der keytool.exe den Server-Keystore, das Zertifikat und den privaten Schlüssel.

      > **Hinweis**
      >
      > Abhängig von der Java-Version kann "jre7" für den Speicherort der Java-keytool.exe abweichen.

      ```
      Keytool.exe -genkey -alias server -keyalg RSA -keysize 2048 -keystore
      c:\ssl\serverkeystore.jks -storetype JKS
      Keytool.exe -certreq -keyalg RSA -alias server -file c:\ssl\server.csr -
      keystore c:\ssl\serverkeystore.jks
      ```

      > **→ Nicht vergessen**
      >
      > Geben Sie beim Erstellen des Zertifikats den Hostnamen des Serversystems ein, wenn Sie dazu aufgefordert werden. Anderenfalls erhalten Sie beim Herstellen der Verbindung einen Zertifikatfehler auf dem Client.

   c. Geben Sie das Keystore-Kennwort an.

      > **→ Nicht vergessen**
      >
      > Sie müssen die Zertifikatsanforderungs-Datei "server.csr" in einem Texteditor bearbeiten und die Einträge "New Begin Certificate Request" bis "Begin Certificate Request" und "New End Certificate Request" bis "End Certificate Request" anpassen.
4. Führen Sie den folgenden Befehl aus, um das signierte Zertifikat "server.crt" zu erstellen: `Openssl.exe x509 -CA c:\ssl\ca.pem -cakey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\server.csr -out c:\ssl\server.crt -days 365`
5. Importieren Sie das CA- und Serverzertifikat in den Server-Keystore.

   ```
   Keytool.exe -import -alias ca -keystore c:\ssl\serverkeystore.jks -
   trustcacerts -file c:\ssl\ca.pem
   ```

```
Keytool.exe –import –alias server –keystore c:\ssl\serverkeystore.jks –
trustcacerts –file c:\ssl\server.crt
```

6. Führen Sie den folgenden Befehl aus, um die Clientzertifikate "client.req" und "client.key" zu erstellen: `Openssl.exe –newkey rsa:2048 –nodes –out c:\ssl\client.req –keyout c:\ssl\client.key –config c:\ssl\sslc.cnf`

> **Hinweis**
>
> Kopieren Sie die Datei "sslc.cnf" aus `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` nach C:\SSL, und passen Sie die Parameter an.
>
> Dir=c:/ssl # Speicherort für alle Dateien
>
> Certificate= $dir/ca.pem # CA-Zertifikat
>
> Private_key= $dir/ca.key # privater Schlüssel
>
> RANDFILE= $dir/.rand # private Datei mit zufällig gewählten Zahlen

7. Führen Sie den folgenden Befehl aus, um das Clientzertifikat zu signieren: `Openssl.exe x509 –CA c:\ssl\ca.pem –CAkey c:\ssl\ca.key –CAserial c:\ssl\ca.srl –req –in c:\ssl\client.req –out c:\ssl\client.pem –days 365`
8. Importieren Sie das CA- und Clientzertifikat mit dem unten aufgeführten Befehl in den vertrauenswürdigen Keystore. Mit diesem Befehl wird die Datei "trustkeystore.jks" erstellt.

```
Keytool.exe –import –alias ca –keystore c:\ssl\trustkeystore.jks –
trustcacerts –file c:\ssl\ca.pem
Keytool.exe –import –alias client –keystore c:\ssl\trustkeystore.jks –
trustcacerts –file c:\ssl\client.pem
```

9. Exportieren Sie das Clientzertifikat mit dem clientseitigen privaten Schlüssel im PKCS12-Format: `Openssl.exe pkcs12 –export –clcerts –in c:\ssl\client.pem –inkey c:\ssl\client.key –out c:\ssl\client.p12 –name “client certificate”`. Mit diesem Befehl wird die Datei "client.p12" erstellt.
10. Führen Sie den folgenden Befehl aus, um das CA-Zertifikat zu exportieren und die Datei "ca.crt" zu erstellen: `Openssl.exe x509 –in c:\ssl\ca.pem –inform PEM –out c:\ssl\ca.crt –outform DER`
11. Kopieren Sie die Dateien ".p12" und "ca.crt" auf den Clientrechner, um das Client- und CA-Zertifikat zu installieren.

> **Hinweis**
>
> Um Zertifikate in Mozilla Firefox zu installieren, navigieren Sie zu *Extras* > *Einstellungen* > *Erweitert*. Wählen Sie "Zertifikate anzeigen" auf der Registerkarte "Sicherheit", und importieren Sie die Datei "client.p12" auf der Registerkarte "Ihre Zertifikate" und die Datei "ca.crt" auf der Registerkarte "Zertifizierungsstellen".

5.10.1.1.1 Mit vertrauenswürdigem CA-Zertifikat

1. Erstellen Sie das Serverschlüsselpaar, das Zertifikat und den Keystore.
   a. Erstellen Sie eine Datei, in der die Seriennummern des CA-Zertifikats hinterlegt sind, indem Sie folgenden Befehl ausführen: `Echo 02 >c:\ssl\ca.srl`
   b. Navigieren Sie zu `C:\Programme\Java\jre7\bin`, und erstellen Sie mit der keytool.exe den Server-Keystore, das Zertifikat und den privaten Schlüssel.

      > **Hinweis**
      >
      > Abhängig von der Java-Version kann "jre7" für den Speicherort der keytool.exe abweichen.

      ```
      Keytool.exe –genkey –alias server –keyalg RSA –keysize 2048 –keystore
      c:\ssl\serverkeystore.jks –storetype JKS
      Keytool.exe –certreq –keyalg RSA –alias server –file c:\ssl\server.csr –
      keystore c:\ssl\serverkeystore.jks
      ```

      > **→ Nicht vergessen**
      >
      > Geben Sie beim Erstellen des Zertifikats den Hostnamen des Serversystems ein, wenn Sie dazu aufgefordert werden. Anderenfalls erhalten Sie beim Herstellen der Verbindung einen Zertifikatfehler auf dem Client.

   c. Geben Sie das Keystore-Kennwort an.

      > **→ Nicht vergessen**
      >
      > Sie müssen die Zertifikatsanforderungs-Datei "server.csr" in einem Texteditor bearbeiten und die Einträge "New Begin Certificate Request" bis "Begin Certificate Request" und "New End Certificate Request" bis "End Certificate Request" anpassen.

2. Führen Sie den folgenden Befehl aus, um das signierte Zertifikat "server.crt" zu erstellen: `Openssl.exe x509 –CA c:\ssl\ca.pem –cakey c:\ssl\ca.key –CAserial c:\ssl\ca.srl –req –in c:\ssl\server.csr –out c:\ssl\server.crt –days 365`
3. Importieren Sie das Serverzertifikat in den Server-Keystore.

   ```
   Keytool.exe –import –alias server –keystore c:\ssl\serverkeystore.jks –
   trustcacerts –file c:\ssl\server.crt
   ```

4. Führen Sie den folgenden Befehl aus, um die Clientzertifikate "client.req" und "client.key" zu erstellen: `Openssl.exe –newkey rsa:2048 –nodes –out c:\ssl\client.req –keyout c:\ssl\client.key –config c:\ssl\sslc.cnf`

   > **Hinweis**
   >
   > Kopieren Sie die Datei "sslc.cnf" aus `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` nach C:\SSL, und passen Sie die Parameter an:
   >
   > Dir=c:/ssl # Speicherort für alle Dateien
   >
   > Certificate= $dir/ca.pem # CA-Zertifikat
   >
   > Private_key= $dir/ca.key # privater Schlüssel
   >
   > RANDFILE= $dir/.rand # private Datei mit zufällig gewählten Zahlen

5. Führen Sie den folgenden Befehl aus, um das Clientzertifikat zu signieren: `Openssl.exe x509 –CA c:\ssl\ca.pem –CAkey c:\ssl\ca.key –CAserial c:\ssl\ca.srl –req –in c:\ssl\client.req –out c:\ssl\client.pem –days 365`
6. Importieren Sie das Clientzertifikat mit dem unten aufgeführten Befehl in den vertrauenswürdigen Keystore. Mit diesem Befehl wird die Datei "trustkeystore.jks" erstellt.

```
Keytool.exe –import –alias client –keystore c:\ssl\trustkeystore.jks –
trustcacerts –file c:\ssl\client.pem
```

7. Exportieren Sie das Clientzertifikat mit dem clientseitigen privaten Schlüssel im PKCS12-Format: `Openssl.exe pkcs12 –export –clcerts –in c:\ssl\client.pem –inkey c:\ssl\client.key –out c:\ssl\client.p12 –name “client certificate”`. Mit diesem Befehl wird die Datei "client.p12" erstellt.
8. Kopieren Sie die .p12-Datei auf den Clientrechner, um sie zu installieren.

> **Hinweis**
>
> Um Zertifikate in Mozilla Firefox zu installieren, navigieren Sie zu *Extras* > *Einstellungen* > *Erweitert*. Wählen Sie "Zertifikate anzeigen" auf der Registerkarte "Sicherheit", und importieren Sie die Datei "client.p12" auf der Registerkarte "Ihre Zertifikate" und die Datei "ca.crt" auf der Registerkarte "Zertifizierungsstellen".

5.10.1.2 Konfigurieren des Tomcat-SSL-Servers

5.10.1.2.1 Einseitige SSL-Konfiguration

1. Navigieren Sie zu `<INSTALLVERZ>\tomcat\conf\server.xml`
2. Bearbeiten Sie das folgende XML-Tag: `<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="200" SSLEnabled="true" scheme="https" secure="true">`
```
<SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
Connector>
```

> **Hinweis**
>
> Das Kennwort (Password1) und der Speicherort (C:\ssl\serverkeystore.jks) der Keystore-Datei im oben erwähnten XML-Tag dienen nur als Beispiele. Sie können ein beliebiges Kennwort und einen beliebigen Speicherort verwenden.

3. Speichern Sie die Datei und starten Sie den Tomcat-Server neu.

5.10.1.2.2 Beidseitige SSL-Konfiguration

Konfigurieren Sie den Tomcat-Server zur Anforderung der Client-Authentifizierung, indem Sie die u.g. Schritte ausführen.

1. Navigieren Sie zu `<INSTALLVERZ>\tomcat\conf\server.xml`
2. Bearbeiten Sie die "server.xml" und fügen Sie den folgenden XML-Tag hinzu:
```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="200" SSLEnabled="true" scheme="https" secure="true">
<SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
Connector>
```

> **Hinweis**
>
> Das Kennwort (Password1) und der Speicherort (C:\ssl\serverkeystore.jks bzw. C:\ssl\trustkeystore.jks) der Server-Keystore- bzw. Trust-Keystore-Datei im oben erwähnten XML-Tag dienen nur als Beispiele. Sie können ein beliebiges Kennwort und einen beliebigen Speicherort verwenden.

3. Speichern Sie die Datei und starten Sie den Tomcat-Server neu.

> **Hinweis**
>
> Deaktivieren Sie im Internet Explorer die Option "Keine Aufforderung zur Clientzertifikatauswahl, wenn kein oder nur ein Zertifikat vorhanden ist" unter *Internetoptionen* > *Sicherheit* > *Lokales Intranet* > *Stufe anpassen* > *Verschiedenes*.

5.10.1.3 Konfigurieren des BI-Launchpads

5.10.1.3.1 Erstellen eines gemeinsamen geheimen Schlüssels

Der gemeinsame geheime Schlüssel dient der Herstellung einer vertrauenswürdigen Verbindung zwischen dem Client und dem CMS. Sie müssen den Server zur Verwendung der vertrauenswürdigen Authentifizierung vor dem Client konfigurieren.

1. Melden Sie sich bei der CMC an.
2. Navigieren Sie zu "Authentifizierung", und wählen Sie "Enterprise".
3. Aktivieren Sie die vertrauenswürdige Authentifizierung.
4. Wählen Sie "Neuer gemeinsamer geheimer Schlüssel".

> **Hinweis**
>
> Die Meldung "Der gemeinsame geheime Schlüssel wurde generiert und steht zum Herunterladen bereit" wird angezeigt.

5. Wählen Sie "Gemeinsamen geheimen Schlüssel herunterladen".
6. Wählen Sie "Speichern" im Dialogfeld "Herunterladen", und wählen Sie eines der folgenden Verzeichnisse:
   - `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`

- `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`

5.10.1.3.2 Übergabe des gemeinsamen geheimen Schlüssel mit der Datei "TrustedPrincipal.conf"

1. Erstellen Sie unter `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEBINF\config\custom\directory` eine neue Textdatei.
2. Fügen Sie den unten stehenden Text in die neue Datei ein.

```
sso.enabled=true
        trusted.auth.user.retrieval=WEB_SESSION
        trusted.auth.user.param=MyUser
        trusted.auth.shared.secret=MySecret
```

3. Speichern Sie die Datei unter dem Namen "global.properties".

5.10.1.3.3 Bearbeiten der Datei "custom.jsp"

> **Hinweis**
>
> Bevor Sie die Datei "custom.jsp" bearbeiten, erstellen Sie in der CMC einen Benutzer mit dem Namen des Rechners.

1. Fahren Sie fort mit ...
   a. *<INSTALLVERZ>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *custom.jsp* in *com.businessobjects.webpath.InfoView.jar* für das klassische BI-Launchpad.
   b. *<INSTALLVERZ>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.fioriBI* > *web* > *custom.jsp* in *com.businessobjects.webpath.fioriBI.jar* für das "fiorisierte" BI-Launchpad.
2. Bearbeiten Sie die Datei "custom.jsp".

```
<\!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("MySecret","<Shared_Secret_Key>")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<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>
```

> **Hinweis**
>
> Ersetzen Sie den <Gemeinsamen_geheimen_Schlüssel> durch den neuen Schlüssel, der in der Datei *TrustedPrincipal.conf* verfügbar ist. Wie Sie einen gemeinsamen geheimen Schlüssel anlegen, erfahren Sie unter Erstellen eines gemeinsamen geheimen Schlüssels [Seite 130].

5.10.1.3.4 Erstellen der Datei "myScript.js"

1. Navigieren Sie zu *<INSTALLVERZ>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *noCacheCustomResources* und erstellen Sie die Datei "myScript.js".
2. Fügen Sie Folgendes zu "myScript.js" hinzu:

```
function goToLogonPage()
{
window.location = "logon.jsp";
}
```

3. Starten Sie den Tomcat-Server neu.

5.10.1.3.5 Einrichten von BOE Internal und Konfigurieren der benutzerdefinierten Property-Datei

1. Navigieren Sie zu *<INSTALLVERZ>* > *Tomcat* > *webapps* > *BOE* > *WEB-INF* > *internal*.
2. Öffnen Sie die Datei "bilaunchpad.properties", und passen Sie die folgenden Eigenschaften an:

```
redirection.iframe.1.incoming.url=property.ref.app.url.name
redirection.iframe.1.application=InfoView
redirection.iframe.1.bundle.path=/InfoView
redirection.iframe.1.redirectto.url=/custom.jsp
redirection.iframe.2.incoming.url=property.ref.app.url.name
redirection.iframe.2.incoming.url.suffix=/index.html
redirection.iframe.2.application=InfoView
redirection.iframe.2.bundle.path=/InfoView
redirection.iframe.2.redirectto.url=/custom.jsp
redirection.iframe.9.incoming.url=/InfoView/index.html
redirection.iframe.9.application=InfoView
redirection.iframe.9.bundle.path=/InfoView
redirection.iframe.9.redirectto.url=/custom.jsp
```

3. Starten Sie den Tomcat-Server neu.

5.10.1.3.6 Konfigurieren der BOE-Datei "web.xml"

1. Navigieren Sie zu `<INSTALLVERZ>\tomcat\webapps\BOE\WEB-INF`.
2. Bearbeiten Sie die Datei "web.xml" an diesem Speicherort mit dem folgenden Befehl:

```
<init-param>
<param-name>extendedFrameworkExports</param-name>
<param-
value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbr
idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
bel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-
value>
</init-param>
```

3. Fügen Sie der Datei "web.xml" die gewünschten Parameter hinzu, indem Sie die folgenden Schritte ausführen:
   a. `<INSTALLVERZ>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.BIPCoreWeb\web\WEB-INF`
   b. Fügen Sie die folgenden Parameter hinzu:

```
<init-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>New_Shared_Secret_Key</param-value>
</init-param>
```

   c. Wiederholen Sie die Schritte, indem Sie zu `<INSTALLVERZ>\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.BIPCoreWeb\web\WEB-INF` navigieren.

> → Tipp
>
> Um zu überprüfen, ob Sie die vertrauenswürdige Authentifizierung korrekt konfiguriert haben, greifen Sie über folgende URL auf die BI-Launchpad-Anwendung zu: https://[CMS-Name]:8443/BOE/BI/logon.jsp, wobei [CMS-Name] der Name des Rechners ist, auf dem der CMS gehostet wird.

5.10.2 X.509-Authentifizierung für Webdienste

5.10.2.1 Für SOAP-Webdienste

5.10.2.1.1 Konfigurieren von SSL in Tomcat

Wenn Sie Webdienste verwenden, müssen Sie in Tomcat SSL konfigurieren, bevor Sie SAP Business Intelligence konfigurieren.

> ⓘ Hinweis
>
> In der BI-Plattform sollte ein Benutzer vorhanden sein, um den Single Sign-On über X.509-Authentifizierung zu ermöglichen.

1. Navigieren Sie zu `<INSTALLVERZ>\tomcat\conf`.
2. Öffnen Sie die Datei "server.xml" in einem XML-Editor, und bearbeiten Sie das XML-Tag:

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="200" SSLEnabled="true" scheme="https" secure="true">
<SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
Connector>
```

3. Speichern Sie die Datei.

> **Hinweis**
>
> Das Kennwort und der Speicherort in den oben erwähnten Dateien dienen nur als Beispiele. Sie können ein beliebiges Kennwort und einen beliebigen Speicherort hinzufügen.

> **Hinweis**
>
> Weitere Informationen zum Erstellen und Konfigurieren von Keystore-Dateien finden Sie unter Erstellen und Konfigurieren von Zertifikaten und Keystores [Seite 125].

5.10.2.1.2 Konfigurieren der Datei "axis2.xml"

> **Hinweis**
>
> Stellen Sie unter Linux bzw. Unix sicher, dass der Betriebssystembenutzer, der BI auf dem System installiert, über die rekursiven Rechte 755 für das Verzeichnis `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje` verfügt, bevor Sie mit den folgenden Schritten fortfahren. Die Rechte können mit dem Befehl `chmod -R 755` vergeben werden.

1. Navigieren Sie zu `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`.
2. Öffnen Sie die Datei "axis2.xml" in einem XML-Editor.
3. Aktualisieren Sie den XML-Tag mit der neuen Portnummer, um die gesicherte Verbindung zu aktivieren.

```
<transportReceiver name="http"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8080</parameter>
</transportReceiver>
<transportReceiver name="https"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8443</parameter>
</transportReceiver>
```

> **Hinweis**
>
> Die Standardkonfiguration für AxisServlet sieht nur den Erhalt von Anforderungen über HTTP vor. Um HTTPS zu aktivieren, müssen Sie den AxisServletListener mit der Option name = "https" konfigurieren und die entsprechenden Port-Parameter für beide Empfänger definieren. Sie können außerdem mehrere Portnummern hinzufügen bzw. entfernen, indem Sie die XML-Tags aktualisieren.

4. Speichern Sie die "axis2.xml".
5. Starten Sie den Tomcat-Server neu.
6. Starten Sie einen beliebigen Browser, und rufen Sie https://<IP-Adresse>:<HTTPS-Port>/dswsbobje/services/listServices auf, um die gesicherte Verbindung zu überprüfen. Nachdem Sie den Link aufgerufen haben, wird auf der Registerkarte der Sitzung "trustedLoginWithX509" angezeigt.

5.10.2.1.3 Erstellen eines gemeinsamen geheimen Werts

1. Starten Sie die Central Management Console.
2. Navigieren Sie zu *Authentifizierung* > *Enterprise*.
3. Markieren Sie unter *Vertrauenswürdige Authentifizierung* das Kontrollkästchen *Vertrauenswürdige Authentifizierung ist aktiviert*.
4. Wählen Sie *Neuer gemeinsamer geheimer Schlüssel*. Mit diesem Vorgang wird der gemeinsame geheime Schlüssel erstellt.
5. Wählen Sie *Gemeinsamen geheimen Schlüssel herunterladen* und dann *Aktualisieren*.
6. Kopieren Sie die heruntergeladene Datei "TrustedPrincipal.conf" nach `<INSTALLVERZ>SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin` in Windows.

   > **Hinweis**
   >
   > Sie können den gemeinsamen geheimen Wert anzeigen, indem Sie die Datei "TrustedPrincipal.conf" in einem beliebigen XML-Editor öffnen.

5.10.2.1.4 Konfigurieren der Datei "web.xml"

1. Navigieren Sie zu `<INSTALLVERZ>\tomcat\webapps\dswsbobje\WEB-INF`.
2. Öffnen Sie die Datei "web.xml" in einem XML-Editor, und aktualisieren Sie das XML-Tag mit dem Namen des Rechners, der den CMS hostet:

   ```
   <context-param>
           <param-name>cms.default</param-name>
           <param-value>EnterHostMachineName</param-value>
       </context-param>
   ```

3. Fügen Sie dem unten aufgeführten XML-Tag den gemeinsamen geheimen Wert hinzu. Weitere Informationen zur Erstellung eines gemeinsamen geheimen Werts erhalten Sie unter Erstellen eines gemeinsamen geheimen Werts [Seite 135].

   ```
   <context-param>
   <param-name>trusted.auth.shared.secret</param-name>
   <param-value>shared secret value</param-value>
   </context-param>
   ```

4. Speichern Sie die Datei "web.xml".

> **Hinweis**
>
> Die Konfigurationseinstellungen in der Datei "axis2.xml" gehen bei einem Upgrade von einer früheren Version als BI 4.2 SP04 verloren.

5.10.2.2 Für RESTful Web-Services

> **Hinweis**
>
> In der BI-Plattform sollte ein Benutzer vorhanden sein, um die Einzelanmeldung über X.509-Authentifizierung zu ermöglichen.

Informationen dazu, wie Sie vertrauenswürdige Authentifizierungen für RESTful Web-Services erstellen, finden Sie im *Administratorhandbuch für SAP BusinessObjects Business Intelligence* im Abschnitt "HTTPS/SSL konfigurieren".

Um eine vertrauenswürdige Authentifizierung mit X.509-Zertifikaten einzurichten, müssen Sie einen gemeinsamen geheimen Schlüssel erstellen. Weitere Informationen finden Sie im Kapitel "Erstellen eines gemeinsamen geheimen Werts" im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.

Weitere Informationen zum REST-SDK-Endpunkt finden Sie im *Business Intelligence Platform RESTful Web Service Developer Guide* unter *API Reference* > *Authentication* > */v1//logon/trustedx509*.

5.10.3 X.509-Authentifizierung für die CMC

5.10.3.1 Bearbeiten der Datei "custom.jsp" (für die CMC)

> **Hinweis**
>
> Bevor Sie die Datei "custom.jsp" bearbeiten, erstellen Sie in der CMC einen Benutzer mit dem Namen des Rechners. Wenn auf dem Rechner ein Benutzer vorhanden ist, können Sie direkt mit den im Folgenden beschriebenen Schritten beginnen.

1. Navigieren Sie zu `<INSTALLVERZ>\tomcat\webapps\BOE\WEBINF\eclipse\plugins\webpath.CmcApp\web\cutom.jsp` in der Datei "com.businessobjects.webpath.InfoView.jar".
2. Bearbeiten Sie die Datei "custom.jsp".

```
<\!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("MySecret","Shared
Secret Key")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<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>
```

> **Hinweis**
>
> Sie sollten den gemeinsamen geheimen Wert in diesem Code durch den neuen Schlüssel und den Benutzer mit dem Namen des Rechners, der in der CMC erstellt wurde, ersetzen.

5.10.3.2 Erstellen der Datei "myScript.js" (für die CMC)

1. Navigieren Sie zu `<INSTALLVERZ>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.CmcApp\web\noCacheCustomResources and create myScript.js`.
2. Fügen Sie Folgendes zu "myScript.js" hinzu:

```
function goToLogonPage()
{
window.location = "logon.jsp";
}
```

3. Starten Sie den Tomcat-Server neu.

5.10.3.3 Einrichten von BOE Internal und Konfigurieren der benutzerdefinierten Property-Datei (für die CMC)

1. Navigieren Sie zu `<INSTALLVERZ>\tomcat\webapps\BOE\WEB-INF\internal\CmcApp.properties`.
2. Öffnen Sie die Datei "CmcApp.properties", und fügen Sie die folgenden Parameter hinzu:

   `sso.supported.types=vintela, trustedIIS, trustedHeader, trustedParameter, trustedCookie, trustedSession, trustedUserPrincipal, trustedVintela, trustedX509, sapSSO, sitemindera`
3. Starten Sie den Tomcat-Server neu.

5.10.3.4 Konfigurieren der BOE-Datei "web.xml" (für die CMC)

1. Navigieren Sie zu `<INSTALLVERZ>\tomcat\webapps\BOE\WEB-INF`.
2. Bearbeiten Sie die Datei "web.xml" an diesem Speicherort mit dem folgenden Befehl:

```
<init-param>
<param-name>extendedFrameworkExports</param-name>
<param-
value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbr
idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
bel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-
value>
</init-param>
```

3. Fügen Sie der Datei "web.xml" die gewünschten Parameter hinzu, indem Sie die folgenden Schritte ausführen:
   a. Navigieren Sie zu `<INSTALLVERZ>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.CmcApp\web\WEB-INF\web.xml`
   b. Fügen Sie die folgenden Parameter hinzu:

```
<init-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>Shared_Secret_Key</param-value>
</init-param>
```

   c. Wiederholen Sie die Schritte, indem Sie zu `<INSTALLVERZ>\\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.CmcApp\web\WEB-INF\web.xml` navigieren.

> **Hinweis**
>
> Um zu überprüfen, ob Sie die vertrauenswürdige Authentifizierung korrekt konfiguriert haben, greifen Sie über folgende URL auf die BI-Launchpad-Anwendung zu: https://[CMS-Name]:8443/BOE/BI/logon.jsp, wobei [CMS-Name] der Name des Rechners ist, auf dem der CMS gehostet wird.

5.11 OpenID-Connect-Authentifizierung

Sie können die OpenID-Connect-Authentifizierung aktivieren.

Die OpenID-Connect-Authentifizierung basiert auf dem Berechtigungsserver (OAuth). Wie die Unterstützung von Cloud-Laufwerken beruht auch die OpenID-Connect-Authentifizierung auf der Berechtigungsserver-Konfiguration. Weitere Informationen zur Berechtigungsserver-Konfiguration finden Sie unter Berechtigungsserver-Konfiguration [Seite 247].

Die OpenID-Connect-Authentifizierung wurde auf der Grundlage der Enterprise-Authentifizierung entwickelt.

Wie bei der SAML-Authentifizierung müssen Benutzer vorab als Enterprise-Benutzer (secEnterprise) in die BI-Plattform importiert werden.

> **Hinweis**
>
> Beim Importieren von Benutzern müssen Sie sicherstellen, dass auch die E-Mail-ID des Benutzers einbezogen wird.

Im Gegensatz zur SAML-Authentifizierung gilt für die OpenID-Connect-Authentifizierung Folgendes:

- Alle Konfigurationen müssen im Backend der BI-Plattform vorgenommen werden, d.h. nicht in der Schicht des Anwendungsservers.
- Sie ist nicht von der vertrauenswürdigen Authentifizierung abhängig.

Die OpenID-Connect-Authentifizierung wird nur für BI-Launchpad und OpenDocument unterstützt.

5.11.1 OpenID-Connect-Authentifizierung aktivieren

Die OpenID-Connect-Authentifizierung wird nur für BI-Launchpad und OpenDocument unterstützt.

Informationen dazu, wie Sie die OpenID-Connect-Authentifizierung aktivieren, finden Sie unter Einstellungen der Enterprise-Authentifizierung [Seite 65]. Nachdem Sie die OpenID-Connect-Authentifizierung am Plugin für die Enterprise-Authentifizierung im Backend aktiviert haben, müssen Sie für die unterstützten Anwendungen dieselbe Anwendungsschicht aktivieren (z. B. die Datei `FioriBI.properties` für das BI-Launchpad und die Datei `OpenDocument.properties` für OpenDocument-Anwendungen) unter `WEB-INF/config/custom`.

Um den Workflow für die Web-SSO-Authentifizierung zu aktivieren, setzen Sie `logon.webssoauthentication.framework` auf `OpenId`.

Legen Sie als `openid.restful.url` die RESTful-Webdienst-URL der Landschaft fest (z. B. `https://<server>:8443/biprws`).

Sie können sich über OpenID am BI-Launchpad anmelden, indem Sie die URL …`/BO/BI` verwenden. Sobald Sie sich jedoch über die OpenID-Connect-Authentifizierung am BI-Launchpad angemeldet haben, können Sie feststellen, dass der URL der Platzhalter-Kontextpfad "WEBSSO" hinzugefügt wurde. Dieser verbleibt auch in der URL, nachdem Sie sich abgemeldet haben. Wenn Sie sich über dasselbe Fenster mit derselben URL erneut anmelden möchten, müssen Sie "WEBSSO" aus der Browser-URL entfernen.

6 Verwalten von Benutzerattributen

6.1 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
- 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.

6.2 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

LDAP-Hosts konfigurieren [Seite 69]
Importieren von SAP-Rollen [Seite 94]

6.3 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.
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.

6.4 Benutzerdefinierte Benutzerattribute bearbeiten

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.
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.

7 Multitenancy

7.1 Verwalten von Tenants in der CMC

Nach der Konfiguration in der Datei `tenant_template_def.properties` und Ausführung des Multitenancy-Management-Tools zum Erstellen von Tenants, können Sie die Tenants in der Central Management Console (CMC) verwalten.

Wechseln Sie zum Verwaltungsbereich *Multitenancy* der CMC, um Tenants zu verwalten. Sie können die folgenden Aufgaben durchführen:

- Tenant-Eigenschaften festlegen, wie z.B. die maximale Anzahl an Zugriffslizenzbenutzern usw.
- Benutzer- und Gruppenzuordnungen für einen Tenant anzeigen
- Einem Tenant eine Benutzergruppe hinzufügen oder von diesem entfernen
- Einen Tenant löschen

Weitere Informationen über die Datei `tenant_template_def.properties` finden Sie in der „Tenant definition configuration file reference".

1. Festlegen von Tenant-Eigenschaften [Seite 144]
2. Zuweisen von Zugriffsrechten zu einer Tenant-Benutzergruppe [Seite 146]
3. Löschen von Tenants [Seite 149]

7.1.1 Festlegen von Tenant-Eigenschaften

In der Central Management Console (CMC) können Sie die folgenden Eigenschaften festlegen, ohne die Tenant-Eigenschaftendatei zu ändern:

- Tenant-Name
- Beschreibung
- Schlüsselwörter
- Zugriffslizenzbenutzer

Die folgenden schreibgeschützten Tenant-Eigenschaften können nicht in der CMC bearbeitet werden:

- ID
- CUID
- Erstellungsdatum
- Datum der letzten Änderung

Detaillierte Informationen über jede Eigenschaft in der Datei finden Sie in der „Tenant definition configuration file reference".

→ Tipp

Sie können einen Tenant auswählen und in der Symbolleiste auf klicken, um direkt zum Dialogfeld *Eigenschaften* zu wechseln.

Übergeordnetes Thema: Verwalten von Tenants in der CMC [Seite 144]

Nächste Aufgabe: Zuweisen von Zugriffsrechten zu einer Tenant-Benutzergruppe [Seite 146]

7.1.1.1 Ändern des Tenant-Namens

1. Wählen Sie in der Central Management Console (CMC) den Bereich *Multitenancy* aus.
2. Doppelklicken Sie auf den Tenant.
   Das Dialogfeld *Eigenschaften* des Tenants wird angezeigt.
3. Geben Sie in das Feld *Tenant-Name* einen neuen Namen für den Tenant ein.
4. Klicken Sie auf *Speichern und schließen*.
   Der von Ihnen eingegebene Name wird für den Tenant angezeigt.

7.1.1.2 Ändern der Beschreibung des Tenants

1. Wählen Sie in der Central Management Console (CMC) den Bereich *Multitenancy* aus.
2. Doppelklicken Sie auf den Tenant.
   Das Dialogfeld *Eigenschaften* des Tenants wird angezeigt.
3. Geben Sie im Feld *Beschreibung* eine Beschreibung des Tenants ein.
4. Klicken Sie auf *Speichern und schließen*.
   Die eingegebene Beschreibung wird für den Tenant angezeigt.

7.1.1.3 Ändern der Schlüsselwörter des Tenants

1. Wählen Sie in der Central Management Console (CMC) den Bereich *Multitenancy* aus.
2. Doppelklicken Sie auf den Tenant.
   Das Dialogfeld *Eigenschaften* des Tenants wird angezeigt.
3. Geben Sie im Feld *Schlüsselwörter* die Schlüsselwörter des Tenants ein.
4. Klicken Sie auf *Speichern und schließen*.
   Die eingegebenen Schlüsselwörter werden für den Tenant angezeigt.

7.1.1.4 Ändern der Anzahl der Zugriffslizenzbenutzer für einen Tenant

1. Wählen Sie in der Central Management Console (CMC) den Bereich *Multitenancy* aus.
2. Doppelklicken Sie auf den Tenant.
   Das Dialogfeld *Eigenschaften* des Tenants wird angezeigt.
3. Wählen Sie unter *Zugriffslizenzbenutzer* die maximale Anzahl an Zugriffslizenzbenutzern aus, die sich für diesen Tenant an der CMC anmelden können:
   - Um die maximale Anzahl an Benutzern für diesen Tenant anzuzeigen, die sich an der CMC anmelden können, wählen Sie *Wert*, und geben Sie eine Zahl ein.
     Wenn die maximale Anzahl überschritten wird, wird eine Meldung angezeigt und der Benutzer kann sich nicht anmelden.
   - Wenn Sie die Anzahl der Zugriffslizenzbenutzer für diesen Tenant nicht beschränken wollen, wählen Sie *Unbeschränkt*.
4. Klicken Sie auf *Speichern und schließen*.
   Die definierten Werte werden unter der Spalte *Zugriffslizenzbenutzer* auf der *Multitenancy*-Startseite angezeigt.

7.1.2 Zuweisen von Zugriffsrechten zu einer Tenant-Benutzergruppe

Sie können Zugriffsrechte für eine Tenant-Benutzergruppe in der Central Management Console (CMC) festlegen, ohne die Eigenschaftendatei zu ändern.

> → Tipp
>
> Sie können einen Tenant auswählen und in der Symbolleiste auf klicken, um direkt zum Dialogfeld *Benutzersicherheit* zu navigieren.

1. Wählen Sie in der CMC den Bereich *Multitenancy* aus.
2. Klicken Sie mit der rechten Maustaste auf den Tenant und wählen *Benutzersicherheit*.
3. Klicken Sie im Dialogfeld *Benutzersicherheit* auf *Prinzipale hinzufügen*.
4. Verschieben Sie im Dialogfeld *Prinzipale hinzufügen* die Tenant-Benutzergruppe, für die Zugriffsrechte festgelegt werden sollen, aus der Liste *Verfügbare Benutzer oder Gruppen* in die Liste *Ausgewählte Benutzer oder Gruppen*.
5. Klicken Sie auf *Sicherheit hinzufügen und zuweisen*.
6. Wählen Sie im Dialogfeld *Sicherheit zuweisen* die Zugriffsrechtebenen aus, die der Tenant-Benutzergruppe gewährt werden sollen.
7. Um die Ordnerübernahme zu aktivieren, markieren Sie das Kontrollkästchen *Vom übergeordneten Ordner übernehmen*.

   Um die Gruppenübernahme zu deaktivieren, heben Sie die Aktivierung des Kontrollkästchens auf.

8. Um die Gruppenübernahme zu aktivieren, markieren Sie das Kontrollkästchen *Von übergeordneter Gruppe übernehmen*.

   Um die Gruppenübernahme zu deaktivieren, heben Sie die Aktivierung des Kontrollkästchens auf.
9. Klicken Sie auf *OK* und dann auf *Schließen*.

Der Benutzergruppe werden die von Ihnen ausgewählten Zugriffsrechte zugewiesen.

Aufgabenübersicht: Verwalten von Tenants in der CMC [Seite 144]

Vorheriges: Festlegen von Tenant-Eigenschaften [Seite 144]

Nächste Aufgabe: Löschen von Tenants [Seite 149]

7.1.2.1 Entfernen von Zugriffsrechten aus einem Tenant

Sie können Zugriffsrechte aus einer Tenant-Benutzergruppe in der Central Management Console (CMC) entfernen, ohne die Eigenschaftendatei zu ändern.

1. Wählen Sie in der CMC den Bereich *Multitenancy* aus.
2. Klicken Sie mit der rechten Maustaste auf den Tenant und wählen *Benutzersicherheit*.
3. Klicken Sie im Dialogfeld *Benutzersicherheit* auf *Prinzipale hinzufügen*.
4. Verschieben Sie im Dialogfeld *Prinzipale hinzufügen* die Tenant-Benutzergruppe, aus der Rechte entfernt werden sollen, aus der Liste *Verfügbare Benutzer oder Gruppen* in die Liste *Ausgewählte Benutzer oder Gruppen*.
5. Klicken Sie auf *Sicherheit hinzufügen und zuweisen*.
6. Klicken Sie im Dialogfeld *Sicherheit zuweisen* auf *Zugriff entfernen*.
7. Klicken Sie auf *OK* und dann auf *Schließen*.

Es wurden alle Zugriffsrechte aus der Tenant-Benutzergruppe entfernt.

7.1.3 Verwalten von Benutzergruppen für einen Tenant

7.1.3.1 Anzeigen von Benutzer- und Gruppenassoziationen für einen Tenant

Sie können Benutzer- und Benutzergruppenassoziationen für einen Tenant in der Central Management Console (CMC) entfernen, ohne die Eigenschaftendatei zu ändern.

→ Tipp

Sie können einen Tenant auswählen und in der Symbolleiste auf klicken, um direkt zum Dialogfeld *Benutzergruppen* zu navigieren.

1. Wählen Sie in der CMC den Bereich *Multitenancy* aus.
2. Doppelklicken Sie auf den Tenant, für den Sie Benutzer- und Gruppenassoziationen anzeigen möchten.
3. Klicken Sie im Dialogfeld *Eigenschaften* in der Navigationsliste auf *Benutzergruppen*.
   Das Dialogfeld *Benutzergruppen* wird angezeigt, in dem die diesem Tenant zugehörigen Gruppen aufgeführt werden.

7.1.3.2 Hinzufügen einer Benutzergruppe zu einem Tenant

In der Central Management Console (CMC) können Sie einem Tenant eine Benutzergruppe hinzufügen, ohne die Eigenschaftendatei zu ändern.

→ Tipp

Sie können einen Tenant auswählen und in der Symbolleiste auf klicken, um direkt zum Dialogfeld *Gruppen zu Tenant hinzufügen* zu wechseln.

1. Wählen Sie in der CMC den Bereich *Multitenancy* aus.
2. Klicken Sie mit der rechten Maustaste auf den Tenant, dem die Benutzergruppe hinzugefügt werden soll, und wählen Sie *Gruppen zu Tenant hinzufügen*.
3. Verschieben Sie im Dialogfeld *Gruppen zu Tenant hinzufügen* die hinzuzufügende Benutzergruppe von der Liste *Verfügbare Listen* in die Liste *Ausgewählte Gruppen*.
4. Klicken Sie auf *OK*.

Die Benutzergruppe wird dem Tenant hinzugefügt.

7.1.3.3 Entfernen von Benutzergruppen aus einem Tenant

Sie können eine Benutzergruppe aus einem Tenant in der Central Management Console (CMC) entfernen, ohne die Eigenschaftendatei zu ändern.

1. Wählen Sie in der CMC den Bereich *Multitenancy* aus.
2. Doppelklicken Sie auf den Tenant, aus dem Sie eine Benutzergruppe entfernen möchten.
3. Klicken Sie im Dialogfeld *Eigenschaften* des Tenants in der Navigationsliste auf *Benutzergruppen*.
4. Wählen Sie im Dialogfeld *Benutzergruppen* die zu entfernende Benutzergruppe aus und klicken auf *Entfernen*.

Die Benutzergruppe wird aus dem Tenant entfernt.

7.1.4 Löschen von Tenants

Sie können Tenants und alle zugehörigen Objekte in der Central Management Console (CMC) aus dem BI-Repository löschen.

> ⓘ Hinweis
>
> Freigegebene Objekte oder Objekte, für die keine Änderungsberechtigungen gewährt wurden, werden nicht gelöscht.

> → Tipp
>
> Sie können einen Tenant auswählen und in der Symbolleiste auf klicken, um direkt zum Dialogfeld *Löschen* zu navigieren.

1. Wählen Sie in der CMC den Bereich *Multitenancy*.
2. Klicken Sie mit der rechten Maustaste auf einen Tenant und wählen *Löschen*.
3. Verschieben Sie im Dialogfeld *Löschen* den zu löschenden Tenant aus der Liste *Verfügbar* in die Liste *Ausgeschlossen*, und klicken Sie auf *OK*.
4. Klicken Sie im Bestätigungsdialogfeld erneut auf *OK*.

Der Tenant wurde aus dem Central-Management-Server-Repository gelöscht.

Aufgabenübersicht: Verwalten von Tenants in der CMC [Seite 144]

Vorherige Aufgabe: Zuweisen von Zugriffsrechten zu einer Tenant-Benutzergruppe [Seite 146]

8 Verwalten der Lizenz

8.1 Verwalten von Lizenzschlüsseln

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

Weitere Informationen

Anzeigen von Lizenzinformationen [Seite 150]
Hinzufügen von Lizenzschlüsseln [Seite 150]
So zeigen Sie die aktuelle Kontoaktivität an [Seite 151]

8.1.1 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 150]
So zeigen Sie die aktuelle Kontoaktivität an [Seite 151]

8.1.2 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.

> **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.

> **Hinweis**
>
> Wenn Sie ein Update von einer niedrigeren Version auf SAP BusinessObjects Business Intelligence 4.2 Support Package 2 oder eine höhere Version durchführen, verhalten sich die vorhandenen Lizenzen wie abgelaufene Lizenzen. Sie müssen einen neuen Lizenzschlüssel für SAP BusinessObjects Business Intelligence 4.2 generieren und verwenden.

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 150]
So zeigen Sie die aktuelle Kontoaktivität an [Seite 151]

8.1.3 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 150]
Anzeigen von Lizenzinformationen [Seite 150]

9 Verwalten von Servern

9.1 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.

Option in der Navigations-struktur	Beschreibung
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* • *Hochstufverwaltungsdienste* • *Analysis Services* • *Web-Intelligence-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* • *Wird mit Fehlern ausgeführt* • *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.
Zustand	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* • *Wird mit Fehlern ausgeführt* • *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 Sie 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.

Spalte des Detailbereichs	Beschreibung
Beschreibung	Zeigt eine Beschreibung des Servers an. Sie können diese Beschreibung auf der Seite *Eigenschaften* des Servers ändern.
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.

9.2 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.

   > ⓘ Hinweis
   >
   > Dies ist besonders hilfreich, wenn Sie schnell eine Liste der Server anzeigen lassen möchten, die nicht ordnungsgemäß gestartet bzw. unerwartet gestoppt wurden.

9.3 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*.

9.4 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.

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.

9.5 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*.

9.6 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.
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.

9.7 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.

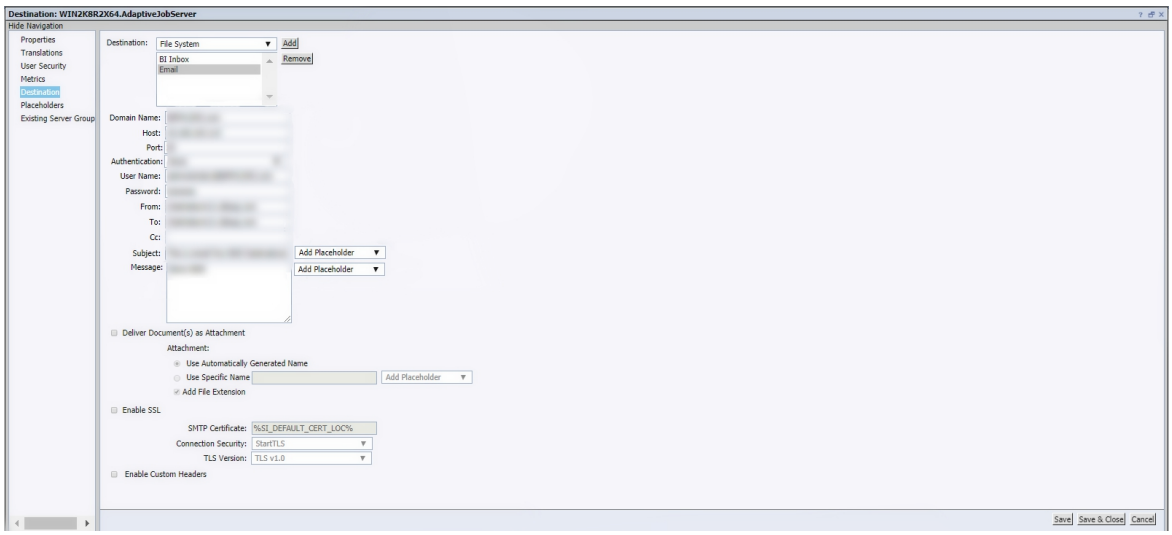
9.8 Löschen von Servern

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*.

9.9 Benutzerdefinierte Kopfinformationen hinzufügen

Die Internetkopfzeile einer E-Mail enthält Informationen zum Verfasser der Nachricht, dem E-Mail-Server, den die Nachricht durchlaufen hat, und dem Programm bzw. der Software, mit der die Nachricht verfasst wurde. Sie können nun E-Mails, die mit SAP BusinessObjects BI zeitgesteuert verarbeitet werden, benutzerdefinierte Kopfinformationen hinzuzufügen. Gehen Sie wie folgt vor, um benutzerdefinierte Kopfinformationen hinzuzufügen:

1. Melden Sie sich an der *CMC* an.
2. Wählen Sie *Server* und anschließend *Serverliste*.
3. Öffnen Sie das Kontextmenü des *Adaptive Job Server*, und wählen Sie *Ziele*.
4. Wählen Sie im Assistenten für das *Ziel* die Option *E-Mail*, und geben
   Sie die folgenden erforderlichen Informationen in die entsprechenden Felder ein:



5. Aktivieren Sie die Option *Benutzerdefinierte Köpfe aktivieren*, und geben Sie die folgenden Internetkopfinformationen in das leere Feld ein:

6. Wählen Sie *Sichern und schließen*.

E-Mails mit zeitgesteuerten Dokumenten enthalten nun Ihre Internetkopfinformationen.

> **Hinweis**
>
> - Wählen Sie beim zeitgesteuerten Verarbeiten die Option *Standardeinstellungen verwenden*, um zeitgesteuerten E-Mails benutzerdefinierte Internetkopfinformationen hinzuzufügen.
> - Es wird empfohlen, alle *Adaptive Job Server* dahingehend zu konfigurieren, jeder E-Mail benutzerdefinierte Kopfinformationen hinzuzufügen.

9.10 Nichtexklusive Servergruppen erstellen

Nichtexklusive Servergruppen können Server oder Servergruppen enthalten, die Bestandteil einer anderen nichtexklusiven Servergruppe oder des allgemeinen Server-Pools sind.

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. Wählen Sie *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*.
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.

   > **Hinweis**
   >
   > Die aufgeführten Server umfassen nur Server, die nicht Teil einer anderen exklusiven Servergruppe sind.
9. Wählen Sie *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.

9.11 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.
5. Klicken Sie auf *OK*.

   Im Verwaltungsbereich *Server* werden nun alle zur übergeordneten Gruppe hinzugefügten Servergruppen angezeigt.

9.12 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.

   > ⓘ Hinweis
   >
   > Für exklusive Servergruppen auf Stammebene sind alle exklusiven Servergruppen unter *Verfügbare Servergruppen* aufgeführt. Sie können nur eine (1) exklusive Servergruppe auswählen und diese in *Mitglied von Servergruppen* verschieben, da für eine exklusive Servergruppe nur eine (1) übergeordnete Servergruppe vorliegen kann.
   >
   > Für untergeordnete exklusive Servergruppen werden keine Servergruppen unter *Verfügbare Servergruppen* aufgeführt, da untergeordnete exklusive Servergruppen jeweils nur eine (1) übergeordnete Servergruppe aufweisen können.
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. Wählen Sie *OK*.

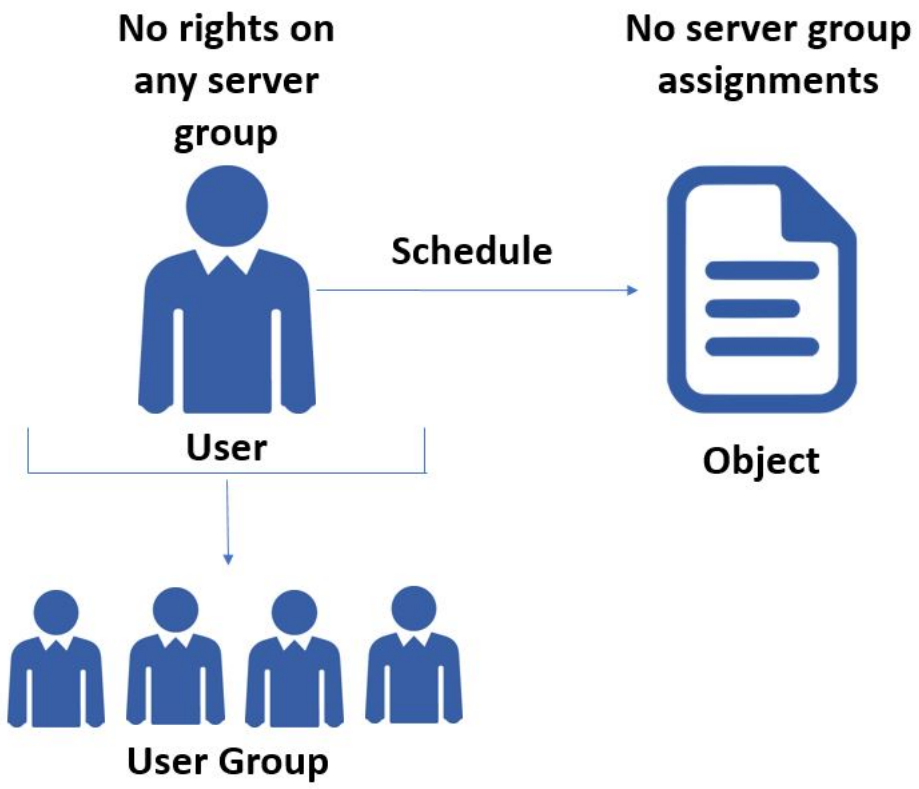
9.13 Rechteverwaltung für Servergruppen

Sie können Zugriffsrechte für Servergruppen auf Benutzer- und Benutzergruppenebene aktivieren. Mit dieser Option kann für alle Benutzer und Benutzergruppen der Zugriff auf Servergruppen gesteuert werden.

> **Hinweis**
>
> - In den folgenden Szenarios dient die zeitgesteuerte Verarbeitung als Beispiel zur Veranschaulichung der Rechteverwaltung für Servergruppen. Analog werden Servergruppenrechte auch für die Anzeige und das Caching verwaltet.
> - Objekte können erfolgreich zeitgesteuert verarbeitet werden, wenn die jeweiligen Server in der Servergruppe oder Servergruppenkombination verfügbar sind. Die zeitgesteuerte Verarbeitung schlägt fehl, wenn kein Server zur Verfügung steht.

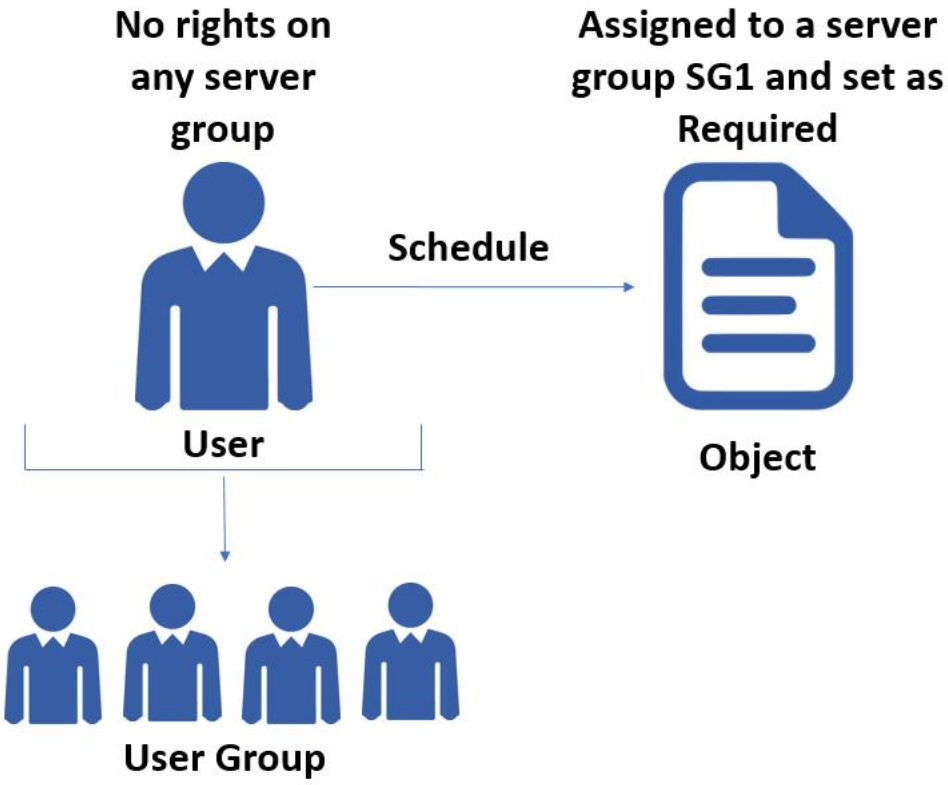
Szenario 1:

Im Idealfall ist ein Benutzer Mitglied einer Benutzergruppe in Business Intelligence. Der Benutzer und die zugehörige Benutzergruppe verfügen für keine der Servergruppen über Berechtigungen. Der Benutzer möchte nun ein Objekt zeitgesteuert verarbeiten, das ebenfalls keiner Servergruppe zugeordnet ist.



Szenario 2:

Wenn Sie dem Objekt im obigen Szenario eine Servergruppe zuordnen, schlägt die zeitgesteuerte Verarbeitung des Objekts fehl.



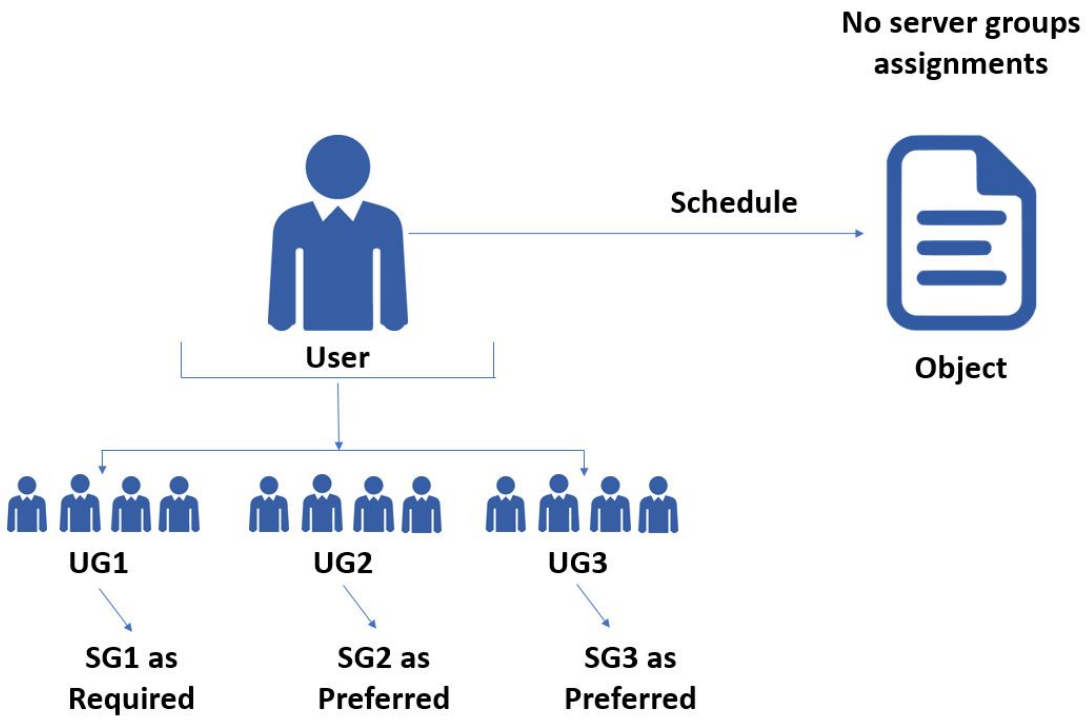
Wenn ein Benutzer ein Objekt zeitgesteuert verarbeitet, wird die Servergruppenzuordnung des entsprechenden Objekts geprüft. Ist dem Objekt eine Servergruppe zugeordnet, wird geprüft, ob der Benutzer über Anzeigerechte für die Servergruppe verfügt.

In Szenario 2 verfügt weder der Benutzer noch die zugehörige Benutzergruppe über Berechtigungen für SG1. Dies hat zur Folge, dass die zeitgesteuerte Verarbeitung des Jobs fehlschlägt. Damit der Benutzer ein Objekt in diesem Szenario erfolgreich zeitgesteuert verarbeiten kann, muss der Benutzer bzw. die zugehörige Benutzergruppe Anzeigerechte für SG1 besitzen.

Szenario 3:

> ⓘ Hinweis
>
> In Szenario 3 und 4 wird davon ausgegangen, dass der Benutzer die Berechtigungen der zugehörigen Benutzergruppe übernimmt.

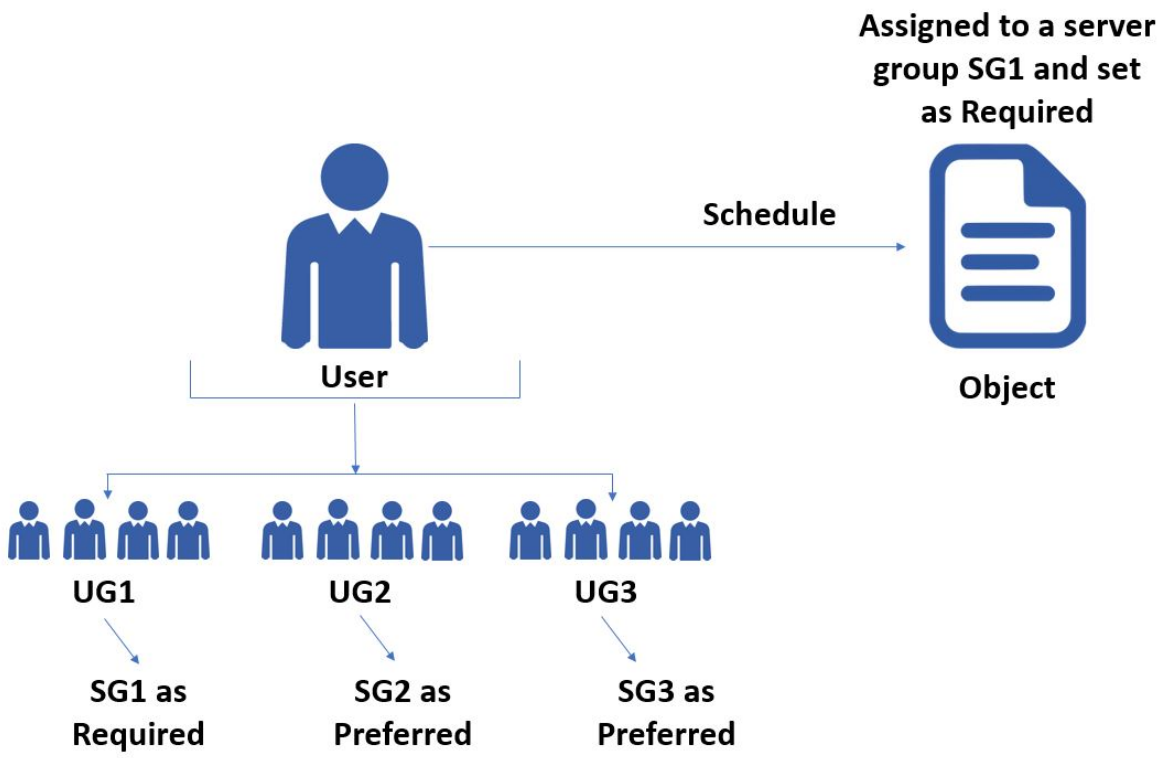
Der Benutzer ist Mitglied der Benutzergruppen UG1, UG2 und UG3, und Sie haben die jeweilige Benutzergruppe den Servergruppen SG1, SG2 und SG3 zugeordnet. SG1 ist als erforderliche Servergruppe und SG2 und SG3 als bevorzugte Servergruppe definiert. Weitere Informationen darüber, wie Sie Servergruppen als "Erforderlich" und "Bevorzugt" definieren, finden Sie unter *Zuordnen einer Benutzergruppe zu einer Servergruppe* im *Business Intelligence Platform Administrator Guide*.



Wenn ein Benutzer mehreren Servergruppen und jede Benutzergruppe einer anderen Servergruppe zugeordnet ist, wird die verfügbare Servergruppe ermittelt. Im obigen Szenario ist die zeitgesteuerte Verarbeitung erfolgreich, weil das Objekt keiner Servergruppe zugeordnet ist und die Kombination der verfügbaren Servergruppen für die Verarbeitung des Objekts SG1, SG2 und SG3 lautet.

Szenario 4:

Sie haben wie in Szenario 3 dargestellt außerdem das Objekt SG1 zugeordnet und SG1 als "Erforderlich" definiert. Weitere Informationen darüber, wie Sie Servergruppen als "Erforderlich" und "Bevorzugt" definieren, finden Sie unter *Zuordnen einer Benutzergruppe zu einer Servergruppe* im *Business Intelligence Platform Administrator Guide*.



Ist dem Objekt eine Servergruppe zugeordnet, wird geprüft, ob Sie dem Benutzer die Anzeigerechte für die Servergruppe gewährt haben. In diesem Szenario wird die verfügbare Servergruppe nicht ermittelt, da die Servergruppenzuordnung auf Objektebene die höchste Priorität hat. In Szenario 4 ist die zeitgesteuerte Verarbeitung des Objekts erfolgreich, da UG1 über Anzeigerechte für SG1 verfügt und der Benutzer diese von UG1 übernimmt.

→ Nicht vergessen

- Die Servergruppenzuordnung aller Benutzergruppen, die der Benutzer zugeordnet ist, muss vor der zeitgesteuerten Verarbeitung eines Objekts geprüft und die verfügbare Servergruppe ermittelt werden.
- Die zeitgesteuerte Verarbeitung ist dann erfolgreich, wenn die für einen Benutzer verfügbare Servergruppe die Servergruppe umfasst, die dem Objekt zugeordnet ist.

Schauen Sie sich die Tabelle unten an:

ⓘ Hinweis

Berücksichtigen Sie, dass SG1 und SG2 der Benutzergruppe UG1 bzw. UG2 zugeordnet sind.

Zugriffsberechtigung	Kombination von Servergruppen (SG1 + SG2)	Suche nach Servern im allgemeinen Pool
Benutzer verfügt über Rechte für alle Servergruppen	Erforderlich + Erforderlich	Falsch

Zugriffsberechtigung	Kombination von Servergruppen (SG1 + SG2)	Suche nach Servern im allgemeinen Pool
Benutzer verfügt über Rechte für alle Servergruppen	Erforderlich + Bevorzugt	Falsch
Benutzer verfügt über Rechte für alle Servergruppen	Bevorzugt + Bevorzugt	Wahr
Benutzer verfügt über keinerlei Rechte für eine Servergruppe	Erforderlich + Erforderlich	Falsch
Benutzer verfügt über keinerlei Rechte für eine Servergruppe	Erforderlich + Bevorzugt	Falsch
Benutzer verfügt über keinerlei Rechte für eine Servergruppe	Bevorzugt + Bevorzugt	Wahr
Benutzer verfügt über Rechte für einige Servergruppen	Erforderlich (Nein) + Erforderlich (Ja)	Falsch
Benutzer verfügt über Rechte für einige Servergruppen	Erforderlich (Nein) + Bevorzugt (Ja)	Falsch
Benutzer verfügt über Rechte für einige Servergruppen	Erforderlich (Ja) + Bevorzugt (Nein)	Falsch
Benutzer verfügt über Rechte für einige Servergruppen	Erforderlich (Nein) + Bevorzugt (Ja)	Wahr

9.14 Gruppenzugehörigkeit eines Servers ändern

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.

   > **Hinweis**
   >
   > Für Servergruppen auf Stammebene sind alle exklusiven Servergruppen unter *Verfügbare Servergruppen* aufgeführt. Sie können nur eine (1) exklusive Servergruppe auswählen und diese in *Mitglied von Servergruppen* verschieben, da für eine exklusive Servergruppe nur eine (1) übergeordnete Servergruppe vorliegen kann. Nachdem Sie eine exklusive Servergruppe unter *Verfügbare Servergruppen* ausgewählt und diese in *Mitglied von Servergruppen* verschoben haben, wird die exklusive Servergruppe aus der Stamm-Servergruppe entfernt und in eine neue Servergruppe verschoben, der sie zugeordnet ist.

> Für untergeordnete Servergruppen werden vorhandene übergeordnete Servergruppen unter *Mitglied von Servergruppen* angezeigt. Weitere exklusive Servergruppen sind unter *Verfügbare Servergruppen* aufgeführt. Sie können die Zuordnung einer untergeordneten Servergruppe zu einer übergeordneten exklusiven Servergruppe aufheben und sie einer anderen übergeordneten exklusiven Servergruppe zuordnen.

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*.

> ⓘ Hinweis
>
> Die Option *Aus Servergruppe entfernen* wird nur für untergeordnete exklusive Servergruppen angezeigt. Wenn eine untergeordnete exklusive Servergruppe aus der übergeordneten Servergruppe entfernt wird, behält sie den Status "exklusiv" bei und wird auf die Stammebene verschoben.
>
> Servergruppen werden im BI-Launchpad angezeigt, wenn der Administrator über die CMC Benutzersicherheitsrechte für bestimmte Servergruppen erteilt.

9.15 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.

9.16 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.

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 167]

9.17 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.

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 166]

9.18 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.

9.19 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 166]
Info zu Servermetriken (Anhang) [Seite 537]

9.20 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.

9.21 So aktivieren oder deaktivieren Sie Ziele für einen Job Server

Damit ein Adaptive Job Server Ausgabeinstanzen unter einem anderen Ziel als dem Standardziel speichern kann, müssen Sie die anderen Ziele auf den Job Servern aktivieren und konfigurieren.

> ⓘ Hinweis
>
> Das verwaltete Ziel (Posteingang) ist standardmäßig aktiviert und auf allen Job Servern konfiguriert. Dies ermöglicht Ihnen die Verwendung der Funktion "Senden an" und die Verteilung von Berichten an Benutzer innerhalb des BI-Plattform-Systems. Zusätzliche Ziele auf dem Server können nach Bedarf aktiviert und konfiguriert werden.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Wählen Sie den Job Server aus, für den Sie ein Ziel aktivieren oder deaktivieren möchten.
3. Wählen Sie im Menü *Verwalten* den Befehl *Eigenschaften* aus.
4. Klicken Sie im Dialogfeld *Eigenschaften* in der Navigationsliste auf *Ziele*.
5. Um ein Ziel zu aktivieren, wählen Sie es in der Liste *Ziel* aus und klicken auf *Hinzufügen*.
6. Um ein Ziel zu deaktivieren, wählen Sie es in der Liste *Ziel* aus und klicken auf *Entfernen*.
7. Klicken Sie auf *Speichern* oder *Speichern und schließen*.

Weitere Informationen

Festlegen der Zieleigenschaften für einen Job Server [Seite 170]

9.22 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 556]

9.23 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.

> ⚠ Achtung
>
> Platzhalter, die nicht zur Bearbeitung vorgesehen sind, sollten in keiner Weise geändert werden. Der Systemadministrator muss sicherstellen, dass nur die richtige Person aus der Administratorgruppe (die für die Knotenverwaltung vorgesehen ist) über die Bearbeitungsrechte für den Knoten verfügt. Für alle anderen Benutzer, einschließlich anderer Mitglieder der Administratorgruppe, sollte die Anzeige/Verwaltung der Knotenobjekte durch Anwendung der entsprechenden Sicherheitsrechte eingeschränkt werden. Wenn einer der Platzhalterwerte versehentlich beschädigt wurde und der CMS nicht angezeigt wird, lesen Sie den folgenden SAP-Hinweis 3269127.

> ⓘ Hinweis
>
> Im SAP-Knowledge-Base-Artikel 3278916 erfahren Sie, wie Sie einschränken können, dass Platzhalter verändert werden, um so mögliche schädliche Beeinträchtigungen der BI-Landschaft zu verhindern.

Weitere Informationen

Server- und Knotenplatzhalter [Seite 556]

9.24 Festlegen der Zieleigenschaften für einen Job Server

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Wählen Sie den Job Server aus, dessen Einstellung Sie ändern möchten.
3. Wählen Sie im Menü *Verwalten* den Befehl *Eigenschaften* aus.
4. Klicken Sie im Dialogfeld *Eigenschaften* in der Navigationsliste auf *Ziele*.
5. Wählen Sie ein Ziel aus der Liste aus, und klicken Sie dann auf *Hinzufügen*.

6. Legen Sie die Eigenschaften für das Ziel fest:
7. Klicken Sie auf *Speichern* oder *Speichern und schließen*.
8. Stellen Sie sicher, dass das Ziel aktiviert ist.

Weitere Informationen

So aktivieren oder deaktivieren Sie Ziele für einen Job Server [Seite 169]
Eigenschaften für Posteingangsziele [Seite 171]
Eigenschaften für Dateisystemziele [Seite 175]
Eigenschaften für FTP-Ziele [Seite 173]
Eigenschaften für E-Mail-Ziele [Seite 172]

9.24.1 Eigenschaften für Posteingangsziele

Beim Posteingangsziel wird ein Objekt oder eine Instanz in den Benutzer-Posteingängen auf dem BI-Plattform-System gespeichert. Wenn Sie einen Benutzer hinzufügen, wird automatisch ein Benutzer-Posteingang erstellt.

> ⓘ Hinweis
>
> Das verwaltete Ziel (Posteingang) auf dem Destination Job Server ist auf allen Job Servern standardmäßig aktiviert und konfiguriert. Dies ermöglicht Ihnen die Verwendung der Funktion "Senden an" und die Verteilung von Berichten an Benutzer innerhalb des BI-Plattform-Systems. Zusätzliche Ziele auf dem Adaptive Job Server können nach Bedarf aktiviert und konfiguriert werden.

Sendeliste

Geben Sie an, welche Benutzer oder Benutzergruppen Instanzen empfangen sollen, die vom Job Server generiert oder verarbeitet wurden.

Zielname

Verwenden Sie den automatisch generierten Standardnamen für die Instanz, oder geben Sie einen bestimmten Namen an. Sie können dem jeweiligen Namen Variablen hinzufügen, indem Sie in der Liste *Platzhalter hinzufügen* darauf klicken.

Dokument senden als

Wählen Sie die gewünschten Optionen aus:

- *Verknüpfung*
  Das System sendet eine Verknüpfung an das angegebene Ziel.
- *Kopie*
  Das System sendet eine Kopie der Objektinstanz an das Ziel.

9.24.2 Eigenschaften für E-Mail-Ziele

Die folgenden Einstellungen sind für E-Mail-Ziele verfügbar.

Domänenname

Geben Sie den voll qualifizierten Domänennamen des SMTP-Servers ein.

Host

Geben Sie den Namen des SMTP-Servers ein.

Port

Geben Sie den Port ein, der für den SMTP-Server verfügbar ist. (Der Standard-SMTP-Port ist 25.)

Authentifizierung

Wählen Sie "Einfach" oder "Anmeldung" aus, wenn der Job Server mit einer der folgenden Methoden authentifiziert werden muss, um E-Mails versenden zu können.

Benutzername

Geben Sie einen Benutzernamen an, der berechtigt ist, E-Mails und Anhänge über den SMTP-Server zu versenden.

Kennwort

Geben Sie für den Job Server das SMTP-Serverkennwort an.

Von

Geben Sie eine E-Mail-Adresse als Absender an. Sie können diese Standardeinstellung bei der zeitgesteuerten Verarbeitung eines Objekts außer Kraft setzen.

"An", "Cc", "Betreff" und "Nachricht"

Legen Sie die Standardwerte für Benutzer fest, die Berichte für dieses SMTP-Ziel zeitgesteuert verarbeiten.

> **Hinweis**
>
> Diese Standardeinstellungen können vom Benutzer bei der zeitgesteuerten Verarbeitung eines Objekts außer Kraft gesetzt werden.

Antwort an

Über die Option *Antwort an* können Sie nun bestimmte Benutzer als Ziel für eine E-Mail angeben. Dies ist sowohl für die zeitgesteuerte Verarbeitung in der CMC als auch im BI-Launchpad möglich.

Platzhalter hinzufügen

Über die Liste *Platzhalter hinzufügen* können Sie dem Nachrichtentext Platzhaltervariablen hinzufügen. Beispielsweise können Sie den Berichttitel bzw. Autor oder die URL für den Viewer hinzufügen, in dem der Bericht vom E-Mail-Empfänger angezeigt werden soll.

Anlage hinzufügen

Aktivieren Sie dieses Kontrollkästchen, wenn eine Kopie des Berichts oder der Programminstanz an die E-Mail-Nachricht angefügt werden soll. Wenn Sie eine Anlage hinzufügen, können Sie unter den folgenden Namenskonventionen wählen:

- *Automatisch generiert*
  Wählen Sie diese Option, wenn die BI-Plattform einen zufallsgenerierten Dateinamen erzeugen soll.
- *Bestimmter Name*
  Wählen Sie diese Option, wenn Sie einen Dateinamen eingeben möchten. Sie können dem Dateinamen auch eine Variable hinzufügen. Um eine Variable hinzuzufügen, wählen Sie aus der Liste *Platzhalter hinzufügen* einen Platzhalter für eine Variableneigenschaft aus.
- *Dateierweiterung hinzufügen*
  Fügt dem angegebenen Dateinamen die Erweiterung .%EXT% hinzu. Dies ist mit dem Auswählen von "Dateierweiterung" aus der Liste *Platzhalter hinzufügen* vergleichbar. Indem Sie dem Dateinamen eine Erweiterung hinzufügen, kann Windows ermitteln, welches Programm zum Öffnen der Datei verwendet werden soll.

9.24.2.1 Einrichten von SMTP über SSL

Um SMTP über SSL einzurichten, muss dasselbe Zertifikat in den Server- und Client-Systemen vorhanden sein.

Um SMTP über SSL einzurichten, führen Sie die folgenden Schritte aus:

1. Wechseln Sie unter Windows zu `<InstallVerz>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.Wechseln Sie zusätzlich für mit der BI-Plattform verbundene Clients zu `<InstallVerz>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.

   > **Hinweis**
   >
   > Navigieren Sie bei allen anderen unterstützten Plattformen zum entsprechenden Ordner.

2. Geben Sie dem Zertifikat den Namen „certificate.crt“.

   Beispielsweise sendet der Server beim Verbinden mit dem SMTP-Server die Zertifikatsinformationen. Die Zertifikatsinformationen müssen in eine Nur-Text-Datei kopiert werden, die in „certificate.crt“ umbenannt wird. Diese muss im Ordner „win64_x64“ für die Windows-Plattform und für die Clients im Ordner „win32_86“ abgelegt werden.

SMTP über SSL ist nun eingerichtet.

> **Hinweis**
>
> Wenn der Benutzer das Kontrollkästchen *SSL aktivieren* markiert, wird ein sicherer Kanal aktiviert. Damit ist eine sichere SMTP-Übertragung über SSL möglich.

9.24.3 Eigenschaften für FTP-Ziele

Die folgenden Einstellungen sind für FTP-Ziele verfügbar.

Host

Tragen Sie hier die Angaben zum FTP-Host ein.

Port

Geben Sie die Nummer des FTP-Ports ein (Standard-FTP-Port: 21).

Benutzername

Geben Sie einen Benutzer an, der über die erforderlichen Rechte zum Hochladen von Berichten auf den FTP-Server verfügt.

Kennwort

Geben Sie das Kennwort des Benutzers ein.

Konto

Geben Sie, sofern erforderlich, die Angaben zum FTP-Konto ein.

Das Konto ist Teil des Standard-FTP-Protokolls, wird jedoch selten genutzt. Stellen Sie das entsprechende Konto nur bereit, wenn es vom FTP-Server angefordert wird.

Verzeichnis

Geben Sie das Verzeichnis auf dem FTP-Server an, in dem das Objekt gespeichert werden soll. Ein relativer Pfad wird relativ zum Root-Verzeichnis des FTP-Servers interpretiert.

Automatisch generiert

Wählen Sie diese Option, wenn die BI-Plattform einen zufallsgenerierten Dateinamen erzeugen soll.

Bestimmter Name

Wählen Sie diese Option, wenn Sie den Dateinamen selbst eingeben möchten. Der Dateiname kann auch Variablen enthalten. Um eine Variable hinzuzufügen, wählen Sie aus der Liste einen Platzhalter für eine Variableneigenschaft aus.

Dateierweiterung hinzufügen

Fügt dem angegebenen Dateinamen die Erweiterung .%EXT% hinzu. Dies ist mit dem Auswählen von "Dateierweiterung" aus der Liste *Platzhalter hinzufügen* vergleichbar. Indem Sie dem Dateinamen eine Erweiterung hinzufügen, kann Windows ermitteln, welches Programm zum Öffnen der Datei verwendet werden soll.

9.24.4 Eigenschaften für SFTP-Ziele

Die folgenden Einstellungen sind für SFTP-Ziele verfügbar.

Host

Tragen Sie hier die Angaben zum SFTP-Host ein.

Port

Geben Sie die Nummer des SFTP-Ports ein (Standard-SFTP-Port: 22).

Benutzername

Geben Sie einen Benutzer an, der über die erforderlichen Rechte zum Hochladen von Berichten auf den SFTP-Server verfügt.

Kennwort

Geben Sie das Kennwort des Benutzers ein.

Konto

Geben Sie, sofern erforderlich, die Angaben zum SFTP-Konto ein.

Das Konto ist Teil des Standard-SFTP-Protokolls, wird jedoch selten genutzt. Stellen Sie das entsprechende Konto nur bereit, wenn es vom SFTP-Server angefordert wird.

Verzeichnis

Geben Sie das Verzeichnis auf dem SFTP-Server an, in dem das Objekt gespeichert werden soll. Ein relativer Pfad wird relativ zum Root-Verzeichnis des SFTP-Servers interpretiert.

Automatisch generiert

Wählen Sie diese Option, wenn die BI-Plattform einen zufallsgenerierten Dateinamen erzeugen soll.

Bestimmter Name

Wählen Sie diese Option, wenn Sie den Dateinamen selbst eingeben möchten. Der Dateiname kann auch Variablen enthalten. Um eine Variable hinzuzufügen, wählen Sie aus der Liste einen Platzhalter für eine Variableneigenschaft aus.

Fingerabdruck

Geben Sie den Hostschlüssel-Fingerabdruck des SFTP-Servers ein.

Dateierweiterung hinzufügen

Fügt dem angegebenen Dateinamen die Erweiterung .%EXT% hinzu. Dies ist mit dem Auswählen von „Dateierweiterung“ aus der Liste *Platzhalter hinzufügen* vergleichbar. Indem Sie dem Dateinamen eine Erweiterung hinzufügen, kann Windows ermitteln, welches Programm zum Öffnen der Datei verwendet werden soll.

9.24.5 Eigenschaften für Dateisystemziele

Ein Dateisystemziel ist ein Ziel auf einem nicht verwalteten Datenträger in einem System außerhalb des BI-Plattform-Systems.

Verzeichnis

Geben Sie den absoluten Pfad zum Verzeichnis ein. Das Verzeichnis kann sich auf einem lokalen Laufwerk des Adaptive Job Server-Rechners oder auf einem anderen Rechner befinden, den Sie mit einem UNC-Pfad angeben können.

Automatisch generiert

Wählen Sie diese Option, wenn die BI-Plattform einen zufallsgenerierten Dateinamen erzeugen soll.

Bestimmter Name

Wählen Sie diese Option, wenn Sie den Dateinamen selbst eingeben möchten. Der Dateiname kann auch Variablen enthalten. Um eine Variable hinzuzufügen, wählen Sie aus der Liste einen Platzhalter für eine Variableneigenschaft aus.

Dateierweiterung hinzufügen

Fügt dem angegebenen Dateinamen die Erweiterung .%EXT% hinzu. Dies ist mit dem Auswählen von "Dateierweiterung" aus der Liste *Platzhalter hinzufügen* vergleichbar. Indem Sie dem Dateinamen eine Erweiterung hinzufügen, kann Windows ermitteln, welches Programm zum Öffnen der Datei verwendet werden soll.

Benutzername

Geben Sie einen Benutzer an, der berechtigt ist, Dateien in das Zielverzeichnis zu schreiben.

Kennwort

Geben Sie das Kennwort für den Benutzer ein.

Im folgenden Beispiel befindet sich das Zielverzeichnis auf einem Netzlaufwerk, auf das der Adaptive Job Server-Rechner über einen UNC-Pfad zugreift. Jeder Dateiname wird zufällig generiert. Es wurden ein Benutzername und ein Kennwort angegeben, die den Adaptive Job Server dazu berechtigen, Dateien in das entfernte Verzeichnis zu schreiben.

9.25 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:

- 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 18]. 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 von Servern [Seite 157].

→ 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 Verwalten von Web Application Container Servern (WACS)

10.1 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.

10.2 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.

10.2.1 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.

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.

> **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.

10.2.2 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*.
   - 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.

10.2.3 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*.

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 189]

10.2.4 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*.

10.3 Hinzufügen oder Entfernen von Diensten auf dem WACS

10.3.1 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.

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.

10.3.2 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.

Der Dienst wird vom WACS entfernt.

10.4 Konfigurieren von WACS für AD Kerberos

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:

- 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

Weitere Informationen zur Durchführung dieser Aufgaben finden Sie im Kapitel „Verwalten von Web-Application-Container-Servern (WACS)“ des *Administratorhandbuchs für die BI-Plattform*.

Nachdem Sie den Rechner, auf dem der WACS gehostet wird, für die Verwendung der AD Kerberos-Authentifizierung eingerichtet haben, führen Sie diese Schritte über die Central Management Console (CMC) aus.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den WACS, für den Sie AD konfigurieren möchten.
   Der Bildschirm *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.

10.5 Konfigurieren der WACS AD Kerberos-Einzelanmeldung

Wenn Sie die AD Kerberos-Einzelanmeldung für auf dem WACS gehostetes BI-Launchpad oder Web Services SDK und QaaWS konfigurieren, müssen Sie sicherstellen, dass Sie den Rechner, auf dem WACS gehostet wird, für die AD Kerberos-Authentifizierung und die AD Kerberos-Einzelanmeldung konfiguriert haben. Weitere Informationen finden Sie im Kapitel „Verwalten von Web-Application-Container-Servern (WACS)“ des *Administratorhandbuchs für die BI-Plattform*.

Nachdem Sie den Rechner, auf dem der WACS gehostet wird, für die Verwendung von AD Kerberos-Authentifizierung und -Einzelanmeldung eingerichtet haben, führen Sie diese Schritte über die Central Management Console (CMC) aus.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Doppelklicken Sie auf den WACS, den Sie konfigurieren möchten.
   Der Bildschirm *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.

10.6 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 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.

    > **Hinweis**
    >
    > Weitere Informationen zur Einrichtung einer vertrauenswürdigen Authentifizierung mit X.509-Zertifikaten finden Sie in Für RESTful Web-Services [Seite 136].

    > **Hinweis**
    >
    > Sie können das Zertifikat eines ABAP-Systems in die BI-Plattform importieren, indem Sie folgenden Befehl ausführen: `keytool -import -trustcacerts -alias <Alias_Name>`

`-file <CA_certificate_path> -keystore <trust_keystore_path>` . In der folgenden Tabelle wird der Befehl erläutert:

Befehl	Beschreibung
-alias	Aliasname
-file	Dateipfad des Zertifikats des ABAP-Systems
-keystore	Dateipfad des vertrauenswürdigen Keystore

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.

10.7 WACS und Ihre IT-Umgebung

In diesem Abschnitt wird beschrieben, wie Sie den WACS in einer komplexen Umgebung konfigurieren.

10.7.1 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.

10.7.1.1 WACS für die Unterstützung von HTTP mit einem Reverse Proxy konfigurieren

Um einen WACS in einer Implementierung mit einem Reverse Proxy zu verwenden, konfigurieren Sie den WACS so, 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*.

10.7.1.2 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 für HTTPS für externen Datenverkehr über den Reverseproxy und den anderen WACS für die Kommunikation mit Clients im internen Netzwerk über HTTPS.

10.7.2 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.

10.8 Fehlerbehebung

10.8.1 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 549]

10.8.2 Status eines WACS anzeigen lassen

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 „Wird mit Fehlern ausgeführt“. 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.

10.8.3 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-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.

10.8.3.1 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*.

10.8.3.2 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*.

10.8.4 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*.

10.8.5 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.

11 Verwalten von Anwendungen

11.1 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:

- *Warnungsanwendung*
- *Analysis, Edition für OLAP*
- *Analysis Office Runtime*
- *Berechtigungsserver-Konfiguration*
- *BEx Web Applications*
- *BI Administration Cockpit*
- *BI-Launchpad*
- *BI-Arbeitsbereiche*
- *Central Management Console*
- *Collaboration*
- *BI-Kommentaranwendung*
- *Crystal Reports-Konfiguration*
- *HANA-Authentifizierung*
- *Information-Design-Tool*
- *Information-Steward-Anwendung*
- *BI Admin Studio*
- *Multitenancy-Management-Tool*
- *OpenDocument*
- *Anwendung zur Plattformsuche*
- *Hochstufverwaltung*
- *Papierkorb-Anwendung*
- *RESTful-Webdienst*
- *SAP BusinessObjects Mobile*
- *SAP Analytics Cloud*
- *Übersetzungsmanagement-Tool*
- *Universe-Design-Tool*
- *Versionsverwaltung*
- *Versionsverwaltung*

- *Grafischer Vergleich*
- *Web Intelligence*
- *Webdienst*
- *Workflow-Assistent*

11.2 Allgemeine Einstellungen

11.2.1 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*.

11.2.2 Protokollierungsebene der Ablaufverfolgung der Webanwendung in der CMC einstellen

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: Fiorisiertes BI-Launchpad, CMC, OpenDocument, 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*.
4. Starten Sie den Webanwendungsserver neu.

Die neue Ablaufverfolgungsprotokollierungsebene wird nach der nächsten Anmeldung an der Webanwendung wirksam.

Weitere Informationen

Ablaufverfolgungsprotokollierungsebenen [Seite 193]

11.2.2.1 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.
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.

11.3 Anwendungseinstellungen

11.3.1 Verwalten des CMC-Registerkartenzugriffs

11.3.1.1 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.

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 196]
Verwalten von Rechten zur Konfiguration des Zugriffs auf die Registerkarte "CMC" für andere Benutzer oder Benutzergruppen [Seite 198]

11.3.1.2 Arbeiten mit dem CMC-Registerkartenzugriff

11.3.1.2.1 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*
    - *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.

11.3.1.2.1.1 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*.

   > ⓘ 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 199]

11.3.1.2.1.2 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 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.

11.3.1.2.1.3 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.

11.3.1.2.1.4 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.

Weitere Informationen

Delegierte(r) Verwaltung und Zugriff auf CMC-Registerkarten [Seite 193]
Übernahme des Zugriffs auf eine CMC-Registerkarte [Seite 196]

11.3.1.2.1.5 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*.

11.3.1.2.2 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 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 200]

11.3.1.2.3 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.
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 196]
Übernahme des Zugriffs auf eine CMC-Registerkarte [Seite 196]

11.3.2 Verwalten der BI-Launchpad-Einstellungen

In diesem Abschnitt wird erläutert, wie Sie im BI-Launchpad die folgenden Einstellungen vornehmen können:

- Ändern der Anzeigeeinstellungen für das BI-Launchpad
- Konfigurieren von Details der RESTful-URL in der Central Management Console für die Anmeldung am BI-Launchpad
- Einrichten der Registerkarte "Authentifizierung" und der CMS-Sichtbarkeit im BI-Launchpad
- Konfigurieren einer E-Mail-Verknüpfung für die Option *Administrator kontaktieren* im BI-Launchpad

11.3.2.1 Anzeigeeinstellungen des BI-Launchpad ändern

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

11.3.2.2 Details der RESTful-URL in der CMC für die Anmeldung am fiorisierten BI-Launchpad konfigurieren

Nachdem Sie BI 4.2 SP4 installiert bzw. ein Upgrade darauf durchgeführt haben, müssen Sie eine URL für RESTful Web-Services konfigurieren, damit sich Benutzer am fiorisierten BI-Launchpad anmelden können.

Um URL-Details für RESTful Web-Services in der CMC zu konfigurieren, führen Sie die folgenden Schritte durch:

1. Melden Sie sich als Administrator bei der CMC an.
2. Navigieren Sie zu *Verwalten* > *Anwendungen* > *RESTful Web-Services* > *Eigenschaften*.
3. Geben Sie die WACS-URL an (Hostname oder vollständig qualifizierter Name, unter dem der WACS-Server installiert ist).

11.3.2.3 Registerkarte "Authentifizierung" und CMS-Sichtbarkeit im fiorisierten BI-Launchpad einrichten

Um die Registerkarte "Authentifizierung" und die CMS-Sichtbarkeit im fiorisierten BI-Launchpad einzurichten, führen Sie folgende Schritte aus:

1. Navigieren Sie zu `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Wenn Sie die mit der BI-Plattform installierte Tomcat-Version verwenden, können Sie auch auf folgenden Speicherort zugreifen: `C:\Programme (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEBINF\config\custom`.
2. Erstellen Sie mit dem Notepad eine neue Datei, und speichern Sie diese unter folgendem Namen: "FioriBI.properties".
3. Fügen Sie Folgendes hinzu, um die Authentifizierungsoptionen auf dem Anmeldebildschirm von BI-Launchpad einzubeziehen: `authentication.visible=true`.

   Ersetzen Sie <Authentifizierung> durch die Standardauthentifizierungstypen: "secEnterprise, secLDAP, secWinAD, secSAPR3".
4. Fügen Sie Folgendes hinzu, um den Standardauthentifizierungstyp zu ändern: `authentication.default=<authentication>`.
5. Geben Sie Folgendes ein, um Benutzer zur Eingabe des CMS-Namens auf dem Anmeldebildschirm von BI-Launchpad aufzufordern: `cms.visible=true`.
6. Speichern und schließen Sie die Datei.
7. Starten Sie Ihren Webanwendungsserver neu.

11.3.2.4 E-Mail-Verknüpfung für die Option "Administrator kontaktieren" im fiorisierten BI-Launchpad konfigurieren

Um eine E-Mail-Verknüpfung für die Option *Administrator kontaktieren* im fiorisierten BI-Launchpad zu konfigurieren, führen Sie die folgenden Schritte durch:

1. Navigieren Sie zu `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Wenn Sie die mit der BI-Plattform installierte Tomcat-Version verwenden, können Sie auch auf folgenden Speicherort zugreifen: `C:\Programme (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEBINF\config\custom`.
2. Erstellen Sie mit dem Notepad eine neue Datei, und speichern Sie diese unter folgendem Namen: "FioriBI.properties".
3. Ändern Sie in der Datei die Eigenschaft `admin.user.email=administrator@bilp.com`, um die E-Mail-ID des Administrators einzuschließen.

11.3.3 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.

11.3.3.1 Ändern der Anzeigeeinstellungen in Web Intelligence

1. Wechseln Sie zum Bereich *Anwendungen* der CMC, und wählen Sie *Web Intelligence*.
2. Wählen Sie *Verwalten* > *Eigenschaften*.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
3. Legen Sie eine der folgenden Anzeigeoptionen fest:

Option	Beschreibung
Anzeigeoptionen für geänderte Daten > *Dimensionen und Details*	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.
Anzeigeoptionen für geänderte Daten > *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 maximale Größe eingebetteter Bilder ein.
Unterstützung für geografische Karten:	Unterstützung geografischer Karten in Web Intelligence aktivieren oder deaktivieren.

Option	Beschreibung
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 schließen.
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. • 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. • 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.
JavaScript	Ihre Auswahl hier legt fest, wie Zellen mit den Attributen "Inhalt lesen als: HTML" und "Inhalt lesen als: Hyperlink" in Web-Intelligence-Dokumenten gerendert werden. • *JavaScript deaktivieren und Hyperlinks und ausschließlich von Web Intelligence verwendete HTML-Elemente aktivieren* Mit der Standardoption werden Hyperlinks und eine eingeschränkte Menge von für Web-Intelligence-Funktionen erforderlichen HTML-Elementen aktiviert. Sie entfernt JavaScript und alle weiteren HTML-Elemente aus den Dokumenten.

Option	Beschreibung
	• *Nur HTML-Elemente aktivieren, die auf der Seite mit autorisierten HTML-Elementen definiert sind* Mit dieser Option werden nur die HTML-Elemente und -Attribute aktiviert, die Sie auf der Seite *Autorisierte HTML-Elemente* definiert haben. • *JavaScript, HTML-Elemente und Hyperlinks aktivieren* Mit dieser Option werden alle JavaScript- und HTML-Elemente sowie Hyperlinks aktiviert. Wenn Sie diese Option ändern, müssen Sie sich von der Anwendung ab- und wieder anmelden, um die Änderungen in Web Intelligence anzuzeigen. ⚠ Achtung • Mit Web Intelligence können Sie dank dessen Formelfunktionen eingebetteten JavaScript-/HTML-Code in Dokumentzellen verwenden. Dieser Code kann in der Central Management Console aktiviert oder deaktiviert werden. Durch die Autorisierung von JavaScript, HTML-Dateien und Hyperlinks erkennen Sie jedoch das Risiko an, dass Sie sich Cross-Site-Scripting aussetzen. Cross-Site-Scripting ermöglicht es Angreifern, Websites zu ändern oder Code auf anderen Systemen auszuführen. Diese Schwachstelle betrifft Produkte wie Internetbrowser, wenn sie Skripte ausführen. Die Mehrzahl der Cross-Site-Scripting-Angriffe resultiert aus nicht sicherer Programmierung auf dem Zielsystem. • Der Code kann angepasst werden, indem HTML-Tags und Attribute in *BI-Admin-Studio* > *Anwendungen* > *HTML-Elemente* > autorisiert werden. Für die Kompatibilität dieses Codes und seine möglichen Auswirkungen übernimmt SAP jedoch keine Verantwortung. Beispielsweise erfordert Ihr Code möglicherweise Anpassungen infolge von Browser-Aktualisierungen, der Unterstützung von JavaScript-Versionen oder der dynamischen Einbettung von Code in die Webseite. Der Code erfordert möglicherweise Anpassungen, um in diesem neuen Kontext ausgeführt werden zu können.
Inhaltsanpassung für neue Dokumente	Verwenden Sie diese Optionen, um festzulegen, ob der Inhalt des neuen Dokuments von rechts nach links oder von links nach rechts ausgerichtet werden soll oder ob er vom bevorzugten Anzeigegebietsschema und/oder Produktgebietsschema des Benutzers abhängen soll.
Funktionsumschalttasten	Verwenden Sie dieses Textfeld zur Eingabe von Umschalttasten, um Vorschaufunktionen zu aktivieren. Diese Umschalttasten können auch in SAP-Hinweisen verwendet werden, um das Standardverhalten zu ändern. Diese Liste der Umschalttasten muss als Liste im JSON-Format eingegeben werden.

4. Klicken Sie auf *Speichern und schließen*.

> **Hinweis**
>
> Um mit Ihrer Auswahl zu den standardmäßigen Anzeigevariablen zurückzukehren, klicken Sie auf *Zurücksetzen*.

11.3.4 Verwalten von Einstellungen für Crystal Reports

- Sie können steuern, auf welche Funktionen Ihre Benutzer bei Crystal-Reports-Dokumenten Zugriff haben, indem Sie Eigenschaften für die Crystal-Reports-Anwendung festlegen.
- Wechseln Sie in der CMC zu *Anwendungen*.
- Wählen Sie *Crystal-Reports-Konfiguration*.
- Klicken Sie auf *Eigenschaften verwalten*.
  Das Dialogfeld *Eigenschaften* wird angezeigt.
- Klicken Sie auf *Verschiedene Einstellungen*.
- Legen Sie eine der folgenden Anzeigeoptionen fest:
  - *SmartView*: zeigt standardmäßig die letzte Instanz (sofern verfügbar) oder den Bericht selbst an
  - *Support für geografische Karten*: geografische Karten in Crystal Reports aktivieren oder deaktivieren

11.3.5 Verwalten von Central Management Console-Einstellungen

Im Bereich *Anwendungen* der CMC in der BI-Plattform können Sie die Anzeigeoptionen der Central Management Console über *Verwalten* > *Eigenschaften* ändern.

Für die Central Management Console können Sie Folgendes konfigurieren:

- Verarbeitungserweiterungen
- Verarbeitungseinstellungen
- Programmobjektrechte

11.3.5.1 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.

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 erteilen. 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.

> **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`

11.3.5.1.1 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 *Skripte/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*.

> **Hinweis**
>
> Wenn Sie ein Upgrade auf SAP BusinessObjects Business Intelligence 4.3 Support Package 3 durchführen, werden Programmobjektrechte standardmäßig für alle verweigert. Ein Administratorbenutzer (oder ein beliebiger Benutzer in der Administratorgruppe) kann dies aktivieren.
>
> Unter *Java-Programme ausführen* befindet sich das Kontrollkästchen *Identitätsmaskierung verwenden*. In 4.3 Support Package 3 ist das Kontrollkästchen *Identitätsmaskierung verwenden* entfernt.

11.3.5.2 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\win64_x64\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:

- 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.

11.3.5.2.1 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.

11.3.6 Verwalten der Einstellungen der BI-Kommentaranwendung

Bei BI-Kommentar handelt es sich um eine in der CMC eingeführte Anwendung. Mit ihr können die Benutzer eines bestimmten Dokuments zusammenarbeiten, indem sie die darin verfügbaren Daten/Statistiken kommentieren.

BI-Kommentar erlaubt es Benutzern, Kommentare zu in Berichten enthaltenen Daten/Statistiken zu posten.

→ Empfehlung

Standardmäßig erstellt und wartet BI-Kommentar zwar eigene Tabellen in der Audit-Datenbank.

> ⓘ Hinweis
>
> Um BI-Kommentar mit der Audit-Datenbank auf einer anderen Plattform als Windows zu verwenden, lesen Sie bitte im Datenzugriffshandbuch nach, wie die ODBC-Treiber zu konfigurieren sind.

Dennoch empfiehlt SAP das Konfigurieren einer neuen Datenbank, um Kommentare, die über die BI-Kommentaranwendung erstellt wurden, zu speichern. Die Datenbanken, die BI-Kommentar unterstützen, sind dieselben, die Auditing unterstützen. Die unterstützten Datenbanken und die entsprechenden zertifizierten JDBC-JAR-Dateien für BI-Kommentar umfassen:

- IBM DB2 Workgroup Edition – db2jcc4.jar
- Microsoft SQL Server – sqljdbc4.jar
- MySQL – com.mysql.jdbc_5.1.5.jar
- Oracle – ojdbc6.jar
- SAP HANA – ngdbc.jar
- Sybase Adaptive Server Enterprise – jconn4.jar
- Sybase SQL Anywhere – jconn4.jar

> ⓘ Hinweis
>
> Unabhängig davon, ob Sie BI-Kommentar mit der Audit-Datenbank oder einer anderen unterstützten Datenbank konfigurieren, müssen Sie "MySQL jdbc jar" im Ordner "jdbc" unter folgendem Verzeichnis ablegen, damit BI-Kommentar mit der MySQL-Datenbank funktioniert: `<INSTALLVERZ\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.
>
> Wenn Sie BI-Kommentar mit IBM DB2 konfigurieren, benötigt das System eine temporäre Tablespace-Seitengröße von 8 K, 16 K bzw. 32 K. Der Standardwert für die Seitengröße ist 4K.

> **Hinweis**
>
> Ist die Audit-Datenbank standardmäßig nicht konfiguriert/aktiviert, funktioniert BI-Kommentar nur, wenn Sie manuell eine neue Datenbank für BI-Kommentar konfigurieren.
>
> Wenn Sie BI-Kommentar mit Audit-Datenbanken konfigurieren und die Audit-Datenbank löschen, werden alle in der Audit-Datenbank gespeicherten Kommentare ebenfalls gelöscht.
>
> Die Audit-Datenbank verwendet entweder ODBC oder systemeigene Datenbanktreiber. Sie benötigen einen JDBC-Treiber, um eine Kommentar-Datenbank zu konfigurieren.

> **Hinweis**
>
> Die Größe eines Kommentars ist auf 2.000 UTF-8-Zeichenbyte oder 666 UTF-16-Zeichenbyte beschränkt.

> **Hinweis**
>
> Sie können Kommentare nicht mit dem Föderations-Tool migrieren.

> **Hinweis**
>
> BI-Kommentar wird für MaxDB-Verbindungen nicht unterstützt.

> **Hinweis**
>
> Um vom Benutzer vorgenommene Kommentareinträge zu löschen, verwenden Sie die folgende Abfrage:
>
> ```
> DELETE from dba.COMMENTARY_MASTER where UserName ='<User Name>'
> ```

11.3.6.1 Konfigurieren einer neuen BI-Kommentardatenbank

Sie haben eine JDBC-Verbindung eingerichtet.

> **Hinweis**
>
> Nachdem Sie eine neue BI-Kommentar-Datenbank konfiguriert haben, ist der vom Adaptive Processing Server bereitgestellte Kommentardienst für das Schreiben von Kommentaren in die Datenbank zuständig. Die folgende Schritte müssen auf jedem Computer im Cluster ausgeführt werden, auf dem der Kommentardienst ausgeführt wird.

Um eine neue JDBC-Verbindung einzurichten, führen Sie folgende Schritte aus:

1. Legen Sie die JAR-Datei mit dem JDBC-Treiber für die Datenbank, die Sie konfigurieren möchten, am folgenden Speicherort ab. `<INSTALLVERZ\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

   > **Hinweis**
   >
   > Wenn Sie ein Upgrade auf SAP BusinessObjects Business Intelligence 4.2 Support Package 2 durchführen und bereits in einer Vorgängerversion eine neue Datenbank für BI-Kommentar konfiguriert

haben, müssen Sie die Datenbanktreiberdatei aus dem Ordner "jdbc" in `<INSTALLVERZ\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib\external>` nach `<INSTALLVERZ\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>` verschieben.

2. Starten Sie den SIA neu.

Um eine neue Datenbank für BI-Kommentar zu konfigurieren, gehen Sie wie folgt vor:

1. Melden Sie sich bei der CMC an.
2. Wählen Sie auf der CMC-Startseite die Option *Anwendungen* aus dem Dropdown-Menü.
3. Wählen Sie aus der Liste *Anwendungsname* die Option *BI-Kommentaranwendung*.

   Das Popupfenster *BI-Kommentar* wird angezeigt. Standardmäßig ist das Optionsfeld *Audit-Datenbank verwenden* ausgewählt.
4. Wählen Sie das Optionsfeld *Use other supported database* (Andere unterstützte Datenbank verwenden) aus.
5. Geben Sie den *Typ*, *Datenbanknamen*, *Host*, *Port*, *Benutzernamen* und das *Kennwort* im Bereich *Configure Commentary Database* (Kommentardatenbank konfigurieren) ein.
6. Wählen Sie *Speichern & schließen*.
7. Starten Sie den APS neu.

   Änderungen an der Konfiguration der BI-Kommentardatenbank werden erst dann wirksam, wenn Sie den Adaptive Processing Server (APS) neu starten.

   Mithilfe von *Verbindung testen* können Sie Ihre Verbindung prüfen.

   > **Hinweis**
   >
   > Wenn Sie ein Upgrade auf SAP BusinessObjects Business Intelligence 4.3 Support Package 3 vornehmen und bereits eine Datenbank für BI-Kommentar für JDBC aus den früheren Versionen konfiguriert hatten, wird bei Auswahl von *Verbindung testen*, *Speichern und schließen* oder *Speichern* nun ein leeres Kennwortfeld angezeigt.

   Sie können ältere Kommentare löschen oder bereinigen, indem Sie das Kontrollkästchen *Alle Kommentare löschen, die älter sind als* aktivieren und die Anzahl von Tagen festlegen.

   > **Hinweis**
   >
   > Sie müssen alle APS-Server neu starten, die den BI-Kommentardienst hosten, damit die Änderungen wirksam werden.

Sie haben nun eine neue Datenbank zur Speicherung von Kommentaren aus der BI-Kommentaranwendung heraus konfiguriert.

11.3.7 Verwalten der Papierkorbeinstellungen

Papierkorb

Der Papierkorb ist eine neue Anwendung in der CMC. Löscht der Benutzer ein Element aus dem BOE-System, wird dieses in den Papierkorb verschoben. Dort wird es bis zum Leeren des Papierkorbs temporär gespeichert, Dies bietet dem Benutzer die Möglichkeit, versehentlich gelöschte Berichte/Ordner an ihrem ursprünglichen Speicherorten wiederherzustellen.

Mit der Papierkorb-Anwendung kann der Administrator:

- die Wiederherstellung jedes gelöschten Elements (z. B. Berichte und Ordner) initiieren
- Elemente aus dem Papierkorb dauerhaft löschen
- ein automatisches Cleanup für den Papierkorb durchführen

Ausschließlich Elemente im öffentlichen Ordner können temporär im Papierkorb gespeichert werden.

11.3.7.1 Wiederherstellen eines Elements aus dem Papierkorb

Der Papierkorb zeigt eine Liste der gelöschten Elemente an. Um ein Element aus dem Papierkorb wiederherzustellen, gehen Sie wie folgt vor:

1. Melden Sie sich bei der CMC an.
2. Wählen Sie auf der CMC-Startseite im Bereich *Verwalten* den *Papierkorb*.
3. Klicken Sie mit der rechten Maustaste auf das Element, das Sie wiederherstellen wollen, und wählen im Kontextmenü den Befehl *Wiederherstellen*.
4. Wählen Sie *OK*.

   Sie können zum Speicherort des wiederhergestellten Elements navigieren, um sicherzustellen, dass die Wiederherstellung erfolgreich war.

   > ⓘ Hinweis
   >
   > Wenn Sie ein Element aus dem Papierkorb wiederherstellen, an dessen Wiederherstellungsort bereits ein anderes Element mit demselben Namen vorhanden ist, wird das wiederhergestellte Element an diesem Ort unter folgendem Namen gespeichert: "<Elementname> wiederhergestellt(1, 2, ...)".
   >
   > Wenn der übergeordnete Ordner eines aus dem Papierkorb wiederhergestellten Elements gelöscht wurde, wird er im Zuge der Wiederherstellung neu erstellt. Allerdings enthält der übergeordnete Ordner dann nur die Elemente, die aus dem Papierkorb wiederhergestellt wurden.
   >
   > Ein im Papierkorb befindliches Element lässt sich nicht öffnen/ansteuern.

Sie haben erfolgreich ein Element aus dem Papierkorb wiederhergestellt.

11.3.7.2 Dauerhaftes Löschen von Elementen aus dem Papierkorb

Als Administrator sind Sie berechtigt, ausgewählte Elemente dauerhaft aus dem Papierkorb zu löschen oder den Papierkorb zu leeren.

Um ein Element dauerhaft aus dem Papierkorb zu löschen, gehen Sie wie folgt vor:

1. Melden Sie sich bei der CMC an.
2. Wählen Sie auf der CMC-Startseite im Bereich *Verwalten* den *Papierkorb*.
3. Klicken Sie mit der rechten Maustaste auf das Element, das Sie löschen wollen, und wählen im Kontextmenü den Befehl *Löschen*.
4. Wählen Sie *OK*.

Sie haben erfolgreich ein Element aus dem Papierkorb gelöscht.

Leeren des Papierkorbs

Um den Papierkorb zu leeren, gehen Sie wie folgt vor:

1. Melden Sie sich bei der CMC an.
2. Wählen Sie auf der CMC-Startseite im Bereich *Verwalten* den *Papierkorb*.
3. Wählen Sie *Papierkorb leeren*.

Sie haben den Papierkorb erfolgreich geleert.

11.3.7.3 Aktivieren des automatischen Cleanup für den Papierkorb

Sie können den Papierkorb einem regelmäßigen automatischen Cleanup unterziehen.

Um das automatische Cleanup des Papierkorbs zu aktivieren, gehen Sie wie folgt vor:

1. Melden Sie sich bei der CMC an.
2. Wählen Sie auf der CMC-Startseite im Bereich *Verwalten* den *Papierkorb*.
3. Wählen Sie im Dialogfeld *Papierkorb* die Option *Eigenschaften*.

   Das Dialogfeld *Properties*:*Recycle Bin* (Eigenschaften: Papierkorb) wird geöffnet.
4. Aktivieren Sie das Kontrollkästchen und geben Sie (in Tagen) an, wie lange das System bis zur automatischen Bereinigung eines gelöschten Elements warten soll.
5. Wählen Sie *OK*.

Sie haben das automatische Cleanup für den Papierkorb erfolgreich aktiviert.

11.3.8 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 192]

11.3.8.1 Ändern der Standardeigenschaften von Warnmeldungen

1. Wechseln Sie in den Bereich *Anwendungen* der CMC, und wählen Sie *Warnungsanwendung* aus.
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 215]

11.3.8.2 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.
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 und keinen E-Mail-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 192]
Verwalten von Warnmeldungseinstellungen [Seite 215]

11.3.9 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.

11.3.10 Verwalten von Einstellungen für SAP BusinessObjects Mobile

Sie können für SAP BusinessObjects Mobile festlegen, auf welche Funktionen Benutzer Zugriff haben, indem Sie die zugehörigen Einstellungen und Sicherheitsberechtigungen im Bereich "Anwendungen" der CMC festlegen.

11.3.10.1 Modifizieren der standardmäßigen mobilen Eigenschaften für SAP BusinessObjects Mobile

1. Wechseln Sie zum Bereich *Anwendungen* der CMC.
2. Wählen Sie *SAP BusinessObjects Mobile*, und klicken Sie mit der rechten Maustaste auf diese Anwendung.
3. Wählen Sie *Eigenschaften*.
4. Legen Sie in den *mobilen Eigenschaften* die entsprechenden Werte für folgende Eigenschaften fest:

Eigenschaft	Standardwerte	Beschreibung	Mögliche Werte
`default.corporateCategory`	'Mobile'	Geben Sie einen Namen für die Unternehmenskategorie ein. Dieser Kategorie zugeordnete Dokumente sind Mobile-geeignete Dokumente. Mobile-	Eine vom Administrator ausgewählte spezifische Unternehmenskategorie.

Eigenschaft	Standardwerte	Beschreibung	Mögliche Werte
		Benutzer können mit einer Anwendung von SAP BusinessObjects Mobile auf einem mobilen Gerät (z.B. Blackberry, Android und iOS) auf die BI-Dokumente zugreifen, die dieser Kategorie zugewiesen sind. Geben Sie bei mehreren Kategorienamen die Werte durch Kommas getrennt an. **Hinweis** Für den hier angegebenen Wert wird Groß- und Kleinschreibung berücksichtigt.	
`default.personalCategory`	'Mobile'	Geben Sie einen Namen für die persönliche Kategorie ein. Dieser Kategorie sind persönliche Dokumente des Benutzers zugewiesen, auf die andere mobile Benutzer keinen Zugriff haben. Geben Sie bei mehreren Kategorienamen die Werte durch Kommas getrennt an. **Hinweis** Für den hier angegebenen Wert wird Groß- und Kleinschreibung berücksichtigt.	Eine vom Administrator ausgewählte persönliche Kategorie.
`default.category.mobiledesigned`	'MobileDesigned'	Geben Sie einen Namen für die Kategorie mit mobilem Design ein. Dieser Kategorie zugewiesene Dokumente erscheinen im Seitenlayout-Modus, wenn die Benutzer sie auf dem	Eine vom Administrator ausgewählte persönliche Kategorie.

Eigenschaft	Standardwerte	Beschreibung	Mögliche Werte
		mobilen Gerät anzeigen. Geben Sie bei mehreren Kategorienamen die Werte durch Kommas getrennt an. **Hinweis** Für den hier angegebenen Wert wird Groß- und Kleinschreibung berücksichtigt.	
`default.category.secure`	'Confidential'	Geben Sie einen Namen für die sichere Kategorie ein. Dieser Kategorie zugewiesene Dokumente können von den Benutzern nur im Online-Modus angezeigt werden. Die Benutzer können diese Dokumente nicht herunterladen oder als lokale Kopie speichern. Wenn mehrere Kategorienamen vorhanden sind, geben Sie die Werte durch Komma getrennt ein. **Hinweis** Für den hier angegebenen Wert wird Groß- und Kleinschreibung berücksichtigt.	Eine vom Administrator ausgewählte persönliche Kategorie.
`default.category.featured`	'Featured'	Der Wert für diese Eigenschaft wird derzeit in der SAP-BI-Anwendung nicht genutzt.	
`default.imageSize`	'1048576 bytes'	Geben Sie die maximale Bildgröße an, die in der SAP BI-Anwendung auf dem mobilen Gerät angezeigt wird.	Beliebiger numerischer Wert

Eigenschaft	Standardwerte	Beschreibung	Mögliche Werte
`default.save.maxPages`	20	Geben Sie die Anzahl der pro Seite auf dem mobilen Gerät anzuzeigenden Suchergebnisse an.	Beliebiger numerischer Wert

5. (Optional) Um eine Eigenschaft hinzuzufügen, wählen Sie *+ Weitere hinzufügen ...* und geben die Eigenschaftendetails ein.
6. (Optional) Um eine oder mehrere Eigenschaften zu löschen, aktivieren Sie das Kontrollkästchen der entsprechenden Eigenschaft.
7. Klicken Sie auf *Speichern und schließen*.

11.3.10.2 Modifizieren der standardmäßigen Client-Einstellungen für SAP BusinessObjects Mobile

1. Wechseln Sie zum Bereich *Anwendungen* der CMC.
2. Wählen Sie *SAP BusinessObjects Mobile*, und klicken Sie mit der rechten Maustaste auf diese Anwendung.
3. Wählen Sie *Eigenschaften > Client-Einstellungen*.
4. Legen Sie in den *Client-Einstellungen* die entsprechenden Werte für folgende Eigenschaften fest:

Eigenschaft	Standardwerte	Beschreibung	Mögliche Werte
`savePassword`	'false'	Ermöglicht es dem Mobile-Benutzer, das Kennwort in der Client-Anwendung zu speichern, während die Verbindung hergestellt wird. Durch Auswahl dieser Option muss der Benutzer das Kennwort nicht bei jeder Anmeldung bei der Anwendung eingeben. Um die Option zum Speichern des Kennworts in der Client-Anwendung zu aktivieren, legen Sie den Wert auf "True" fest.	True oder False
`offlineStorage`	'false'	Ermöglicht es dem Mobile-Benutzer, eine lokale Kopie des Dokuments auf dem mobilen Gerät zu speichern.	True oder False

Eigenschaft	Standardwerte	Beschreibung	Mögliche Werte
		Damit der Benutzer eine lokale Kopie des Dokuments speichern kann, legen Sie den Wert auf "True" fest.	
`offlineStorage.ttl`	'365'	Angabe der maximalen Anzahl von Tagen, nach denen das Dokument auf dem Server abläuft.	Beliebiger numerischer Wert
`offlineStorage.appPwd`	'true'	Ermöglicht es dem Mobile-Benutzer, während der Verbindungserstellung Anwendungskennwörter einzugeben. Um die Option für Anwendungskennwörter zu aktivieren, legen Sie den Wert auf "True" fest.	True oder False

5. (Optional) Um eine Eigenschaft hinzuzufügen, wählen Sie *+ Weitere hinzufügen ...* und geben die Eigenschaftendetails ein.
6. (Optional) Um eine oder mehrere Eigenschaften zu löschen, aktivieren Sie das Kontrollkästchen der entsprechenden Eigenschaft.
7. Klicken Sie auf *Speichern und schließen*.

11.3.11 Verwalten des Push-Benachrichtigungsdienstes in SAP BusinessObjects Mobile

Der SAP BusinessObjects Mobile Server leitet Benachrichtigungen an iOS-Geräte der Benutzer von SAP-BusinessObjects-Mobile-Anwendungen weiter. Benachrichtigungen werden in den folgenden Szenarios weitergeleitet:

- Wenn für auf ein Benutzergerät geladene BI-Dokumente ein Update oder eine neue Instanz auf dem Server verfügbar ist
- Wenn im BI-Posteingang des Benutzers ein neues Dokument verfügbar ist
- Wenn die BI-Plattform oder der BOE-Administrator eine Meldung sendet

Der Mobile Server leitet die Benachrichtigungen automatisch über den Apple Push Notification Server (APNS) an das Gerät weiter. Der Benutzer muss nicht mit dem Server verbunden sein, um Push-Benachrichtigungen zu empfangen. Der Benutzer kann auch dann Push-Benachrichtigungen empfangen, wenn die Anwendung nicht im System läuft. In der Anwendung müssen die "Benachrichtigungseinstellungen“ aktiviert sein. Weitere Information zur Konfiguration von Push-Benachrichtigungen finden Sie im *Handbuch zur Implementierung und Konfiguration des Mobile-Servers* für Mobile Server 4.2.

> **Hinweis**
>
> Um Push-Benachrichtigungen in Mobile aktivieren zu können, muss BIMobileService im APS laufen.
>
> Da der BIMobileService nur wenig Speicherplatz benötigt, können Sie Ihn im APS zusammen mit anderen Diensten ausführen.

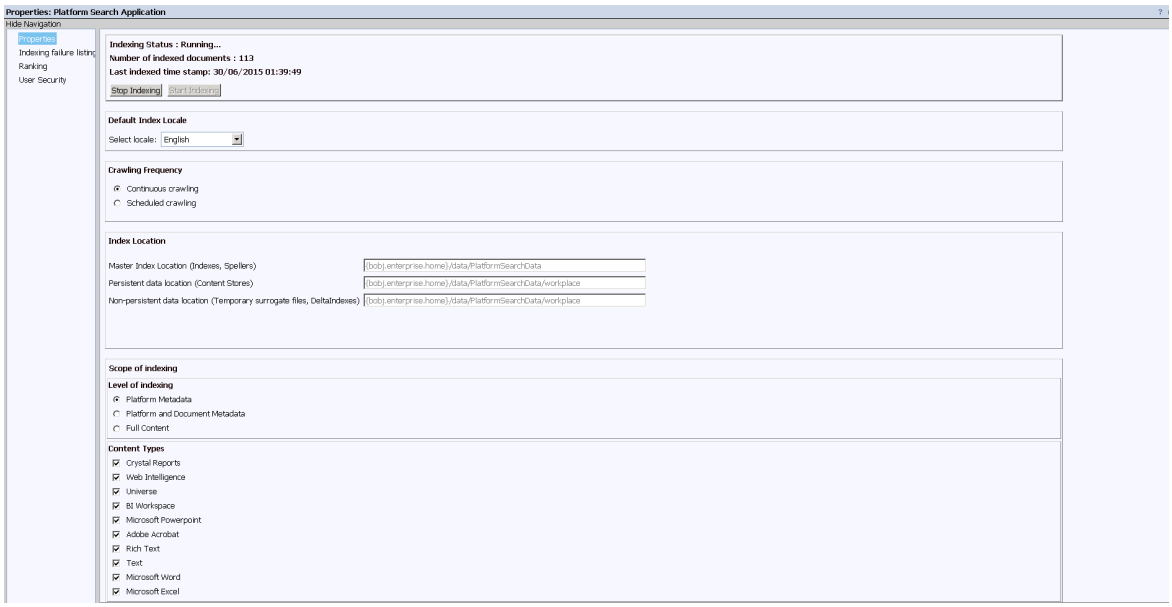
11.3.12 Verwalten der Einstellungen für die Plattformsuche

Im Bereich *Anwendungen* der CMC in der BI-Plattform können Sie für die Plattformsuchanwendung Einstellungen auf Systemebene festlegen.

11.3.12.1 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. 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 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.

Option	Beschreibung
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. **Hinweis** • Der Speicherort des Hauptindex muss 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. • In den Indexdateien können personenbezogene und vertrauliche Informationen gespeichert sein, insbesondere wenn Sie Dokumentinhalte indizieren. Sie dürfen nur Systembenutzern erlauben, auf die freigegebenen Ordner zuzugreifen, und Sie sollten die freigegebenen Ordner in einer verschlüsselten Umgebung speichern, um Datendiebstahl zu verhindern.

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. Als Standard ist die Option aktiviert.
	• 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
	Bei Analysis-Office- und Lumira-Dokumenten wird die Indizierung nicht für den gesamten Inhalt unterstützt. Bei Analysis-Office- und Lumira-Dokumenten wird nur die Indizierung von Metadaten unterstützt.
	Hinweis
	Wenn Sie die Indizierungsebene ändern, wird die Indizierung für die Regenerierung des gesamten BI-Plattform-Repositorys initialisiert.

Option	Beschreibung
Inhaltstypen	Für die Indizierung stehen folgende Inhaltstypen zur Auswahl: • Crystal Reports • Web Intelligence • Universum • BI-Arbeitsbereich • Analysis Office • Lumira • Microsoft PowerPoint • Adobe Acrobat • Rich Text • Text • Microsoft Word • Microsoft Excel Der Inhaltstypenfilter ist nicht für die Indizierung von Plattform-Metadaten relevant. Unabhängig davon, welche Inhaltstypen Sie auswählen, erfolgt die Indizierung der Plattform-Metadaten für alle unterstützten Objekttypen, und die Suchergebnisse im BI-Launchpad geben alle Objekte für das mit den Plattform-Metadaten verbundene Schlüsselwort zurück. Der Inhaltstypenfilter ist für die Indizierung von Dokument-Metadaten (Dokumentautor, Dokumentkopf, Dokumentfuß usw.) und die Indizierung von Inhalten (Grafiken, Diagramme, Tabellen mit Berichten) relevant. Abhängig davon, welche Indizierungsebene und welche Inhaltstypen Sie auswählen, indiziert die Plattformsuche die Dokument-Metadaten und die Inhalte für die ausgewählten Objekttypen aus dem Repository, und bei der Suche nach einem mit Dokument-Metadaten und Inhalten verbundenen Stichwort werden nur diese Objekte in den BI-Launchpad-Suchergebnissen angezeigt.
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.

Option	Beschreibung
Von der Indizierung ausgeschlossene Dokumente	Die Option *Von der Indizierung ausgeschlossene Dokumente* schließt Dokumente von der Indizierung aus. Beispielsweise möchten Sie extrem große Crystal-Reports-Berichte von der Suche ausschließen, um die Report-Application-Server-Ressourcen nicht zu überlasten. Sie haben auch die Möglichkeit, Veröffentlichungen mit Hunderten von personalisierten Berichten zu 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
Weitere Konfiguration – Instanz überspringen	Standardmäßig werden Instanzen von Dokumenten für die Indizierung ausgewählt. Dies verursacht ein „Aufblähen“ der Indexgröße und somit einen erhöhten Speicherplatzverbrauch auf der Festplatte. Der Ordner "Lucene Index Engine" innerhalb des Ordners "PlatformSearchData" wächst aufgrund der Indizierung einer riesigen Menge von Instanzen im Repository auf eine enorme Größe an. Wenn im System Millionen von Dokumenten (oder mehr) vorliegen und zu vielen dieser Dokumente enorme Mengen an Instanzen vorhanden sind (zusammen mit in regelmäßigen Abständen erzeugten zeitgesteuerten Instanzen), wächst der Ordner "Lucene Index Engine" übermäßig stark an, selbst wenn als Indizierungsebene "Plattform-Metadaten" festgelegt ist. Mit der Funktion "Instanz überspringen" der Plattformsuche können Sie die Indizierung von Instanzen durch Aktivierung oder Deaktivierung des entsprechenden Kontrollkästchens unter "Weitere Konfiguration – Instanz überspringen" auf der Eigenschaftenseite der Plattformsuchanwendung der CMC steuern. **Hinweis** • Wenn Sie "Instanz überspringen" aktivieren bzw. deaktivieren, müssen Sie den Adaptive Processing Server der Plattformsuche neu starten. Diese Änderungen wirken sich auf alle Ebenen der Indizierung aus. • Wenn Sie "Instanz überspringen" ändern und die Änderungen auf alle vorhandenen Instanzen anwenden (d. h. alle Instanzen für die Indizierung auswählen) möchten, müssen Sie den Index neu erstellen.

Option	Beschreibung
Von der Indizierung ausgeschlossene Objekte	Die Option *Von der Indizierung ausgeschlossene Objekte* schließt Objekte von der Indizierung aus. Beispielsweise möchten Sie bestimmte Objekte von der Suche ausschließen, um die Report-Application-Server-Ressourcen nicht zu überlasten. Durch Ausschließen bestimmter Objekte können Sie den Zugriff auf diese Dokumente über die Plattformsuche verhindern. Wenn ein Objekt jedoch indiziert wurde, bevor es dieser Gruppe zugewiesen wurde, wird das Objekt ggf. in die Suche eingeschlossen. Damit sichergestellt ist, dass die Dokumente in der Gruppe *Von der Indizierung ausgeschlossene Objekte* nicht in die Suche eingeschlossen werden, müssen Sie den Index neu erstellen. Liste der Objekte, die von der Indizierung ausgeschlossen werden können: • CrystalReport • Webi • LCMJob • Universe • Excel • PDF • PowerPoint • RTF • Txt • Word • AFDashboardPage • ObjectPackage • QaaWS • Profile • Event • Discussions • InformationDesigner • MDAnalysis • Publication • Agnostic • Analytic • Hyperlink • Program • pQuery • DSL.MetaDataFile • Verknüpfung • DataDiscoveryAlbum • AO.Workbook • VISI.Story

Option	Beschreibung
	• VISI.Dataset • VISI.Lums • VISILums • User • UserGroup

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.

11.3.12.2 Liste der Indizierungsfehler

Die "Liste der Indizierungsfehler" enthält eine Auflistung der Dokumente, die nicht indiziert werden konnten. Die Plattformsuche bietet vier 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. Klicken Sie auf *Aktionen* > *Liste der Indizierungsfehler*.
   Das Dialogfeld *Plattformsuchanwendung*, 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.

11.3.13 Konfigurieren der BEx-Webintegration

BEx Web Applications sind webbasierte Anwendungen aus Business Explorer (BEx) von SAP 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.

   > → 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.

Weitere Informationen

Starten eines Servers für BEx Web Applications [Seite 231]
Starten eines eigenständigen Servers für BEx Web Applications [Seite 231]
Konfigurieren der Servereinstellungen [Seite 232]
Überprüfen der Verbindung zum BW-System [Seite 233]
Konfigurieren einer Verbindung zwischen BEx Web Application Designer und der BI-Plattform [Seite 233]

11.3.13.1 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.

11.3.13.2 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.

11.3.13.3 Konfigurieren der Servereinstellungen

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 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 234]

11.3.13.4 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.

> **ⓘ 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.

11.3.13.5 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 234]

11.3.13.5.1 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 232]

11.3.14 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.
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.

11.3.14.1 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 Hostnamen, die Portnummer, die Instanznummer und den Namen der Tenant-Datenbank.

      Sie benötigen diese Informationen in Schritt 2.
2. Konfigurieren Sie eine SAP-HANA-Verbindung in der BI-Plattform.
   a. Wechseln Sie zum 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. Wählen Sie einen *Verbindungstyp* aus.

      > **Hinweis**
      >
      > Wählen Sie *SAP HANA* für eine JDBC-Verbindung und *SAP HANA HTTP* für eine HTTP-Verbindung.

   d. Geben Sie die in Schritt 1 erfasste Portnummer, den Hostnamen, die Instanznummer und den Namen der Tenant-Datenbank ein.

e. Geben Sie im Feld *Eindeutige ID des Identitätsproviders* einen Wert ein, der für Ihre BI-Plattform-Implementierung verwendet wird.
f. Geben Sie den *Dienstprovider-Namen* ein.

> **Hinweis**
>
> Sie können die Konfiguration des SAP-HANA-Dienstprovider-Namen in der indexserver.ini unter `Authentication -> saml_service_provider_name` überprüfen. Sie können ferner den Wert für SAP HANA anpassen, indem Sie den folgenden Befehl eingeben: `ALTER SYSTEM ALTER CONFIGURATION ('indexserver.ini', 'SYSTEM') SET ('authentication', 'saml_service_provider_name') = 'DEV00' WITH RECONFIGURE;`. In diesem Befehl stellt "DEV00" den Dienstprovider-Namen dar, den Sie Ihren Wünschen entsprechend anpassen können. Es wird empfohlen, zur Benennung des Dienstproviders eine Kombination aus System-ID (z.B. DEV) und Instanznummer (z.B. 00) zu wählen.

g. Wählen Sie *Gesicherte Verbindung*.

> **Hinweis**
>
> Die Auswahl von *Gesicherte Verbindung* ist obligatorisch, wenn Sie eine gesicherte JDBC- oder HTTPS-Verbindung herstellen möchten.
>
> - Um eine HTTPS-Verbindung herzustellen, müssen Sie als *Verbindungstyp* die Option *SAP HANA HTTP* und anschließend *Gesicherte Verbindung* wählen.
> - Um eine gesicherte JDBC-Verbindung herzustellen, müssen Sie als *Verbindungstyp* die Option *SAP HANA* und anschließend *Gesicherte Verbindung* wählen.

h. Klicken Sie auf *Ausführen*.
Im Feld *Base64-Zertifikat des Identitätsproviders* wird ein Zertifikat erstellt.

3. Konfigurieren Sie Ihre SAP-HANA-Implementierung.
   a. Melden Sie sich am SAP-HANA-System an.
   b. Klappen Sie *SSL- und Trust-Konfiguration* auf, und wählen Sie *PSE-Verwaltung*.
   c. Wählen Sie die PSE-Datei aus der Dropdown-Liste unter *PSE verwalten* aus.
   d. Wählen Sie *Zertifikate importieren*.
   e. Fügen Sie das im vorhergehenden Schritt auf der BI-Plattform generierte Zertifikat ein.
   f. Wählen Sie *Importieren*.
   g. Starten Sie SAP HANA Studio.
   h. Klappen Sie in der Ansicht *Systeme* Ihr SAP-HANA-System auf. Weitere Informationen finden Sie im https://help.sap.com/viewer/1c837b3899834ddcbae140cc3e7c7bdd/1.0.11/en-US/bdbb7230bb571014b189d813e5861284.htmlSAP HANA One Administration Guide.
   i. Öffnen Sie (Sicherheitseditor) im Ordner "Sicherheit".
   j. Wählen Sie (SAML-Identity-Provider für Zertifikatdatei importieren).
   k. Wählen Sie Ihren Identitätsprovider aus der Liste *SAML-Identity-Provider* aus.
   l. Wählen Sie (implementieren).
   m. Navigieren Sie in der Ansicht *Systeme* zum SAP-HANA-Benutzer.
   n. Öffnen Sie den SAP-HANA-Benutzer im Bereich "Editoren".
   o. Markieren Sie auf der Registerkarte *Benutzer* die Option *SAML* als Authentifizierung, und wählen Sie anschließend *Konfigurieren*.

p. Wählen Sie im Assistenten *Externe SAML-Identitäten* die Option *Hinzufügen*.
q. Wählen Sie Ihren Identitätsprovider aus.
r. Wählen Sie "OK".
s. Wählen Sie Ihren Identitätsprovider aus, und geben Sie den Namen desjenigen Benutzers der BI-Plattform ein, der dem SAP-HANA-Benutzer zugeordnet ist.
t. Wählen Sie "OK".
u. Wählen Sie (implementieren).
v. Starten Sie das SAP-HANA-System neu.
   1. Öffnen Sie das Kontextmenü Ihres SAP-HANA-Systems.
   2. Wählen Sie *Konfiguration und Überwachung*.
   3. Wählen Sie *System neu starten*.

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.

      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.

11.3.14.2 Konfigurieren von SAP-HANA-HTTPS-Verbindungen

Um die SAP-HANA-HTTPS-Verbindung zu konfigurieren, müssen Sie dem TrustStore oder einem anderen Speicherort Ihrer Wahl den HANA-Server und das CA-Zertifikat des HANA-Servers hinzufügen.

> **Hinweis**
>
> Sie müssen das Zertifikat des SAP-HANA-Servers aus dem SAP-HANA-System exportieren, bevor Sie das Zertifikat dem TrustStore oder einem anderen Speicherort hinzufügen.

Hinzufügen von Zertifikaten zum TrustStore

1. Navigieren Sie zum Verzeichnis `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.
2. Führen Sie den folgenden Befehl aus: `..\..\bin\keytool -importcert -file "<absolute path of the certificate>" -alias CertifcateAliasName -keystore cacerts -storepass changeit`.
3. Der HANA-Server und das CA-Zertifikat des HANA-Servers werden im TrustStore hinterlegt.

> **Hinweis**
>
> Wenn sich die Keystore-Datei am Standardspeicherort `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security` befindet, gehen die Änderungen an der Keystore-Datei bei einem Upgrade von SAP Business Intelligence Platform Support Package 4 auf Support Package 5 verloren. Es wird daher empfohlen, das Zertifikat an einem anderen Speicherort hinzuzufügen.

Hinzufügen von Zertifikaten zu anderen Speicherorten

1. Navigieren Sie zum Verzeichnis `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`.
2. Führen Sie den folgenden Befehl aus: `keytool -importcert -file "C:\certificate\HANASERVERCertificate " -alias CertificateAliasName -keystore C:\certificate\cacerts -storepass changeit`.

   > **Hinweis**
   >
   > Der oben angegebene Speicherort dient nur als Beispiel. Sie können den Speicherort Ihren Wünschen entsprechend anpassen.

3. Damit der APS-Server den Dateispeicherort ermitteln kann, führen Sie den folgenden Befehl aus:

   ```
   -Djavax.net.ssl.trustStore= cacerts_PATH
   -Djavax.net.ssl.trustStorePassword= Password
   ```

   > **Hinweis**
   >
   > Die Angaben "cacerts_PATH" und "Password" dienen nur als Beispiel für den Keystore bzw. für das Zertifikatskennwort. Sie können einen beliebigen Pfad und ein beliebiges Kennwort eingeben.

11.3.14.3 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.
SAP HANA Instanznummer	Geben Sie die Instanznummer Ihrer SAP-HANA-Datenbank an.
SAP-HANA-Tenant-Datenbank	Geben Sie den Namen Ihrer SAP-HANA-Tenant-Datenbank an.

11.3.15 Verwalten der SAP-Lumira-Einstellungen

Im Bereich "Anwendungen" der CMC können Sie Rechte für SAP-Lumira-Funktionen, die den Datenimport und die Freigabe von Inhalten betreffen, für alle Benutzer und Benutzergruppen verwalten.

Zur Verwaltung der Rechte für SAP-Lumira führen Sie die folgenden Schritte durch:

1. Wählen Sie auf der CMC-Startseite *Anwendungen* > *SAP Lumira* > *Benutzersicherheit*.
2. Wählen Sie den Benutzer oder die Gruppe aus, für den/die Sie Rechte festlegen möchten.
3. Wählen Sie *Sicherheit zuweisen*.
4. Wählen Sie *Erweitert*.
5. Wählen Sie *Rechte hinzufügen/entfernen*.
6. Legen Sie die Rechte fest, die der Benutzer für SAP Lumira haben soll.
7. Klicken Sie auf *Anwenden*.

11.3.16 Verwalten von Einstellungen für die Zusammenarbeit

11.3.16.1 Verwalten der Integration von Anwendungen für die Zusammenarbeit

Dieses Handbuch ist für BI-Plattform-Administratoren vorgesehen, die die BI-Plattform mit der Anwendung für Zusammenarbeit SAP Jam 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

Nach der Konfiguration von SAP Jam stehen Feeds aus der Anwendung für die Zusammenarbeit im BI-Launchpad zur Verfügung.

Microsoft Internet Explorer 11 wird von SAP Jam nicht unterstützt.

11.3.16.1.1 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) muss in der Central Management Console (CMC) konfiguriert werden.
- Für die Zusammenarbeitsanwendung (SAP Jam) muss eine Enterprise-Organisation festgelegt werden.
- SAP-Jam-Benutzer müssen der Enterprise-Organisation angehören.
- Ein SAP Jam Enterprise Agent ist nur erforderlich, um Benutzer bereitzustellen, die einen lokalen LDAP/AD-Verzeichnisdienst verwenden.

11.3.16.1.2 BI-Plattformkonfiguration

11.3.16.1.2.1 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 abschließend ▶ *Verwalten* ▶ *Eigenschaften* ▶.

Option	Beschreibung
Zusammenarbeit aktivieren	Aktivieren Sie dieses Kontrollkästchen, und wählen Sie *SAP Jam*.
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. 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.

11.3.16.1.2.2 Zusammenarbeit in der CMC aktivieren und konfigurieren

Für diese Aufgabe ist eine gültige Verbindung mit der Administrationskonsole der Anwendung für die Zusammenarbeit (SAP Jam) erforderlich. Sie müssen Sicherheitsdetails an die Konsole übergeben und dort abrufen.

Aus Sicherheitsgründen können die folgenden Standardkonten keine Inhalte an SAP Jam 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* 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 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*.

11.3.16.1.3 SAP-Jam-Konfiguration

11.3.16.1.3.1 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.

   Wenn Ihnen der Wert nicht vorliegt, wenden Sie sich an die Systemadministration für externe Anwendungen.
10. Klicken Sie auf *Registrieren*.

11.3.16.1.3.2 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.

11.3.17 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.

11.3.17.1 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.

Option	Beschreibung
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.
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*.

11.3.17.2 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.

Option	Beschreibung
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*.

11.3.17.3 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*.
   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*.

11.3.18 Berechtigungsserver-Konfiguration

Die Anwendung "Berechtigungsserver-Konfiguration" ist für Datenbankressourcen bestimmt, auf die über den Berechtigungsservermechanismus oder das Berechtigungsserverprotokoll zugegriffen werden kann.

Durchgängige SSO-OAuth-Unterstützung – Unterstützung für einen und mehrere OAuth-Server

In der Central Management Console können Sie mit der Anwendung *Berechtigungsserver-Konfiguration* Berechtigungsserver in der BI-Plattform konfigurieren und verwalten. Innerhalb der Anwendung ist der Administrator für die Registrierung und Verwaltung der Konfigurationen über die Berechtigungsreferenzobjekte zuständig. Jede Berechtigungsserver-Konfiguration hat ein Berechtigungsreferenzobjekt. Sie können Berechtigungsserver-Konfigurationen für agnostische, Google-Drive-, Microsoft-Drive- oder OData-Ressourcen erstellen.

Um eine Berechtigungsserver-Konfiguration zu erstellen, füllen Sie die Pflichtfelder unter *Geben Sie die Konfigurationsinformationen für einen Berechtigungsserver ein.* aus.

Der *Berechtigungsumfang* kann basierend auf Ihren Anforderungen definiert werden, um zu steuern, welche Endbenutzer Zugriff haben, online oder offline.

11.3.18.1 Berechtigungsserver konfigurieren

Sie können einen Berechtigungsserver konfigurieren.

1. Starten Sie die Central Management Console, und melden Sie sich als Administrator an.
2. Wählen Sie auf der Startseite die Option *Anwendungen* in der Spalte *Verwalten* aus.
3. Doppelklicken Sie auf der Seite *Anwendungen* auf *Berechtigungsserver-Konfiguration*.
4. Führen Sie im Dialogfeld *Berechtigungsserver-Konfigurationen* einen der folgenden Schritte aus:
   - Wählen Sie *Verwalten* > *Neue Berechtigungsserver-Konfiguration*
   - Wählen Sie in der Symbolleiste das Symbol *Neue Berechtigungsserver-Konfiguration anlegen*.
5. Geben Sie im Dialogfeld *Neue Berechtigungsserver-Konfiguration anlegen* die folgenden Parameter ein:
   - *Referenzname*
     Wählen Sie eine eindeutige zufällige Zeichenfolge und geben Sie diese zur Identifikation der Konfiguration ein, damit Sie die Konfiguration in verschiedenen Workflows für eine berechtigungsbasierte Einzelanmeldung (SSO) erkennen und auswählen können.
   - *Beschreibung* (optional):
     Geben Sie eine beliebige Anweisung oder ein beliebiges Schlüsselwort ein, um die Konfiguration zu beschreiben und sie in der Liste der verfügbaren Konfigurationen leicht identifizieren zu können.
   - **OpenID-Connect-spezifische Felder**
     Die folgenden Felder sind spezifisch für die OpenID-Connect-Authentifizierung und werden für die berechtigungsbasierte Einzelanmeldung (SSO) nicht benötigt:
     - Kontrollkästchen *Für "OpenID Connect"-Authentifizierung aktiviert*
     - *Aussteller-URI*
     - *JSON-Webschlüsselmengen-URI (jwks_uri)*
     - *Algorithmus für ID-Token-Signatur*
   - *Autorisierungsendpunkt*
     Geben Sie die URL des Berechtigungsservers ein, von dem Sie die Berechtigung erhalten können.
   - *Tokenendpunkt*
     Geben Sie die URL des Berechtigungsservers ein, bei dem Sie durch Austausch des Berechtigungscodes einen Zugriffstoken anfordern können.
   - *Client-ID*
     Geben Sie den Namen der Anwendung ein, die für die Registrierung der BI-Landschaft am Berechtigungsserver verwendet wird.
   - *Geheimer Client-Schlüssel*
     Geben Sie den spezifischen geheimen Code für die Anwendung ein, die bei der Registrierung der BI-Landschaft am Berechtigungsserver verwendet wird.
   - *Umleitungs-URL*
     Geben Sie die URL des Endpunkts in der BI-Landschaft ein, an den der Berechtigungsserver den Berechtigungscode nach erfolgreicher Validierung der Berechtigung senden muss.
   - *Sperrendpunkt* (optional)
     Geben Sie die URL des Berechtigungsservers ein, bei dem die Anwendung die Sperrung aller zuvor ausgestellten Zugriffstoken über einen bestimmten Regenerierungstoken anfordern kann.
   - *Autorisierungsumfang*
     Geben Sie die vom Berechtigungsserver unterstützten Autorisierungsumfänge ein, um die Grenzen für den Zugriff der Anwendung (BI-Landschaft) auf verschiedene verfügbare API-Ressourcen zu definieren.

> **Hinweis**
>
> Die BI-Plattform-Implementierung von OAuth-SSO basiert auf dem Offline-Zugriff. Wenn der Zweck Ihrer Konfiguration des Berechtigungsservers in der BI-Plattform darin besteht, Daten regenerieren oder auf Ressourcen zugreifen zu können, ohne jedes Mal zur Validierung der Berechtigung aufgefordert zu werden, müssen Sie dieses Feld mit dem gewünschten Umfangsparameter zusammen mit einem obligatorischen Parameter (z.B. entweder "refresh_token" oder "offline_access", je nach Anbieter des Berechtigungsservers) konfigurieren.

- *Art der Ressource*
  Wählen Sie die gewünschte Ressourcenart aus der Liste der von der BI-Plattform unterstützten Ressourcenarten aus. Im Folgenden finden Sie die aktuelle Liste der Ressourcenarten, die in der BI-Plattform für die Konfiguration des entsprechenden Berechtigungsservers und den Zugriff über diesen Server unterstützt werden:
  - *Agnostisch* (Standardwert)
    Nicht spezifisch für einen bestimmten Anbieter oder ein bestimmtes Protokoll, um alle Ressourcen anzugeben, auf die mit einer durch einen Berechtigungsserver erteilten Berechtigung zugegriffen werden kann.
  - *GoogleDrive*
    Gibt an, dass es sich um die Konfiguration eines Google-Berechtigungsservers handelt, der für den Zugriff auf Google Drive in verschiedenen BI-Plattform-Szenarien verwendet werden kann. Es kann immer nur eine Konfiguration vom Typ "GoogleDrive" im System vorhanden sein.
  - *Microsoft Drive*
    Gibt an, dass es sich um die Konfiguration eines Microsoft-Berechtigungsservers handelt, der für den Zugriff auf Microsoft Drive in verschiedenen BI-Plattform-Szenarien verwendet werden kann. Es kann immer nur eine Konfiguration vom Typ "Microsoft Drive" im System vorhanden sein.
  - *OData*
    Nicht spezifisch für einen bestimmten Anbieter, sondern um anzugeben, dass sich die Konfiguration auf eine Ressource bezieht, auf die über das OData-Protokoll mit einer durch einen Berechtigungsserver erteilten Berechtigung zugegriffen werden kann. Wie auch im Fall von "GoogleDrive" kann immer nur eine Konfiguration vom Typ "OData" im System vorhanden sein.

> **Hinweis**
>
> Der Parameter *Art der Ressource* hat nichts mit dem OAuth-2.0-Standard zu tun. Er wurde jedoch in der Konfiguration eingeführt, um mögliche Mehrdeutigkeiten bei der Identifizierung bestimmter Ressourcen in der BI-Plattform zu vermeiden. So können die entsprechenden Konfigurationen einfach ausgewählt und in bestimmten Szenarien für die Berechtigungserteilung verwendet werden.

- *Zugriffstyp*
  Dieser Parameter ist spezifisch für die Berechtigungskonfiguration vom Typ *GoogleDrive*. Er wird automatisch ausgefüllt, wenn das Feld *Ressourcentyp* den Wert *GoogleDrive* hat.
- *Benutzerdefinierte Parameter* (optional)
  Geben Sie alle benutzerdefinierten Parameter ein, die beim Anfordern der Berechtigung gesendet werden müssen. Dies bezieht sich auf alle benutzerdefinierten Anforderungen (sofern vorhanden) des zu konfigurierenden Berechtigungsservers.

> **Hinweis**
>
> Der Name des benutzerdefinierten Parameters muss in der Konfiguration eindeutig sein.

> In jeder Berechtigungskonfiguration können maximal fünf benutzerdefinierte Parameter konfiguriert werden.

6. Nachdem Sie alle erforderlichen Parameter ausgefüllt haben, wählen Sie *OK*, um die Details zu validieren, und speichern Sie die Konfiguration.

   Die Konfiguration wird als Systemobjekt vom Typ *Autorisierungsreferenz* im Repository abgelegt. Sie können die Konfiguration in allen unterstützten Szenarien über ihren *Referenznamen* referenzieren.

11.3.18.2 Berechtigungsserver-Konfiguration testen

Sie können Ihre Berechtigungsserver-Konfiguration testen.

1. Nachdem Sie die Berechtigungsserver-Konfiguration erfolgreich gespeichert haben, starten Sie das BI-Launchpad, und melden Sie sich an, um Ihre Konfiguration zu testen.

   > ⓘ Hinweis
   >
   > Es ist derzeit nicht möglich, die Konfiguration von der CMC aus zu testen.
   >
   > Melden Sie sich als Administrator oder mit einem beliebigen BI-Plattform-Benutzerkonto an, das nicht auf die Verwendung der oben gespeicherten Berechtigungskonfiguration beschränkt ist.
   >
   > Verwenden Sie die aktuell für das BI-Launchpad konfigurierte Anmeldemethode (z.B. die Enterprise-Authentifizierung oder eine beliebige andere Authentifizierungsmethode).

2. Wählen Sie das Benutzersymbol.
3. Wählen Sie im daraufhin angezeigten Dropdown-Menü die Option *Einstellungen*.
4. Wählen Sie im Dialogfeld *Einstellungen* im Abschnitt *Benutzerkonto* die Option *Autorisierungstoken*.
5. Wählen Sie in der Spalte *Token verwalten* die Option *Generieren*.
6. Gemäß Ihrer Organisationsrichtlinie erfolgt basierend auf der Berechtigungskonfiguration in Ihrem Berechtigungsserver entweder die Kontovalidierung anhand der im System konfigurierten Zertifikate, oder Sie werden je nach Konfigurationseinstellungen zur Eingabe von Benutzername und Kennwort und/oder zur Multifaktor-Authentifizierung aufgefordert.
7. Sobald die Anmeldeinformationen oder das Zertifikat erfolgreich validiert wurden, sollte die BI-Plattform den Regenerierungstoken erhalten haben. Dieser sollte sicher im BI-Plattform-Repository gespeichert worden sein. Wenn dieser Schritt erfolgreich abgeschlossen wurde, sollten Sie die folgenden Änderungen auf der Registerkarte *Autorisierungstoken* sehen:
   - In der Spalte *Läuft ab am* sollte das Ablaufdatum für den vom Berechtigungsserver ausgestellten Token angezeigt werden. Wenn Ihr Berechtigungsserver einen Token ohne Ablaufdatum ausstellt, wird der Spaltenwert auf *Kein Ablauf* aktualisiert.
   - In der Spalte *Token verwalten* sollte neben der Schaltfläche *Generieren* die Schaltfläche *Löschen* angezeigt werden.
     - Die Schaltfläche *Löschen* dient zum Löschen des vom Berechtigungsserver ausgestellten Tokens. Diese Löschung ist nicht auf das Löschen des Tokens aus dem Repository-Speicher der BI-Plattform beschränkt, sondern kann je nach Konfiguration und Unterstützung auch an den Berechtigungsserver propagiert werden.
     - Wenn als optionaler Parameter *Sperrendpunkt* die richtige URL, die von Ihrem Berechtigungsserver unterstützt wird, eingegeben ist, wird der ausgestellte Token auch auf der

Ebene des Berechtigungsservers gesperrt und aus dem Repository-Speicher der BI-Plattform gelöscht.

8. Wenn der Token ausgestellt und die Spalte *Läuft ab am* entsprechend dem Ablaufdatum des ausgestellten Tokens aktualisiert wurde, funktioniert die Konfiguration ordnungsgemäß und ist für die Verwendung durch den BI-Entwickler und den BI-Endbenutzer bereit.

11.3.19 Konfiguration der Informationsklassifizierung

In der BI-Plattform können Sie den Azure-Policy-Server Ihrer Organisation so konfigurieren, dass Ihre BI-Landschaft den BI-Content klassifizieren kann. Diese Klassifizierungsfunktionen können durch Vertraulichkeitsbezeichnungen angewendet werden, die vom Azure-Policy-Server-Administrator Ihrer Organisation definiert wurden.

> **Hinweis**
>
> Diese Integrationsoption zum Konfigurieren des Policy-Servers wird nur für die Information Protection Platform von Microsoft Azure unterstützt.
>
> Das Release SAP BusinessObjects BI 4.3 SP 04 enthält eine Integrationsoption für die Information Protection Platform von Microsoft Azure. Beachten Sie jedoch, dass die Anwendung zum Konfigurieren der Azure-Policy-Server-Details in der BI-Plattform nicht standardmäßig aktiviert ist. Sie wird als ausgeblendete Funktion ausgeliefert. Informationen zum Einblenden dieser ausgeblendeten Funktion finden Sie im SAP-Hinweis 3409349.

Diese Funktion ist nur auf der Windows-Plattform verfügbar.

11.3.19.1 So konfigurieren Sie die Informationsklassifizierung

1. Melden Sie sich als Administrator an der *Central Management Console* an.
2. Navigieren Sie zu *Anwendungen*.
3. Klicken Sie mit der rechten Maustaste auf die Anwendung *Konfiguration der Informationsklassifizierung*.
4. Wählen Sie *Konfiguration für Informationsklassifizierung*.
5. Aktivieren Sie das Kontrollkästchen *Informationsklassifizierung aktivieren*, um die Konfiguration und die Felder zu aktivieren.
6. Geben Sie die Token-URL des Felds *Richtlinienserver-URL* des Azure-Policy-Servers Ihrer Organisation ein. Die URL muss das Format `https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/token` aufweisen.
7. Geben Sie Werte für *Client-ID* und *Geheimer Client-Schlüssel* aus Ihrer Client-Anwendung auf Azure ein. Diese sind für den Client-Anmeldedaten-Ablaufmodus der Berechtigung für den Zugriff auf den Azure-Policy-Server Ihrer Organisation aktiviert.
8. Klicken Sie auf *Konfiguration speichern und testen*, um die Verbindung zu testen.
9. Wenn der Konfigurationstest erfolgreich war, klicken Sie auf *Speichern* oder *Speichern und schließen*.

> **Hinweis**
>
> Aktivieren Sie nicht das Kontrollkästchen für *Aktiviert für Zertifikatsauthentifizierung*, da dieser Modus der Authentifizierungskonfiguration nicht unterstützt wird.

12 Verwalten von Datenquellen und Verbindungen

12.1 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 49]
Verbindungsrechte [Seite 488]

12.1.1 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*.

12.2 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 49]
Universe-Design-Tool [Seite 494]
Universumsrechte (.unv) [Seite 484]
Information-Design-Tool [Seite 494]
Universumsrechte (.unx) [Seite 486]

12.2.1 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*.

13 Verwalten von Hotbackups

13.1 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 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
>
> - Hotbackup führt keine Sicherung im eigentlichen Sinne durch, sondern verzögert bloß die Löschung von Dateien. Bei der Bearbeitung und Aktualisierung von Dateien werden mehrere Kopien erstellt. Dies bedeutet, dass die Beziehungen zwischen CMS und FRS stets korrekt sind, wodurch eine Sicherung jedes der beiden Server zu unterschiedlichen Zeitpunkten erfolgen kann. Dies geschieht innerhalb des Hotbackup-Fensters.
> - Am Ende einer Systemwiederherstellung finden Sie viele zusätzliche Dateien im FRS vor, die vom Repository Diagnostic Tool gelöscht werden müssen.
> - Initialisieren Sie vor dem Sichern des FRS-Dateispeichers immer die CMS-Sicherung.
>
> 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 einfachsten 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 auf 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 Sicherungssatz abzulegen.

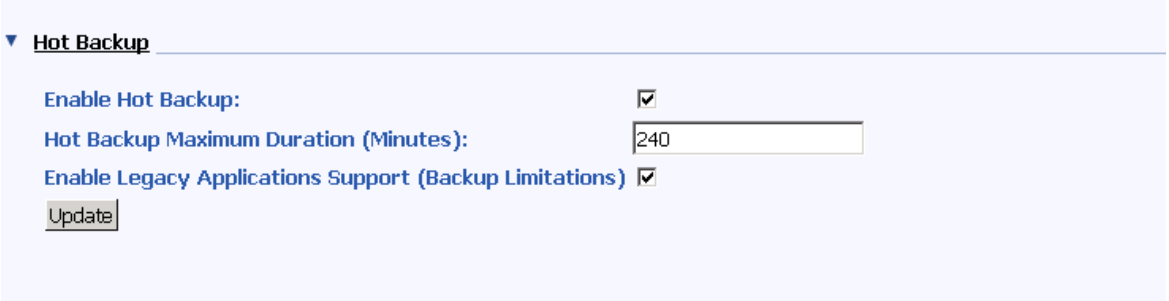
13.1.1 Aktivieren von Hotbackups

1. Öffnen Sie die Central Management Console (CMC).
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 den hier eingegebenen Wert überschreitet, können Inkonsistenzen in den gesicherten Daten auftreten. Um dies zu vermeiden, ist es sicherer, die für die Sicherung benötigte Zeit zu überschätzen.

5. 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.

14 Ordner

14.1 Ordner

Ordner sind Objekte, die zum Gruppieren und Organisieren von anderen Objekten verwendet werden, um den Inhalt in logische Gruppen aufzuteilen. Jedes Objekt in der BI-Plattform muss in einem Ordner enthalten sein.

Standardmäßig übernehmen neue Objekte, die Sie einem Ordner hinzufügen, die Objektrechte des Ordners. Da Sicherheitsmerkmale auf Ordnerebene festgelegt werden können, kann über Ordner der Zugriff auf Informationen gesteuert werden.

Es empfiehlt sich, Ordner in einer bereits in Ihrer Organisation vorhandenen Struktur (wie Abteilungen, Regionen oder Ihrer Datenbanktabelle) einzurichten und anschließend Kategorien zu verwenden, um ein alternatives Organisationssystem einzurichten.

14.1.1 Erstellen von Ordnern

Bevor Sie einen neuen Ordner der obersten Ebene (übergeordneten Ordner) erstellen, stellen Sie sicher, dass *Alle Ordner* angezeigt werden.

Um den Namen, die Beschreibung oder die Schlüsselwörter für einen Ordner rasch zu ändern, markieren Sie den Ordner und wählen *Verwalten* > *Eigenschaften*.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wechseln Sie in das Verzeichnis, in dem Sie einen Ordner erstellen möchten.

   Wenn Sie einen Unterordner erstellen, suchen Sie den Zielordner, in dem Sie den neuen Ordner speichern möchten.
3. Wählen Sie *Verwalten* > *Neu* > *Ordner*.
4. Geben Sie im Dialogfeld *Ordner erstellen* einen Namen für die Gruppe ein, und klicken Sie auf *OK*.

Der neue Ordner wird in der Liste der Ordner und Objekte angezeigt.

Sie können dem Ordner Objekte hinzufügen oder dessen Eigenschaften bearbeiten.

14.1.2 Löschen von Ordnern

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Suchen Sie den zu löschenden Ordner, und wählen Sie ihn aus.

   Um mehrere Ordner gleichzeitig zu löschen, halten Sie die Taste `Strg` oder die `Umschalttaste` gedrückt und klicken auf die zu löschenden Ordner.

3. Wählen Sie *Verwalten* > *Löschen*.
4. Klicken Sie im angezeigten Meldungsfeld *Löschen* auf *OK*, um den Vorgang zu bestätigen.

Der Ordner, alle Unterordner, Berichte und andere Objekte in dem Ordner werden von der BI-Plattform entfernt.

14.1.3 Kopieren oder Verschieben von Ordnern

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie den Ordner aus, den Sie kopieren bzw. verschieben möchten.

   Wenn sich der Ordner nicht auf der obersten Ebene befindet, suchen Sie dessen übergeordneten Ordner, und wählen Sie dessen Inhalt aus. Um gleichzeitig mehrere Ordner zu kopieren oder zu verschieben, halten Sie die `STRG`-Taste oder die `UMSCHALT`-Taste gedrückt, und klicken Sie auf jeden zu kopierenden bzw. zu verschiebenden Ordner.
3. Wählen Sie *Organisieren* > *Kopieren nach* oder *Organisieren* > *Verschieben nach*.
4. Wählen Sie im Dialogfeld *Kopieren nach* oder *Verschieben nach* den Zielordner aus.
5. Klicken Sie auf *Kopieren* oder *Verschieben*.

Der von Ihnen ausgewählte Ordner wird in das neue Ziel kopiert bzw. verschoben.

14.1.4 Beschränken von Berichtinstanzen auf Ordnerebene

Durch Festlegen von Beschränkungen können Sie Berichtsinstanzen automatisch aus der BI-Plattform löschen.

Beschränkungen, die Sie für einen Ordner festlegen, wirken sich auf alle darin enthaltenen Objekte aus. Sie können folgende Beschränkungen auf Ordnerebene festlegen:

- Die Anzahl der Instanzen für jedes Objekt, jeden Benutzer oder jede Benutzergruppe
- Die Anzahl an Tagen, die die Instanzen für den Benutzer oder die Gruppe gespeichert werden

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Suchen Sie den Ordner, für den Sie Beschränkungen festlegen möchten, unLocate and select the folder for which to set limits, and select *Aktionen* > *Grenzwerte*.
3. Aktivieren Sie im Dialogfeld *Grenzwerte* das Kontrollkästchen *Überzählige Instanzen löschen, wenn die Anzahl der Objektinstanzen mehr als N beträgt*, und geben Sie die maximale Anzahl an Instanzen pro Objekt, die der Ordner enthalten darf, bevor die Instanzen gelöscht werden, in das Feld ein.

   Standardwert: 100.
4. Klicken Sie auf *Aktualisieren*.
5. Um die Anzahl an Instanzen pro Benutzer oder Gruppe zu beschränken, klicken Sie neben *Überzählige Instanzen für die folgenden Benutzer/Gruppen löschen* auf *Hinzufügen*.
6. Wählen Sie einen Benutzer oder eine Gruppe aus, klicken Sie auf >, um den Benutzer oder die Gruppe zur Liste *Ausgewählte Benutzer/Gruppen* hinzuzufügen, und klicken Sie auf *OK*.
7. Geben Sie für jeden in Schritt 6 hinzugefügten Benutzer bzw. jede hinzugefügte Gruppe in das Feld *Höchstanzahl von Instanzen pro Objekt* die maximale Anzahl an Instanzen ein, die in der BI-Plattform angezeigt werden sollen.

Standardwert: 100.

8. Um die Anzahl an Instanzen pro Benutzer oder Gruppe zu beschränken, klicken Sie neben *Instanzen nach N Tagen für die folgenden Benutzer/Gruppen löschen* auf *Hinzufügen*.
9. Wählen Sie einen Benutzer oder eine Gruppe aus, klicken Sie auf >, um den Benutzer oder die Gruppe zur Liste *Ausgewählte Benutzer/Gruppen* hinzuzufügen, und klicken Sie auf *OK*.
10. Geben Sie für jeden in Schritt 9 hinzugefügten Benutzer bzw. jede hinzugefügte Gruppe in das Feld *Höchstalter einer Instanz in Tagen* das Höchstalter für Instanzen ein, ab dem sie aus der BI-Plattform gelöscht werden sollen.

    Standardwert: 100.
11. Klicken Sie auf *Aktualisieren*.

Weitere Informationen

Beschränkungen für Instanzen festlegen [Seite 304]

14.1.5 Beschränkung von Dokumenten in Posteingängen

Durch Festlegen von Beschränkungen können Sie Dokumente automatisch aus der BI-Plattform löschen.

Beschränkungen, die Sie für einen Posteingang festlegen, wirken sich auf alle darin enthaltenen Objekte aus. Sie können folgende Beschränkungen auf Posteingangsebene festlegen:

- die Anzahl der Dokumente für jeden Posteingang, jeden Benutzer oder jede Benutzergruppe
- die Anzahl an Tagen, über die die Dokumente für den Benutzer oder die Gruppe vorgehalten werden

1. Wechseln Sie zum Verwaltungsbereich *Posteingänge* der CMC.
2. Klicken Sie mit der rechten Maustaste auf *Posteingänge*, und wählen Sie *Beschränkungen*.
3. Aktivieren Sie im Dialogfeld *Beschränkungen* das Kontrollkästchen *Überzählige Dokumente löschen, wenn die Anzahl der Dokumente mehr als N beträgt:*, und geben Sie die maximale Anzahl an Dokumenten ein, die der Posteingang umfassen soll, bevor die Dokumente aus dem Posteingang gelöscht werden.

    Standardwert: 100
4. Wählen Sie *Aktualisieren*.
5. Um die Anzahl Dokumente pro Benutzer oder Gruppe zu beschränken, klicken Sie neben *Überzählige Dokumente für die folgenden Benutzer/Gruppen löschen* auf *Hinzufügen*.
6. Wählen Sie einen Benutzer oder eine Gruppe aus, klicken Sie auf >, um den Benutzer oder die Gruppe zur Liste *Ausgewählte Benutzer/Gruppen* hinzuzufügen, und wählen Sie *OK*.
7. Geben Sie für jeden in Schritt 6 hinzugefügten Benutzer bzw. jede hinzugefügte Gruppe in das Feld *Höchste Anzahl an Dokumenten* die maximale Anzahl an Dokumenten ein, die in BI angezeigt werden sollen.

    Standardwert: 100
8. Um das Alter der Dokumente pro Benutzer oder Gruppe zu beschränken, klicken Sie neben *Dokumente nach N Tagen für die folgenden Benutzer/Gruppen löschen* auf *Hinzufügen*.
9. Wählen Sie einen Benutzer oder eine Gruppe aus, klicken Sie auf >, um den Benutzer oder die Gruppe zur Liste *Ausgewählte Benutzer/Gruppen* hinzuzufügen, und wählen Sie *OK*.

10. Geben Sie für jeden in Schritt 9 hinzugefügten Benutzer bzw. jede hinzugefügte Gruppe in das Feld *Höchste Anzahl an Dokumenten pro Benutzer* die maximale Anzahl an Tagen ein, bevor diese aus BI gelöscht werden sollen.

    Standardwert: 100

11. Wählen Sie *Aktualisieren*.

15 Kategorien

15.1 Arbeiten mit Kategorien

15.1.1 Erstellen einer Kategorie

1. Wählen Sie in der CMC den Bereich *Kategorien* aus.
2. Wählen Sie *Verwalten* > *Neu* > *Kategorie*.
3. Geben Sie im Dialogfeld *Kategorie erstellen* unter *Geben Sie einen neuen Kategorienamen ein* einen Namen für die Kategorie ein.
4. Klicken Sie auf *OK*.

Die Kategorie wird der BI-Plattform hinzugefügt.

15.1.2 Löschen einer Kategorie

Wenn Sie eine Kategorie löschen, werden alle darin enthaltenen Unterkategorien gelöscht. In der Kategorie enthaltene Berichte und andere Objekte werden jedoch nicht von der BI-Plattform gelöscht.

1. Wählen Sie in der CMC den Bereich *Kategorien* aus.
2. Wählen Sie die zu löschende Kategorie.

   Wenn die Kategorie sich nicht auf der obersten Ebene befindet, suchen Sie die übergeordnete Kategorie und anschließend die Unterkategorie. Um gleichzeitig mehrere Kategorien zu löschen, halten Sie die `STRG`-Taste oder die `UMSCHALT`-Taste gedrückt, und klicken Sie auf jede zu löschende Kategorie.
3. Wählen Sie *Verwalten* > *Löschen*.
4. Klicken Sie im angezeigten Meldungsfeld *Löschen* auf *OK*, um den Vorgang zu bestätigen.

Die Kategorie wird von der BI-Plattform gelöscht.

15.1.3 Verschieben einer Kategorie

Beim Verschieben einer Kategorie behält diese die mit ihr verknüpften Objekte und deren Objektrechte bei.

So könnten Sie beispielsweise eine Kategorie namens "Umsatz Südamerika" haben, auf die nur Personen in dieser Region zugreifen können, sowie eine Kategorie namens "Weltumsatz", die die Weltumsatz-Berichte enthält, auf die alle Personen zugreifen können. Sie verschieben die Regionskategorien in die Kategorie

"Weltumsatz". Die Kategorie "Umsatz Südamerika" behält ihre Berechtigungen und zugehörigen Objekte bei, obwohl sie eine Unterkategorie der Kategorie "Weltumsatz" ist.

1. Wählen Sie in der CMC den Bereich *Kategorien* aus.
2. Wählen Sie die zu verschiebende Kategorie aus.

   Wenn die Kategorie sich nicht auf der obersten Ebene befindet, suchen Sie ihre übergeordnete Kategorie und anschließend die Unterkategorie. Um gleichzeitig mehrere Kategorien zu verschieben, halten Sie die `STRG`-Taste oder die `UMSCHALT`-Taste gedrückt, und klicken Sie auf jede zu verschiebende Kategorie.
3. Wählen Sie *Organisieren* > *Verschieben nach*.

   Wenn die BI-Plattform zahlreiche Kategorien enthält, geben Sie den Namen der Kategorie im Feld *Titel durchsuchen* ein, oder Sie klicken auf *Vorherige*, *Nächste* oder + (Pluszeichen), um die Kategorienliste zu durchsuchen.
4. Im Dialogfeld *Verschieben in* wählen Sie die Zielkategorie aus und klicken dann auf *Verschieben*.

Die Kategorie wird zu dem neuen Ziel verschoben.

15.1.4 Hinzufügen von Objekten zu Kategorien

1. Wählen Sie in der CMC den Bereich *Ordner* aus.
2. Suchen und wählen Sie das Objekt aus, das Sie einer Kategorie hinzufügen möchten.
3. Wählen Sie *Verwalten* > *Kategorien*.
4. Wählen Sie im Dialogfeld *Kategorien* die Kategorie aus, der Sie das Objekt hinzufügen möchten.
5. Klicken Sie auf *Speichern und schließen*.

Das Objekt wird der Kategorie hinzugefügt.

15.1.5 Entfernen oder Löschen von Objekten aus einer Kategorie

Wenn Sie ein Objekt entfernen, entfernen Sie es zwar aus der Kategorie, aber es bleibt auf der BI-Plattform erhalten. Wenn Sie ein Objekt löschen, entfernen Sie es aus der Kategorie und löschen es außerdem von der BI-Plattform.

1. Wählen Sie in der CMC den Bereich *Kategorien* oder *Persönliche Kategorien* aus.
2. Doppelklicken Sie auf die Kategorie, aus der Sie ein Objekt entfernen oder löschen möchten.
3. Wählen Sie die zu entfernenden oder zu löschenden Objekte aus.
4. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf *Aktionen* > *Aus Kategorie entfernen*, um das Objekt nur aus der Kategorie zu entfernen.
   - Wählen Sie *Verwalten* > *Löschen*, um das Objekt aus der Kategorie zu entfernen und von der Plattform zu löschen.
5. Klicken Sie im Dialogfeld *Aus Kategorie entfernen* bzw. *Löschen* auf *OK*, um das Entfernen bzw. Löschen zu bestätigen.

Das Objekt wird entfernt bzw. gelöscht.

15.1.6 Anzeigen der persönlichen Kategorien eines Benutzers

Falls Sie über die entsprechenden Zugriffsrechte verfügen, können Sie die persönlichen Kategorien für Benutzer anzeigen, bearbeiten oder löschen.

1. Wählen Sie in der CMC den Bereich *Kategorien* aus.
2. Wählen Sie das Benutzerkonto aus, für das Sie die persönlichen Kategorien anzeigen möchten.

Eine Liste der persönlichen Kategorien des Benutzers wird angezeigt.

15.1.7 Hinzufügen von mehreren Objekten zu einer Kategorie

1. Wechseln Sie zum Verwaltungsbereich *Kategorien* oder *Persönliche Kategorien* der CMC.
2. Suchen und wählen Sie die Kategorie aus, der Sie Objekte hinzufügen möchten.
3. Wählen Sie *Aktionen* > *Zu Kategorie hinzufügen*.
4. Suchen Sie im Dialogfeld *Zu Kategorie hinzufügen* unter *Verfügbare Objekte* die Objekte, die Sie hinzufügen möchten, und klicken Sie auf >, um die Objekte in die Liste *Ausgewählte Objekte* zu verschieben.
5. Klicken Sie auf *OK*.

16 Objektverwaltung

16.1 Standardeinstellungen

Die Standardeinstellungen gestatten Ihnen, benutzerdefinierte Eigenschaften für diverse Inhaltsobjekte zu bearbeiten und zu verwalten. Die Standardeinstellungen können sich je nach Objekttyp unterscheiden. In diesem Abschnitt werden die unterschiedlichen verfügbaren Standardeinstellungen aufgeführt und Verknüpfungen zu anderen Themen, über die weitere Informationen aufgerufen werden können, werden bereitgestellt. Die Standardeinstellungen sind alphabetisch aufgelistet.

Komponentenfehler

Diese Einstellung gilt nur für Objektpakete.

Ziele

Diese Einstellung gilt nur für Objekte, die gesendet werden können.

Ereignisse

Diese Einstellung gilt nur für Objekte, die zeitgesteuert verarbeitet werden können, und funktioniert wie die Ereigniseinstellungen für die zeitgesteuerte Verarbeitung.

Fallback-Server

Im Fenster *Eigenschaften: Eigenschaften: Neues Ereignis* in den *Ereigniseinstellungen* wird das Feld *Fallback-Server* als Sicherung für die vorhandene *Serveroption* zur *Failover-Unterstützung für Event Server mit Dateiereignissen* eingeführt.

Die Liste *Fallback-Server* unterstützt jedes Ereignis zusammen mit der vorhandenen *Serveroption* bei der Auswahl des Standard-Event-Servers.

Wenn beispielsweise der Standard-Event-Server ausgefallen ist, kann jeder Event Server aus der Fallback-Liste das Dateiereignis wie vorgesehen verarbeiten.

Diese Option ist sowohl im Szenario *Erstellen* als auch im Szenario *Dateiereignis bearbeiten* verfügbar.

Benachrichtigung

Diese Einstellung gilt nur für Objekte, die zeitgesteuert verarbeitet werden können, und funktioniert wie die Benachrichtigungseinstellungen für die zeitgesteuerte Verarbeitung.

Programmanmeldung

Diese Einstellung gilt nur für Programmobjekte.

Programmparameter

Diese Einstellung gilt nur für Programmobjekte.

Wiederholung

Diese Einstellung gilt nur für Objekte, die zeitgesteuert verarbeitet werden können, und funktioniert wie die Wiederholungseinstellungen für die zeitgesteuerte Verarbeitung.

Zeitgesteuert verarbeiten für

Diese Einstellung gilt nur für Objekte, die zeitgesteuert verarbeitet werden können, und funktioniert wie die *"Zeitgesteuert verarbeiten für"*-Einstellungen für die zeitgesteuerte Verarbeitung.

Zeitsteuerungsserver-Gruppe

Diese Einstellung gilt nur für Objekte, die zeitgesteuert verarbeitet werden können, und funktioniert wie die Ereigniseinstellungen für die zeitgesteuerte Verarbeitung.

Weitere Informationen

Festlegen von Komponentenfehleroptionen für ein Objektpaket [Seite 285]

Senden von Objekten oder Instanzen an ein Ziel [Seite 270]
Zeitgesteuerte Verarbeitung von Objekten auf der Grundlage von Ereignissen [Seite 297]
Zeitgesteuerte Verarbeitung von Objekten zum Auslösen eines Ereignisses [Seite 297]
Konfigurieren von Erfolgs- oder Fehlerbenachrichtigungen für eine Instanz [Seite 298]
Festlegen des Benutzerkontos für ein Programmobjekt [Seite 284]
Festlegen von Befehlszeilenargumenten [Seite 281]
Festlegen eines Arbeitsverzeichnisses für ein Programmobjekt [Seite 281]
Angeben des Pfads zu externen oder Hilfsdateien [Seite 282]
Festlegen der erforderlichen Parameter für Java-Programme [Seite 283]
Ermöglichen des Zugriffs durch Java-Programme auf andere Dateien [Seite 284]
Wiederholungsmuster [Seite 288]
Ausführungsoptionen für Wiederholungsmuster [Seite 289]
Zeitgesteuerte Verarbeitung eines Berichtsobjekts für einzelne Benutzer [Seite 301]
Auswählen eines Servers oder einer Servergruppe für die zeitgesteuerte Verarbeitung von Objekten [Seite 301]

16.2 Hinzufügen von Objekten in der CMC

Sie müssen über Administratorrechte verfügen, um ein Objekt in der CMC hinzufügen zu können.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Suchen Sie die Kategorie, der Sie Objekte hinzufügen möchten, und wählen Sie sie aus.
3. Wählen Sie *Verwalten* > *Hinzufügen* aus, und wählen Sie dann eine der folgenden Optionen aus:

Option	Beschreibung
Programmdatei	Fügt ein Programmobjekt hinzu
Lokales Dokument	Fügt andere Objekttypen hinzu

   Es wird ein Dialogfeld angezeigt, in dem Sie die Objekteigenschaften angeben können.

4. Legen Sie die Eigenschaften des Objekts fest.

   Welche Eigenschaftenfelder angezeigt werden, hängt vom Typ des Objekts ab, das Sie veröffentlichen möchten. Die Eigenschaftenfelder sind in der Tabelle „"Objekteigenschaften in der CMC"“ zusammengefasst.
5. Um das Objekt einer Kategorie zuzuweisen, wählen Sie die Kategorie aus der Liste aus.
6. Klicken Sie auf *OK*.
   Das Dialogfeld wird geschlossen, und die CMC wird regeneriert, um das Objekt und weitere Ordnerinhalte anzuzeigen.

16.3 Kopieren von Objekten

1. Suchen Sie im Bereich *Ordner* das Objekt, das Sie kopieren möchten, und wählen Sie es aus.
2. Klicken Sie auf *Organisieren* > *Kopieren nach*.
   Das Dialogfeld *Kopieren* wird angezeigt.
3. Suchen Sie im Bereich *Ziele auswählen* den Zielordner, in den Sie das Objekt kopieren möchten, und klicken Sie auf >, um ihn in die Liste *Ziele* zu verschieben.

   > **Hinweis**
   >
   > Um den Zielordner zu verschieben, wählen Sie ihn im Detailbereich auf der rechten Seite aus.

   > **→ Tipp**
   >
   > Verwenden Sie `UMSCHALTTASTE` + `Klicken` oder `STRG` + `Klicken`, um mehrere Ordner auszuwählen.

4. Klicken Sie abschließend auf *Kopieren*.
   Das ausgewählte Objekt wird in den Zielordner kopiert.

16.4 So verschieben Sie ein Objekt

1. Suchen Sie im Bereich *Ordner* das Objekt, das Sie verschieben möchten, und wählen Sie es aus.
2. Klicken Sie auf *Organisieren* > *Verschieben nach*.
   Das Dialogfeld *Verschieben* wird angezeigt.
3. Wählen Sie den Zielordner aus.

   > **Hinweis**
   >
   > Um den Zielordner zu verschieben, wählen Sie ihn im Detailbereich auf der rechten Seite aus.

   > **→ Tipp**
   >
   > Verwenden Sie `UMSCHALTTASTE` + `Klicken` oder `STRG` + `Klicken`, um mehrere Ordner auszuwählen.

4. Klicken Sie auf *Verschieben*.
   Das Objekt wird vom ursprünglichen Ordner in den Zielordner verschoben.

16.5 Erstellen von Objektverknüpfungen

Verknüpfungen sind hilfreich, wenn Sie einem Benutzer Zugriff auf ein Objekt gewähren möchten, ohne dass er Zugriff auf den gesamten Ordner erhält, in dem sich das Objekt befindet.

Nach dem Erstellen der Verknüpfung können Benutzer mit Zugriffsrechten für den Ordner, in dem sich die Verknüpfung befindet, auf dieses Objekt und seine Instanzen zugreifen.

1. Suchen Sie im Bereich *Ordner* das Objekt, für das Sie eine Verknüpfung erstellen möchten, und wählen Sie es aus.
2. Klicken Sie auf *Organisieren* > *Verknüpfung erstellen*.
   Das Dialogfeld *Verknüpfung erstellen in* wird angezeigt.
3. Suchen Sie im Bereich *Ziele auswählen* den Ordner, in dem Sie eine Verknüpfung erstellen möchten, und klicken Sie auf >, um den Ordner in die Liste *Ziele* zu verschieben.

   > **Hinweis**
   >
   > Um den Zielordner zu verschieben, wählen Sie ihn im Detailbereich auf der rechten Seite aus.

4. Klicken Sie auf *Verknüpfung erstellen*.
   Eine Verknüpfung zum Objekt wird im angegebenen Ordner angezeigt.

16.6 Löschen von Objekten

Löschen können Sie entweder Objekte, Ordner (hierbei werden alle Objekte und Instanzen dieses Ordners gelöscht) oder Objektinstanzen (anstelle des Objekts selbst).

> **Hinweis**
>
> Wenn Sie ein Objekt löschen, werden alle vorhandenen und zeitgesteuerten Instanzen gelöscht.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das Objekt aus, das Sie löschen möchten.
3. Klicken Sie auf *Verwalten* > *Löschen*.
4. Wenn in einer Meldung eine Bestätigung angefordert wird, klicken Sie auf *OK*.

16.7 So suchen Sie nach einem Objekt bzw. nach Objekten

Die Suchfunktion ermöglicht die Suche nach bestimmten Zeichenfolgen innerhalb von Objekttiteln und -beschreibungen.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.

   Das Feld "Suchen" befindet sich in der oberen rechten Ecke des Verwaltungsbereichs *Ordner*. Der Suchtyp ist standardmäßig auf *Titel durchsuchen* festgelegt.
2. Geben Sie die Suchkriterien an.
   a. Wenn Sie nach einem anderen Kriterium als dem Dateinamen suchen möchten, klicken Sie auf *Titel durchsuchen*, um den Suchtyp zu ändern.

      Folgende Optionen stehen zur Verfügung:

- *Alle Felder durchsuchen*
  Durch diese Option werden alle mit Objekten verknüpften Dateinamen, Schlüsselwörter und Beschreibungen durchsucht.
- *Titel durchsuchen*
  Dies ist die Standardoption, durch die nach Dateinamen gesucht wird.
- *Schlüsselwort suchen*
  Durch diese Option werden alle mit Objekten verknüpften Schlüsselwörter durchsucht.
- *Beschreibung suchen*
  Durch diese Option werden alle mit Objekten verknüpften Beschreibungen durchsucht.

b. Geben Sie den Suchtext im Feld "Suchen" ein.

3. Klicken Sie auf *Suchen*.
   Nachdem die Suche beendet ist, wird eine Liste der Ergebnisse angezeigt, die mit den Suchkriterien übereinstimmen.

16.8 Senden von Objekten oder Instanzen an ein Ziel

Sie können entweder eine Kopie eines Objekts oder einer Instanz bzw. eine Verknüpfung zum Objekt oder zur Instanz senden. Darüber hinaus können Sie das Ziel auswählen, beispielsweise "FTP", "SFTP" oder "BI-Posteingang". Nicht alle Objekttypen können auch an alle Ziele gesendet werden.

> **Hinweis**
>
> Mithilfe von *Organisieren* > *Senden* können Sie vorhandene Objekte oder Instanzen eines Objekts an verschiedene Ziele senden. Der Befehl *Senden* ist nur für vorhandene Objekte oder Instanzen geeignet. Sie veranlasst das System nicht dazu, das Objekt auszuführen, neue Instanzen zu erstellen oder die Daten für eine Berichtsinstanz zu regenerieren.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das Objekt oder die Instanz aus, das bzw. die Sie senden möchten.
   - Wenn Sie ein Objekt senden möchten, wählen Sie es aus, klicken auf *Organisieren* > *Senden* und wählen ein Ziel aus.
   - Wenn Sie eine Instanz senden möchten, wählen Sie das Objekt aus, und klicken Sie auf *Aktionen* > *Verlauf*. Wählen Sie im Dialogfeld *Verlauf* eine Instanz aus, klicken Sie auf *Senden* und dann auf die gewünschte Zieloption.
     Wählen Sie nur Instanzen mit dem Status "Erfolgreich" oder "Fehlgeschlagen". Instanzen mit dem Status "Wiederkehrend" oder "Ausstehend" werden zeitgesteuert verarbeitet und enthalten noch keine Daten.

Zieloption	Beschreibung
BI-Posteingang	Sendet das Objekt an den BI-Launchpad-Posteingang eines Benutzers.
E-Mail	Sendet das Objekt an die E-Mail-Adresse eines Benutzers.
FTP-Adresse	Sendet das Objekt an einen Speicherort auf einem FTP-Server.
SFTP-Adresse	Sendet das Objekt an einen Speicherort auf einem SFTP-Server.

Zieloption	Beschreibung
Dateispeicherort	Sendet das Objekt an einen lokalen Festplattenspeicherort.

> **Hinweis**
>
> Senden Sie Interactive Analysis-Dokumente nur an BI-Posteingänge oder an ein E-Mail-Ziel, das in den Informationsplattformdiensten konfiguriert ist.

> **→ Tipp**
>
> Verwenden Sie `UMSCHALTTASTE` + `Klicken` oder `STRG` + `Klicken`, um mehrere Objekte auszuwählen.

3. Konfigurieren Sie die Zieloption.

   Sie können auswählen, ob Sie die Standardeinstellungen des Adaptive Job Servers oder eigene Einstellungen verwenden möchten. Wenn Sie Ihre eigenen Einstellungen verwenden, können Sie Folgendes angeben:

   - Die Benutzer und Gruppen, die das Objekt empfangen (falls an ein BI-Posteingangs- oder E-Mail-Ziel gesendet)
   - Ob eine Kopie des Objekts oder eine Verknüpfung zum Objekt gesendet werden soll
   - Den Namen des gesendeten Objekts
   - Ob Instanzen nach dem Senden von Objekten bereinigt werden sollen
   - Die Einstellungen für den Zieltyp (z. B. ein Verzeichnis für den Dateispeicherort oder der Hostname und der Verbindungsport für den FTP- bzw. SFTP-Server)
4. Klicken Sie abschließend auf *Senden*.

16.9 Ändern der Eigenschaften von Objekten

1. Wählen Sie im Verwaltungsbereich *Ordner* der CMC ein Objekt aus.
2. Klicken Sie auf *Verwalten* > *Eigenschaften*.
   Das Dialogfeld *Eigenschaften* wird angezeigt.
3. Nehmen Sie Ihre Änderungen vor.

   Sie können Objektnamen, Schlüsselwörter und Beschreibung ändern.
4. Klicken Sie abschließend auf *Speichern und schließen*.

16.10 So überprüfen Sie die Beziehungen eines Objekts

1. Navigieren Sie zu dem Objekt, für das Sie die Beziehungsabfrage ausführen möchten.
2. Klicken Sie auf *Verwalten* > *Extras* > *Beziehungen überprüfen*.

   Der Bereich *Abfrageergebnisse* wird mit den Ergebnissen der Beziehungsabfrage angezeigt.

> → Tipp
>
> Überprüfen Sie ggf. weitere Beziehungen von Ergebnisobjekten, indem Sie ein Objekt und dann *Verwalten* > *Extras* > *Beziehungen überprüfen* auswählen.

3. Um zur ursprünglichen Abfrage zurück zu navigieren, wählen Sie den Namen des Objekts aus dem Strukturbereich aus.

16.11 Erstellen eines neuen Hyperlinks

1. Navigieren Sie im Bereich *Ordner* oder *Persönliche Ordner* zu dem Ordner, in dem Sie einen neuen Hyperlink erstellen möchten.
2. Klicken Sie auf *Verwalten* > *Neu* > *Hyperlink*.
   Das Dialogfeld *Hyperlink* wird angezeigt.
3. Geben Sie für den Hyperlink einen Titel, eine Beschreibung und Schlüsselwörter ein.
4. Klicken Sie im Navigationsbereich auf *URL*.
5. Geben Sie in das Feld *URL* die URL ein.
6. Klicken Sie auf *OK*.

17 Berichte

17.1 Auswählen der Regenerierungsoptionen für einen Bericht

Regenerierungsoptionen können nur in Crystal Reports-Berichten festgelegt werden.

> → Tipp
>
> Klicken Sie auf *Bericht regenerieren*, um den Bericht sofort zu regenerieren.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Markieren Sie einen Bericht und wählen anschließend *Aktionen* > *Regenerierungsoptionen*.
3. Wählen Sie im Dialogfeld *Regenerierungsoptionen* die zu regenerierenden Berichtselemente in der `.rpt`-Quelldatei aus.
4. Klicken Sie auf *Aktualisieren*.

17.2 Auswählen von Berichtanzeigeoptionen für einen Crystal-Reports-Bericht

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie den Bericht aus, für den Anzeigeoptionen festgelegt werden sollen.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Anzeigeserver-Gruppe*.
5. Wählen Sie unter *Datenregenerierung für die Anzeige* die Option *Berichtspezifische Anzeigeeinstellungen verwenden*, und wählen Sie Optionen für den Bericht aus.
6. Klicken Sie auf *Speichern und schließen*.

17.3 Auswählen der Standardserver zum Verarbeiten eines Objekts

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Berichtsobjekt aus, für das die Standardserver angegeben werden sollen.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.

4. Führen Sie im Dialogfeld *Standardeinstellungen* einen der folgenden Schritte aus:
   - Um die Standardserver für die zeitgesteuerte Verarbeitung eines Berichtsobjekts anzugeben, wählen Sie in der Navigationsliste *Zeitsteuerungsserver-Gruppe*.
   - Zum Angeben der Standardserver für die Verarbeitung eines Objekts, das Sie anzeigen, wählen Sie in der Navigationsliste *Anzeigeserver-Gruppe*, wenn das Objekt ein Crystal-Reports-Bericht ist, oder *Web-Intelligence-Prozesseinstellungen*, wenn das Objekt ein Web-Intelligence-Dokument ist.
5. Klicken Sie auf *Speichern und schließen*.

17.4 Ändern der Datenbankeinstellungen in Crystal-Reports-Berichten

Sie können den Datenbanktyp auswählen, Standarddatenbank-Anmeldeinformationen festlegen, die Datenquelle bzw. die Datenquellen für ein Crystal-Reports-Berichtsobjekt und seine Instanzen anzeigen und Benutzer optional beim Anzeigen einer Crystal-Reports-Berichtsinstanz zur Eingabe eines Anmeldenamens und -kennworts auffordern.

Wenn Sie mehrere Berichtsobjekte auswählen, um die Datenbankeinstellungen zu ändern, werden nur die Berichtsobjekte aktualisiert, die über dieselbe Datenquellenverbindung verfügen. Informationen über unterstützte Datenbanken und Treiber finden Sie im Dokument "Supported Platforms" (Unterstützte Plattformen) im SAP Service Marketplace.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Berichtsobjekt aus, für das die Datenbankeinstellungen geändert werden sollen.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Datenbankkonfiguration*.
5. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie *Ursprüngliche Datenbank-Anmeldeinformationen aus dem Bericht verwenden*, und geben Sie einen Benutzernamen und ein Kennwort für die ursprüngliche Berichtsdatenbank ein.
   - Wählen Sie *Hier angegebene benutzerdefinierte Datenbank-Anmeldeinformationen verwenden*, und geben Sie einen Servernamen (oder einen DSN für eine ODBC-Datenquelle, einen Datenbanknamen, einen Benutzernamen und ein Kennwort für die vordefinierten Datenbanktreiber oder für einen benutzerdefinierten Datenbanktreiber ein. Wenn Sie das Standardtabellenpräfix in Ihrer Datenbank geändert haben, geben Sie ein benutzerdefiniertes Tabellenpräfix an.
6. Führen Sie eine der folgenden Aktionen aus:
   - Um Benutzer beim Regenerieren eines Berichts zur Eingabe eines Kennworts aufzufordern, wählen Sie *Benutzer zur Datenbankanmeldung auffordern*.
     Die Benutzer werden beim ersten Regenerieren eines Berichts von der BI-Plattform aufgefordert. Wenn die Benutzer den Bericht erneut regenerieren, werden sie nicht aufgefordert. Diese Option wirkt sich nicht auf zeitgesteuerte Instanzen aus.
   - Um die Anmeldeinformationen und das Kennwort des Benutzers zum Anmelden an der Datenbank zu verwenden, wählen Sie *SSO-Kontext für Datenbankanmeldung verwenden*.
     Die BI-Plattform muss für die End-to-End-Einzelanmeldung oder für die Einzelanmeldung an der Datenbank konfiguriert werden. Weitere Informationen finden Sie im *Handbuch für die Implementierung von Webanwendungen* für SAP BusinessObjects Business Intelligence.

- Um die gleichen Datenbankanmeldeinformationen zu verwenden, die auch bei Ausführung des Berichts auf dem Job Server verwendet wurden, wählen Sie *Dieselbe Datenbankanmeldung wie beim Ausführen des Berichts verwenden*.
- Um die für das Benutzerkonto festgelegten Datenbankanmeldeinformationen zu verwenden, wählen Sie *Benutzeranmeldedaten für Datenbank zur Datenbankanmeldung verwenden*.

7. Klicken Sie auf *Speichern und schließen*.

17.5 Aktualisieren der Standardparameterwerte für einen Crystal-Reports-Bericht

Wenn ein Crystal Reports-Bericht Parameter enthält, können Sie den Standardwert für jeden Parameter festlegen. Die Standardwerte werden beim Generieren einer Berichtsinstanz verwendet.

Über Parameterfelder (mit voreingestellten Werten) können Benutzer Daten in der BI-Plattform anzeigen und festlegen, welche Daten in der BI-Plattform angezeigt werden sollen. Bei Verwendung einer BI-Plattform-Anwendung wie BI-Launchpad können die Benutzer einen Bericht mit den Standardwerten öffnen oder andere Werte auswählen. Wenn Sie keinen Standardwert angeben, werden Benutzer bei der zeitgesteuerten Verarbeitung des Berichts zur Eingabe eines Werts aufgefordert.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Crystal Reports-Berichtsobjekt, für das die Standardeingabeaufforderungswerte aktualisiert werden sollen.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Eingabeaufforderungen*.

   Diese Option ist nur verfügbar, wenn ein Berichtsobjekt Parameter enthält. Andernfalls ist diese Option nicht verfügbar; überspringen Sie diesen Schritt.
5. Wählen Sie in der Spalte *Standardwert* einen Standardwert für den Parameter aus.

   Die Optionen zum Ändern des Standardwerts werden angezeigt. Je nach Art des Parameterwerts können Sie einen Wert direkt in das Feld eingeben oder aus einer Liste auswählen.
6. Klicken Sie auf die Schaltfläche *Wert bereinigen*, um den aktuellen Wertesatz für den Parameter zu bereinigen.
7. Aktivieren Sie das Kontrollkästchen *Bei Anzeige auffordern*, damit Benutzern eine Eingabeaufforderung angezeigt wird, bevor Sie eine Berichtsinstanz in einer BI-Plattformanwendung anzeigen können.
8. Klicken Sie auf *Speichern und schließen*.

17.6 Aktualisieren der Eingabeaufforderungen für ein Web-Intelligence-Dokument

Wenn ein Bericht Parameter enthält, können Sie den Standardeingabeaufforderungswert für jeden Parameter festlegen. Der Standardwert wird beim Generieren einer Berichtsinstanz verwendet.

Über Eingabeaufforderungsfelder (mit voreingestellten Werten) können Benutzer Daten angeben, die angezeigt werden sollen. In einer BI-Plattform-Anwendung wie BI-Launchpad können die Benutzer den Bericht entweder mit den vorgegebenen Standardwerten verwenden oder andere Werte auswählen. Wenn Sie keinen Standardwert angeben, werden Benutzer bei der zeitgesteuerten Verarbeitung des Berichts zur Eingabe eines Werts aufgefordert.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Web-Intelligence-Dokument aus, für das Eingabeaufforderungen aktualisiert werden sollen.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Eingabeaufforderungen*.

   Diese Option wird nur angezeigt, wenn das Web-Intelligence-Dokumentobjekt Eingabeaufforderungen enthält. Andernfalls ist diese Option nicht verfügbar.
5. Klicken Sie auf *Ändern*.
6. Wählen Sie eine Eingabeaufforderung, und geben Sie einen Wert dafür ein.

   Wenn die verfügbaren Werte nicht angezeigt werden, klicken Sie auf die Schaltfläche *Werte regenerieren*.
7. Wiederholen Sie die Schritte 5 und 6 für jeden Eingabeaufforderungswert, den Sie ändern möchten.
8. Klicken Sie auf *Anwenden* und anschließend auf *Speichern und schließen*.

Weitere Informationen

Aktualisieren der Standardparameterwerte für einen Crystal-Reports-Bericht [Seite 275]

17.7 Verwenden von Filtern

Filter können nur für manche Berichttypen angewendet werden. Filter können beispielsweise nicht in Web-Intelligence-Dokumenten, Crystal-Reports-Berichten im Format `.rptr` oder Berichten, die in SAP Crystal Reports für Enterprise erstellt wurden, verwendet werden.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Berichtsobjekt, dem Filter hinzugefügt werden sollen.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Filter*.
5. Um Auswahlformeln zu aktualisieren oder neue hinzuzufügen, führen Sie eine der folgenden Aktionen durch:
   - Erstellen oder bearbeiten Sie im Feld *Datensatzauswahl* eine oder mehrere Datensatzauswahlformeln, die die Datensätze für die zeitgesteuerte Verarbeitung von Berichten einschränken.
   - Erstellen oder bearbeiten Sie im Feld *Gruppenauswahl* eine oder mehrere Gruppenauswahlformeln, die die Gruppen für die zeitgesteuerte Verarbeitung von Berichten einschränken.
6. Klicken Sie auf *Speichern und schließen*.

17.8 Auswählen eines Druckers für Crystal-Reports-Berichte

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Berichtsobjekt, dem ein Drucker zugeordnet werden soll.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Druckeinstellungen*.
5. Aktivieren Sie unter *Druckeinstellungen* das Kontrollkästchen *Crystal Reports-Berichte bei zeitgesteuerter Verarbeitung drucken*.

   Die Crystal-Reports-Berichte werden im SAP-Crystal-Reports-Format an den Drucker gesendet. Dieses Format kollidiert nicht mit dem von Ihnen bei der Zeitsteuerung des Berichts ausgewählten Seitenlayout.
6. Geben Sie im Feld *Anzahl der Exemplare* die Anzahl der Kopien ein, die gedruckt werden sollen.
7. Wählen Sie unter *Seitenbereich* die Option *Alle* aus, um alle Seiten des Berichts zu drucken, oder wählen Sie *Seiten* und geben in den Feldern die erste und die letzte zu druckende Seite ein.
8. Führen Sie in der Liste *Sortieroption setzen auf* folgende Schritte aus:
   - Wählen Sie *Sortieren*, um den Bericht zu sortieren.
   - Wählen Sie *Nicht sortieren*, wenn Sie den Bericht nicht sortieren möchten.
   - Wählen Sie *Druckerstandardwerte verwenden*, um die Standardsortiereinstellung des Druckers zu verwenden.
9. Führen Sie in der Liste *Seitenskalierung* folgende Schritte aus:
   - Wählen Sie *Passend skalieren*, um die Berichtsseite proportional zu skalieren, um sie an die ausgedruckte Seite anzupassen.
   - Wählen Sie *Nur an Größe anpassen*, um die Berichtsseite zu verkleinern, um sie an die ausgedruckte Seite anzupassen.
   - Wählen Sie *Nicht skalieren*, wenn Sie den Bericht nicht skalieren möchten.
10. Aktivieren Sie das Kontrollkästchen *Seite zentrieren*, um den Bericht auf der gedruckten Seite zu zentrieren.
11. Aktivieren Sie das Kontrollkästchen *Horizontale Seiten an eine Seite anpassen*, um horizontale Seiten an eine gedruckte Seite anzupassen.
12. Führen Sie unter *Seitenlayout angeben* einen der folgenden Schritte aus:
    - Wählen Sie *Standarddrucker*, um auf dem Standarddrucker des Crystal Reports Job Servers auszudrucken.
    - Wählen Sie *Drucker angeben*, und geben Sie den Pfad und Namen des Druckers in das Feld ein. Wenn Ihr Jobserver unter Windows läuft, geben Sie **`\\<PrintServer>\<PrinterName>`** ein, wobei `<PrintServer>` der Name des Druckerservers und `<PrinterName>` der Name des Druckers ist. Falls Ihr Jobserver unter Unix ausgeführt wird, stellen Sie sicher, dass der Unix-Drucker eingeblendet (nicht ausgeblendet) ist, und geben Sie den Druckbefehl ein, den Sie normalerweise verwenden, wie z.B. `lp -d <Druckername>`.
13. Klicken Sie auf *Speichern und schließen*.

17.9 Auswählen von Seitenlayoutoptionen für Crystal Reports-Berichte und PDF-Objekte

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Berichtsobjekt aus, für das Sie das Seitenlayout festlegen möchten.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Druckeinstellungen*.
5. Führen Sie unter *Druckeinstellungen* eine der folgenden Aktionen durch, um den Standarddruckmodus auszuwählen:
   - Wählen Sie *Immer als PDF drucken (Vorschau)*, um beim Drucken des Berichts aus einem Webviewer die PDF-Druckeinstellungen zu verwenden.
   - Wählen Sie *Crystal Reports-Voreinstellung verwenden*, um die in den CMC-Einstellungen definierten standardmäßigen Druckeinstellungen für Crystal-Reports-Berichte zu verwenden.
6. Führen Sie unter *Seitenlayout angeben* in der Liste *Layout einstellen auf:* eine der folgenden Aktionen durch:
   - Wählen Sie *Standard für Berichtsdatei*, um das in Crystal Reports definierte Seitenlayout zu verwenden.
   - Wählen Sie *Angegebene Druckereinstellungen*, um das standardmäßige Seitenlayout des Druckers zu verwenden, und wählen Sie den standardmäßigen Crystal-Reports-Job-Server-Drucker oder einen anderen Drucker aus.
     Sie können zeitgesteuert verarbeitete Berichtsinstanzen nur auf dem unter *Crystal Reports-Berichte bei zeitgesteuerter Verarbeitung drucken* angegebenen Drucker drucken. Das bedeutet, Sie können nicht in einem Bericht das Standardseitenlayout eines Druckers festlegen und ihn dann auf einem anderen Drucker drucken.
   - Wählen Sie *Benutzerdefinierte Einstellungen*, um alle Seitenlayouteinstellungen anzupassen, und wählen Sie die Seitenausrichtung und das Seitenformat aus.
7. Klicken Sie auf *Speichern und schließen*.

17.10 Zuweisen einer Verarbeitungserweiterung zu einem Bericht

Sie können einem einzelnen Berichtsobjekt auch mehrere Verarbeitungserweiterungen zuweisen.

Bevor Sie einem Berichtsobjekt eine Verarbeitungserweiterung zuweisen können, muss die Verarbeitungserweiterung in der CMC registriert werden.

Verarbeitungserweiterungen sind nicht relevant für Web-Intelligence-Dokumente, Crystal-Reports-Berichte im Format `.rptr` oder Berichte, die in SAP Crystal Reports für Enterprise erstellt wurden.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das Berichtsobjekt aus, dem eine Verarbeitungserweiterung zugewiesen werden soll.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.

4. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Erweiterungen*.
5. Wählen Sie in der Liste *Verfügbare Verarbeitungserweiterungen* eine Verarbeitungserweiterung aus, und klicken Sie auf >, um sie in die Liste *Diese Verarbeitungsanforderungen (in angegebener Reihenfolge) verwenden* zu verschieben.

   Die Liste *Verfügbare Verarbeitungserweiterungen* enthält nur registrierte Verarbeitungserweiterungen.
6. Verwenden Sie die Schaltflächen *Nach oben* und *Nach unten*, um die Reihenfolge für die Verwendung der Verarbeitungserweiterungen festzulegen.
7. Klicken Sie auf *Speichern und schließen*.

Die Verarbeitungserweiterungen werden dem Berichtsobjekt zugewiesen.

17.11 Anzeigen einer Miniaturansicht der ersten Seite eines Crystal-Reports-Berichts

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Suchen und wählen Sie den Bericht aus, für dessen erste Seite eine Miniaturansicht angezeigt werden soll.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Miniaturansicht*.
5. Aktivieren Sie das Kontrollkästchen *Bericht-Miniaturansicht anzeigen*.
6. Klicken Sie auf *Speichern und schließen*.

17.12 Hinzufügen von Berichten in das BI-Repository und Hinzufügen von Hyperlinks

Um das Aufbrechen der Hyperlinks zwischen Berichten zu vermeiden, fügen Sie zuerst die Berichte hinzu und erstellen dann die Hyperlinks.

Diese Funktion ist nicht auf Web-Intelligence-Dokumente oder in Crystal Reports für Enterprise erstellte Berichte anwendbar. Weitere Informationen zu den Aufgaben in SAP Crystal Reports erhalten Sie in der SAP-Crystal-Reports-Hilfe.

1. Erstellen Sie in Crystal Reports die Berichte ohne Hyperlinks.
2. Fügen Sie die Berichte zum BI-Plattform-Repository hinzu.
3. Melden Sie sich über Crystal Reports bei der Plattform an.
4. Erstellen Sie Hyperlinks zwischen dem Startbericht und dem Zielbericht.

Crystal Reports legt automatisch fest, ob zwischen den Berichten eine relative oder absolute Verknüpfung erstellt wird. In der BI-Plattform sind relative Verknüpfungen Berichten eines Objektpakets zugewiesen und absolute Verknüpfungen sind einzelnen Berichtsobjekten oder Instanzen zugewiesen.

17.13 Anzeigen von Universen für Web-Intelligence-Dokumente

In der CMC können Sie überprüfen, welche Universen von einem Web-Intelligence-Dokument verwendet werden.

Ein Universum entspricht einer Darstellung der in einer Datenbank verfügbaren Informationen. Sie erstellen unter Verwendung von Objekten in einem Universum Abfragen für Web-Intelligence-Dokumente.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das Web-Intelligence-Dokumentobjekt, für das Universen angezeigt werden sollen.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Berichtsuniversen*.

Es wird eine Liste der vom Dokument verwendeten Universen angezeigt.

17.14 Warnmeldungen zu einem Crystal-Reports-Bericht anzeigen

Sie können Warnmeldungen zu einem Crystal-Reports-Bericht in der Central Management Console (CMC) anzeigen.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Suchen Sie den Ordner oder die Kategorie mit dem Crystal-Reports-Bericht, den Sie anzeigen möchten, und wählen Sie den Bericht aus.
3. Wählen Sie *Weitere Aktionen* > *Warnmeldungen*.

   Das Dialogfeld *Warnmeldungen* wird mit den Instanzen angezeigt, die die Warnmeldung ausgelöst haben.
4. Doppelklicken Sie auf einen Instanztitel, um die Instanz zu öffnen.

18 Programmobjekte

18.1 Festlegen von Befehlszeilenargumenten

Für jedes Programmobjekt können Sie Befehlszeilenargumente angeben, indem Sie den Befehl *Standardeinstellungen* im Menü *Verwalten* verwenden.

Sie können beliebige Argumente angeben, die von der Befehlszeilenschnittstelle des Programms unterstützt werden. Sie werden ohne Analyse direkt auf der Befehlszeile angegeben.

1. Wählen Sie im Verwaltungsbereich *Ordner* der CMC das Programmobjekt aus.
2. Wählen Sie *Verwalten* > *Standardeinstellungen*.
3. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Programmparameter*.
4. Geben Sie im Feld *Argumente* die Befehlszeilenargumente für das Programm ein, und verwenden Sie dabei dasselbe Format wie für die Befehlszeile selbst.

   Wenn Sie in einem Programm mit Schleifenoption den Wert für die Schleife beispielsweise auf 100 festlegen möchten, müssten Sie **`-loops 100`** eingeben.
5. Klicken Sie auf *Speichern und schließen*.

18.2 Festlegen eines Arbeitsverzeichnisses für ein Programmobjekt

1. Wählen Sie im Verwaltungsbereich *Ordner* der CMC das Programmobjekt aus.
2. Wählen Sie *Verwalten* > *Standardeinstellungen*.
3. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Programmparameter*.
4. Geben Sie im Feld *Arbeitsverzeichnis* den vollständigen Pfad des Verzeichnisses ein, das Sie als Arbeitsverzeichnis für das Programmobjekt festlegen möchten.

   Wenn Sie z. B. unter Windows ein Arbeitsverzeichnis mit der Bezeichnung `Arbeitsverzeichnis` erstellt haben, geben Sie **`C:\Arbeitsverzeichnis`** ein. Geben Sie unter UNIX **`/Arbeitsverzeichnis`** ein.
5. Klicken Sie auf *Speichern und schließen*.

18.3 Ändern des Standardarbeitsverzeichnisses für Programmobjekte

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.

2. Wählen Sie den Adaptive Job Server aus, der den Dienst zur zeitgesteuerten Verarbeitung von Programmen hostet.

   Um zu überprüfen, ob ein Adaptive Job Server den Dienst zur zeitgesteuerten Verarbeitung von Programmen hostet, wählen Sie den Server aus und wählen *Verwalten* > *Eigenschaften*.
3. Wählen Sie *Verwalten* > *Eigenschaften*.
4. Geben Sie im Dialogfeld *Eigenschaften* unter *Temporäres Verzeichnis* den vollständigen Pfad zu dem Verzeichnis ein, das als Arbeitsverzeichnis festzulegen ist.
5. Klicken Sie auf *Speichern und schließen*.

18.4 Angeben des Pfads zu externen oder Hilfsdateien

Für einige binäre Dateien, Batchdateien oder Shell-Skripte müssen Sie den Speicherort von externen oder Hilfsdateien angeben.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das ausführbare Programmobjekt aus, für das der Pfad angegeben werden soll.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* auf *Programmparameter*.
5. Geben Sie im Feld *Externe Abhängigkeiten* den vollständigen Pfad der erforderlichen Datei ein, und klicken Sie auf *Hinzufügen*.
6. Um externe Abhängigkeiten zu bearbeiten oder zu entfernen, wählen Sie den Pfad unter *Externe Abhängigkeiten*, und klicken Sie auf *Bearbeiten* oder *Entfernen*.
7. Wiederholen Sie den Schritt 5 für jede externe oder Hilfsdatei, für die der Pfad anzugeben ist.
8. Klicken Sie auf *Speichern und schließen*.

18.5 Laden von externen oder Hilfsdateien auf den File Repository Server

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das ausführbare Programmobjekt, für das Dateien hochgeladen werden sollen.
3. Wählen Sie *Aktionen* > *Zugeordnete Dateien*.
4. Klicken Sie auf *Durchsuchen*, suchen Sie die benötigte Datei, und klicken Sie auf *Datei hinzufügen*.
5. Wiederholen Sie den Schritt 4 für jede zu ladende Datei.
6. Klicken Sie auf *Speichern und schließen*.

18.6 Hinzufügen einer Umgebungsvariablen

In der CMC können Sie ein ausführbares Programmobjekt durch Hinzufügen oder Ändern von Umgebungsvariablen konfigurieren.

Die Standardvariable wird durch Änderungen an einer vorhandenen Umgebungsvariablen übersteuert (d. h., die Änderungen werden der Variablen nicht angefügt). An den Umgebungsvariablen vorgenommene Änderungen wirken sich jedoch nur in der temporären Shell aus, in der die Informationsplattformdienste das Programm ausführen. Beim Beenden des Programms werden daher die Umgebungsvariablen zerstört.

So legen Sie zum Beispiel eine Pfadvariable fest, mit der ein `Bin`-Verzeichnis eines Benutzers an einen vorhandenen Pfad angehängt wird:

- Unter Windows geben Sie ein: **`path=%path%;c:\usr\bin`**
- Unter Unix geben Sie ein: **`PATH=$PATH:/usr/bin`**

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das ausführbare Programmobjekt aus, dem eine Umgebungsvariable angefügt werden soll.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* auf *Programmparameter*.
5. Geben Sie im Feld *Umgebungsvariablen* die Umgebungsvariable als **`<Name>=<Wert>`** ein, und klicken Sie auf *Hinzufügen*.

   `<Name>` ist der Name der Umgebungsvariablen, und `<Wert>` ist der Wert für die Umgebungsvariable. Die Informationsplattformdienste legen die Umgebungsvariablen mit der für das Betriebssystem geeigneten Syntax fest. Unter UNIX müssen Sie jedoch die dort geltenden Konventionen und die Groß- und Kleinschreibung beachten. Beispielsweise müssen unter Unix alle Namenswerte in Großbuchstaben eingegeben werden.
6. Klicken Sie auf *Speichern und schließen*.

18.7 Festlegen der erforderlichen Parameter für Java-Programme

Zum erfolgreichen zeitgesteuerten Verarbeiten und Ausführen eines Java-Programms müssen Sie den Informationsplattformdiensten den Basisnamen der `.class`-Datei bereitstellen, die die IProgramBase-Schnittstelle aus dem SAP BusinessObjects Enterprise Java SDK implementiert.

Die Java-Laufzeitumgebung muss auf allen Rechnern installiert sein, auf denen ein Adpative Job Server ausgeführt wird.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das Java-Programmobjekt aus, für das die erforderlichen Parameter angegeben werden sollen.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Programmparameter*.

5. Geben Sie im Feld *Auszuführende Klasse* den Basisnamen der `.class`-Datei ein, die `IProgramBase` aus dem SAP BusinessObjects Enterprise Java SDK implementiert (`com.businessobjects.sdk.plugin.desktop.program.IProgramBase`). Geben Sie z. B. **`Arius`** ein, wenn der Dateiname `Arius.class` lautet.
6. Klicken Sie auf *Speichern und schließen*.

18.8 Ermöglichen des Zugriffs durch Java-Programme auf andere Dateien

Sie können Java-Programmen den Zugriff auf Dateien erteilen, zum Beispiel auf Java-Bibliotheken auf dem Rechner mit dem Dienst zur zeitgesteuerten Verarbeitung von Programmen.

Die Java-Laufzeitumgebung muss auf allen Rechnern installiert sein, auf denen ein Adpative Job Server ausgeführt wird.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das Java-Programmobjekt aus, dem Sie den Zugriff auf Dateien auf dem Adaptive Job Server gewähren möchten, der den Dienst zur zeitgesteuerten Verarbeitung von Programmen hostet.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Programmparameter*.
5. Geben Sie in das Feld *Klassenpfad* den vollständigen Pfad zu jeder erforderlichen Java-Bibliotheksdatei ein, die auf dem den Dienst zur zeitgesteuerten Verarbeitung von Programmen hostenden Adaptive Job Server abgelegt ist.

   Trennen Sie die Pfade mit dem Klassenpfad-Trennzeichen für Ihr Betriebssystem. Verwenden Sie z. B. unter Windows ein Semikolon und unter Unix einen Doppelpunkt zur Trennung der Pfade.
6. Klicken Sie auf *Speichern und schließen*.

18.9 Festlegen des Benutzerkontos für ein Programmobjekt

Die Java-Laufzeitumgebung muss auf allen Rechnern installiert sein, auf denen ein Adpative Job Server ausgeführt wird.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das ausführbare Programmobjekt aus, für das ein Benutzerkonto festgelegt werden soll.
3. Wählen Sie *Verwalten* > *Standardeinstellungen*.
4. Klicken Sie im Dialogfeld *Standardeinstellungen* in der Navigationsliste auf *Programmanmeldung*.
5. Geben Sie im Feld *Benutzername* und *Kennwort* die Anmeldedaten des Kontos ein, unter dem das Programm ausgeführt werden soll.
6. Klicken Sie auf *Speichern und schließen*.

19 Objektpakete

19.1 Erstellen von Objektpaketen

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC, und navigieren Sie zu dem Ordner, in dem das Objektpaket erstellt werden soll.
2. Klicken Sie auf *Verwalten* > *Neu* > *Objektpaket*.
   Das Dialogfeld *Objektpaket* wird angezeigt.
3. Geben Sie für das Objektpaket einen Titel, eine Beschreibung und Schlüsselwörter ein.
4. Klicken Sie auf *OK*.

Wenn das Objektpaket dem System hinzugefügt wurde, können Sie Eigenschaften, Inhalt, Zeitsteuerungsinformationen, Ziel, Benutzerrechte, Objekteinstellungen und die Benachrichtigung für das Objektpaket ändern. Verwenden Sie dazu die Befehle *Verwalten* > *Eigenschaften* oder *Verwalten* > *Standardeinstellungen*.

19.2 Hinzufügen neuer Objekte zu einem Objektpaket

1. Doppelklicken Sie im Verwaltungsbereich *Ordner* der CMC auf ein Objektpaket.
   Der Inhalt des Objektpakets wird im *Detailbereich* angezeigt.
2. Klicken Sie je nachdem, welche Art von Objekt hinzugefügt werden soll, auf *Verwalten* > *Hinzufügen* > *Lokales Dokument* oder *Programmdatei*.
   Je nach ausgewählter Option werden unterschiedliche Dialogfelder angezeigt.
3. Klicken Sie auf *Durchsuchen*, und wählen Sie das Objekt aus, das Sie hinzufügen möchten.
4. Legen Sie die entsprechenden Eigenschaften fest.

   Wenn Sie ein Programmobjekt hinzufügen, legen Sie den Programmtyp fest, indem Sie auf *Ausführbare Datei*, *Java* oder *Skript* klicken.
5. Klicken Sie auf *OK*.

19.3 Festlegen von Komponentenfehleroptionen für ein Objektpaket

Gehen Sie wie folgt vor, um festzulegen, wie sich ein Komponentenfehler auf ein Objektpaket zur Laufzeit auswirkt.

1. Navigieren Sie im Verwaltungsbereich *Ordner* der CMC zum Objektpaket, und wählen Sie es aus.
2. Klicken Sie auf *Verwalten* > *Standardeinstellungen*.
3. Klicken Sie in der Navigationsliste auf *Komponentenfehler*.
4. Aktivieren oder Deaktivieren Sie das Kontrollkästchen *Fehler bei zeitgesteuertem Paket aufgrund von Fehler bei einzelner Komponente*.
5. Klicken Sie auf *Speichern und schließen*.

20 Zeitgesteuerte Verarbeitung

20.1 Objekt zeitgesteuert verarbeiten

Um schnell die Standardeinstellungen für die zeitgesteuerte Verarbeitung für ein Objekt zu ändern, klicken Sie im Dialogfeld *Zeitgesteuert verarbeiten* auf *Standardeinstellungen*, stellen Sie die Zeitsteuerungsoptionen ein, und klicken Sie auf *Speichern*.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das Objekt aus, das zeitgesteuert verarbeitet werden soll.
3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.

   Das Dialogfeld *Zeitgesteuert verarbeiten* wird mit den Standardeinstellungen für das Objekt angezeigt.
4. Geben Sie einen Titel für die Instanz ein.
5. Klicken Sie auf *Wiederholung*, und wählen Sie ein Wiederholungsmuster aus.
   Wählen Sie beispielsweise *Wöchentlich*, um das Objekt einmal wöchentlich ausführen zu lassen.
6. Geben Sie Ausführungsoptionen und Zeitsteuerungsparameter an.

   > **Hinweis**
   >
   > Die Option *Separate CSV pro Datenprovider generieren* steht derzeit nur für *FTP*- und *Dateisystem*-Ziele zur Verfügung.

   Wählen Sie beispielsweise *Montag*, *Mittwoch* und *Freitag* aus.
7. Klicken Sie auf *Zeitgesteuert verarbeiten*.

Die BI-Plattform erstellt eine zeitgesteuerte Instanz und führt sie entsprechend den von Ihnen angegebenen Zeitsteuerungsinformationen aus. Sie können die zeitgesteuerte Instanz im Dialogfeld *Verlauf* für das Objekt anzeigen.

> **Hinweis**
>
> Sie können einen Bericht auch für mehrere Ziele gleichzeitig zeitgesteuert verarbeiten, wenn Sie den BI-Content in der Central Management Console (CMC) oder im BI-Launchpad zeitgesteuert verarbeiten. Bei Verwendung der CMC werden die von Ihnen ausgewählten Werte die Standardzeitsteuerungswerte im Launchpad.
>
> Weitere Informationen zu Zieloptionen für die zeitgesteuerte Verarbeitung finden Sie unter Zieloptionen für die zeitgesteuerte Verarbeitung [Seite 444].

Weitere Informationen

Wiederholungsmuster [Seite 288]
Ausführungsoptionen für Wiederholungsmuster [Seite 289]

20.1.1 Wiederholungsmuster

Wählen Sie zuerst ein Wiederholungsmuster und anschließend die Ausführungsoptionen für das Wiederholungsmuster aus.

Wiederholungsmuster	Beschreibung
Jetzt	Wenn ein Benutzer auf *Zeitgesteuert verarbeiten* klickt, wird das Objekt ausgeführt.
Einmal	Das Objekt wird einmal ausgeführt. Sie können die Ausführungszeit sowie das Start- und Enddatum festlegen.
Stündlich	Das Objekt wird stündlich ausgeführt. Sie können die Häufigkeit und die Uhrzeit der Objektausführung sowie das Start- und Enddatum festlegen.
Täglich	Das Objekt wird einmal alle `<N>` Tage ausgeführt. Sie können die Häufigkeit und die Uhrzeit der Objektausführung sowie das Start- und Enddatum festlegen.
Wöchentlich	Das Objekt wird wöchentlich ausgeführt. Sie können festlegen, an welchen Tagen und zu welcher Uhrzeit das Objekt ausgeführt wird, und das Anfangs- und Enddatum der Ausführung bestimmen.
Monatlich	Das Objekt wird alle `<N>` Monate ausgeführt. Sie können die Häufigkeit und die Uhrzeit der Objektausführung sowie das Start- und Enddatum festlegen.
Am n-ten Tag des Monats	Das Objekt wird am `<n-ten>` Tag jedes Monats ausgeführt. Sie können den Tag des Monats und die Uhrzeit der Ausführung sowie ein Start- und Enddatum festlegen.
Am ersten Montag des Monats	Das Objekt wird jeden Monat am ersten Montag ausgeführt. Sie können die Ausführungszeit sowie das Start- und Enddatum festlegen.
Am letzten Tag des Monats	Das Objekt wird jeden Monat am letzten Tag ausgeführt. Sie können ein Start- und Enddatum festlegen.
Tag x der n-ten Woche des Monats	Das Objekt wird jeden Monat an einem bestimmten Tag einer bestimmten Woche ausgeführt. Sie können die Woche und den Tag, die Uhrzeit und das Start- und Enddatum der Ausführung festlegen.
Kalender	Das Objekt wird an den in einem Kalender angegebenen Daten ausgeführt.
Geschäftszeiten	Das Objekt wird an den Wochentagen und zu den Zeiten ausgeführt, die unter *Werktage* und *Geschäftszeiten* angegeben sind.

Weitere Informationen

Ausführungsoptionen für Wiederholungsmuster [Seite 289]

20.1.2 Ausführungsoptionen für Wiederholungsmuster

Wählen Sie zuerst ein Wiederholungsmuster und anschließend die Ausführungsoptionen für das Muster aus. Nicht alle Ausführungsoptionen sind für alle Objekte verfügbar. Wenn Sie eine Ausführungsoption auswählen, die eine Variable enthält, zeigt die BI-Plattform den Standardwert der Variablen an. Sie können die Standardwerte nach Bedarf ändern.

Ausführungsoption für Wiederholungsmuster	Beschreibung
Startdatum/-zeit	Diese Listen werden für alle Wiederholungsmuster angezeigt außer *Jetzt* und *Kalender*. Wählen Sie die Uhrzeit (Stunde, Minute und AM oder PM) sowie das Datum aus, an dem die Ausführung des Objekts gestartet werden soll. Die BI-Plattform führt das Objekt gemäß dem angegebenen Zeitplan sobald wie möglich nach dem Startzeitpunkt aus. Als Standardwert werden aktuelles Datum und aktuelle Uhrzeit verwendet. Wenn Sie als Startzeit beispielsweise einen Zeitpunkt drei Monate nach dem aktuellen Zeitpunkt angeben, wird das Objekt von der BI-Plattform erst zu diesem Startdatum ausgeführt, auch wenn alle anderen Kriterien erfüllt sind. Nach dem Startdatum führt die BI-Plattform den Bericht zu der angegebenen Uhrzeit aus.
Enddatum/-zeit	Diese Listen werden für alle Wiederholungsmuster angezeigt außer *Jetzt* und *Kalender*. Wählen Sie die Uhrzeit (Stunde, Minute) sowie AM oder PM und das Datum aus, an dem die Ausführung des Objekts gestoppt werden soll. Wenn die Endzeit verstrichen ist, wird das Objekt von der Plattform nicht mehr ausgeführt. Der Standardwert entspricht dem aktuellen Zeitpunkt und einem Datum in ferner Zukunft. So wird sichergestellt, dass ein Objekt auf unbestimmte Zeit in dieser Form ausgeführt wird.
Stunde (n) und *Minute (x)*	Diese Listen werden angezeigt, wenn Sie das Wiederholungsmuster *Stündlich* auswählen. Wählen Sie ein Intervall (in Stunden und Minuten) aus, in dem das Objekt ausgeführt werden soll. Wenn Sie keinen Wert für <n> oder <x> eingeben, wird der Bericht von der BI-Plattform jede Stunde ausgeführt.

Ausführungsoption für Wiederholungsmuster	Beschreibung
Tage (n)	Dieses Feld wird angezeigt, wenn Sie das Wiederholungsmuster *Täglich* auswählen. Geben Sie das Intervall (in Tagen) ein, in dem das Objekt ausgeführt werden soll. Wenn Sie keinen Wert für <n> eingeben, wird der Bericht von der BI-Plattform jeden Tag ausgeführt.
Montag, *Dienstag*, *Mittwoch*, *Donnerstag*, *Freitag*, *Samstag* und *Sonntag*	Diese Kontrollkästchen werden angezeigt, wenn Sie das Wiederholungsmuster *Wöchentlich* und *Geschäftszeiten* auswählen. Aktivieren Sie das Kontrollkästchen neben jedem Wochentag, an dem der Auftrag ausgeführt werden soll.
Monat (n)	Dieses Feld wird angezeigt, wenn Sie das Wiederholungsmuster *Monatlich* auswählen. Geben Sie das Intervall (in Monaten) ein, in dem das Objekt ausgeführt werden soll. Wenn Sie keinen Wert für <n> eingeben, wird der Bericht von der BI-Plattform jeden Monat ausgeführt.
Tag (n)	Dieses Feld wird angezeigt, wenn Sie das Wiederholungsmuster *Am n-ten Tag des Monats* auswählen. Wählen Sie den Tag des Monats aus, an dem das Objekt ausgeführt werden soll. Wenn Sie keinen Wert für <n> auswählen, wird der Bericht von der BI-Plattform jeden Tag ausgeführt.
Woche (n) und *Tag (x)*	Diese Listen werden angezeigt, wenn Sie das Wiederholungsmuster *Tag X der N-ten Woche des Monats* auswählen. Wählen Sie die Woche innerhalb des Monats sowie den Wochentag aus, an dem das Objekt ausgeführt werden soll. Wenn Sie keinen Wert für <n> oder <x> eingeben, wird der Bericht von der BI-Plattform jeden Tag ausgeführt.
Geschäftszeiten Beginn	Dieses Feld wird angezeigt, wenn Sie das Wiederholungsmuster *Geschäftszeiten* auswählen. Geben Sie an, wann Ihr Arbeitstag beginnt.
Geschäftszeiten Ende	Dieses Feld wird angezeigt, wenn Sie das Wiederholungsmuster *Geschäftszeiten* auswählen. Geben Sie an, wann Ihr Arbeitstag endet.

20.2 Zeitgesteuerte Verarbeitung eines Objekts mit dem Enterprise-Standardspeicherort als Ziel

Um Instanzen ausschließlich auf dem Output FRS (File Repository Server) – und in keinem anderen Speicherort – zu speichern, wählen Sie *Enterprise-Standardspeicherort* als Ziel.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das Objekt, für das das Standardziel festgelegt werden soll.
3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie auf *Ziele*.
5. Wählen Sie in der Liste *Ziel* die Option *Enterprise-Standardspeicherort*.
6. Klicken Sie auf *Zeitgesteuert verarbeiten*.

20.3 Zeitgesteuertes Verarbeiten eines Objektes für einen Dateispeicherort

Sie können Objekte bei der zeitgesteuerten Verarbeitung so konfigurieren, dass sie an einen nicht verwalteten Datenträger ausgegeben werden. In diesem Fall speichert die BI-Plattform eine Ausgabeinstanz auf dem Output File Repository Server (FRS) und dem angegebenen Ziel.

Bevor Sie ein Objekt für einen Dateispeicherort zeitgesteuert verarbeiten:

- Als Dateispeicherort muss ein lokales Verzeichnis auf dem Verarbeitungsserver angegeben werden. Für unter Windows ausgeführte Server kann das Verzeichnis entweder ein UNC-Pfad (Universal Naming Convention) oder ein lokales Verzeichnis sein.
- Der Dateispeicherort muss auf dem Adaptive Job Server konfiguriert und aktiviert sein.
- Der verarbeitende Server muss über ausreichende Zugriffsrechte für den Dateispeicherort verfügen.

Handelt es sich bei dem Objekt um ein Web-Intelligence-Dokument oder ein Objektpaket, kann kein nicht verwalteter Datenträger als Ziel angegeben werden. Bei einem Objektpaket können Sie jedoch die einzelnen Objekte im Objektpaket für die Ausgabe an einen nicht verwalteten Datenträger konfigurieren.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Objekt für die zeitgesteuerte Verarbeitung aus.
3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie auf *Ziele*.
5. Wählen Sie in der Liste *Ziel* die Option *Dateisystem*.
6. Aktivieren oder deaktivieren Sie das Kontrollkästchen *Instanz im Verlauf beibehalten*.
7. Aktivieren oder deaktivieren Sie das Kontrollkästchen *Standardeinstellungen verwenden*.

   Wenn Sie das Kontrollkästchen *Standardeinstellungen verwenden* aktiviert haben, wechseln Sie zu Schritt 9.
8. Wenn Sie das Kontrollkästchen *Standardeinstellungen verwenden* deaktiviert haben, führen Sie folgende Aktionen durch:

a. Geben Sie in das Feld *Benutzername* einen Benutzernamen mit Zugriffsrechten zum Speichern von Dateien im Zielverzeichnis ein.
b. Geben Sie in das Feld *Kennwort* das für den Zugriff auf das Zielverzeichnis erforderliche Benutzerkennwort ein.
c. Geben Sie in das Feld *Verzeichnis* ein lokales Festplattenverzeichnis, ein zugeordnetes Verzeichnis oder einen UNC-Pfad zu dem Verzeichnis ein, an das die Instanz gesendet werden soll.
d. Wählen Sie unter *Dateiname* die Option *Automatisch generierten Namen verwenden* oder *Spezifischen Namen verwenden*.

> **Hinweis**
>
> Ab BI 4.3 P03 Patch 8 ist es obligatorisch, bei der Zeitsteuerung für ein Dateiziel einen Benutzernamen und ein Kennwort hinzuzufügen. Diese Änderungen entsprechen der im SAP-Sicherheitshinweis 3387498 beschriebenen Anforderung.

9. Klicken Sie auf *Zeitgesteuert verarbeiten*.

20.4 Zeitgesteuertes Verarbeiten von Objekten für einen FTP-Server

Sie können Objekte bei der zeitgesteuerten Verarbeitung so konfigurieren, dass sie an einen FTP-Server ausgegeben werden. Damit die Verbindung mit dem FTP-Server hergestellt werden kann, müssen Sie einen Benutzer angeben, der über die erforderlichen Rechte zum Hochladen auf den Server verfügt. Wenn Sie ein FTP-Ziel angeben, speichert das System eine Ausgabeinstanz sowohl auf dem Output File Repository Server als auch unter dem angegebenen Ziel.

Bevor Sie dieses Ziel verwenden können, muss es auf den Adaptive Job Servern aktiviert und konfiguriert werden.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Objekt für die zeitgesteuerte Verarbeitung aus.
3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie auf *Ziele*.
5. Wählen Sie in der Liste *Ziel* die Option *FTP-Server*.
6. Aktivieren oder deaktivieren Sie das Kontrollkästchen *Instanz im Verlauf beibehalten*.
7. Aktivieren oder deaktivieren Sie das Kontrollkästchen *Standardeinstellungen verwenden*.

   Wenn Sie das Kontrollkästchen aktiviert haben, wechseln Sie zu Schritt 9.
8. Wenn Sie das Kontrollkästchen *Standardeinstellungen verwenden* deaktiviert haben, führen Sie folgende Aktionen durch:
   a. Geben Sie im Feld *Host* die IP-Adresse des Host-Rechners des FTP-Servers ein, an den die Instanz gesendet werden soll.
   b. Geben Sie im Feld *Port* den Port des FTP-Servers ein, an den die Instanz gesendet werden soll.
   c. Geben Sie im Feld *Benutzername* einen Benutzernamen mit Zugriffsrechten zum Hochladen des Objekts auf den FTP-Server ein.
   d. Geben Sie im Feld *Kennwort* das Benutzerkennwort ein, das für den Zugriff auf den FTP-Server erforderlich ist.

e. Geben Sie im Feld *Konto* das Konto ein, das für den Zugriff auf den FTP-Server erforderlich ist.
f. Geben Sie im Feld *Verzeichnis* den Pfad zum FTP-Verzeichnis ein, an das die Instanz gesendet werden soll.
g. Wählen Sie unter *Dateiname* die Option *Automatisch generierten Namen verwenden* oder *Spezifischen Namen verwenden*.

9. Klicken Sie auf *Zeitgesteuert verarbeiten*.

20.5 Zeitgesteuertes Verarbeiten von Objekten für einen SFTP-Server

Sie können Objekte bei der zeitgesteuerten Verarbeitung so konfigurieren, dass sie an einen sicheren FTP-Server (SFTP) ausgegeben werden. Damit die Verbindung mit dem SFTP-Server hergestellt werden kann, müssen Sie einen Benutzer angeben, der über die erforderlichen Rechte zum Hochladen auf den Server verfügt. Wenn Sie ein SFTP-Ziel angeben, speichert das System eine Ausgabeinstanz sowohl auf dem Output File Repository Server als auch unter dem angegebenen Ziel.

Bevor Sie dieses Ziel verwenden können, muss es auf den Adaptive Job Servern aktiviert und konfiguriert werden.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Objekt für die zeitgesteuerte Verarbeitung aus.
3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie auf *Ziele*.
5. Wählen Sie in der Liste *Ziel* die Option *SFTP-Server*.
6. Aktivieren oder deaktivieren Sie das Kontrollkästchen *Instanz im Verlauf beibehalten*.
7. Aktivieren oder deaktivieren Sie das Kontrollkästchen *Standardeinstellungen verwenden*.

   Wenn Sie das Kontrollkästchen aktiviert haben, wechseln Sie zu Schritt 9.
8. Wenn Sie das Kontrollkästchen *Standardeinstellungen verwenden* deaktiviert haben, führen Sie folgende Aktionen durch:
   a. Geben Sie im Feld *Host* die IP-Adresse des Host-Rechners des SFTP-Servers ein, an den die Instanz gesendet werden soll.
   b. Geben Sie im Feld *Port* den Port des SFTP-Servers ein, an den die Instanz gesendet werden soll.
   c. Geben Sie im Feld *Benutzername* einen Benutzernamen mit Zugriffsrechten zum Hochladen des Objekts auf den SFTP-Server ein.
   d. Geben Sie im Feld *Kennwort* das Benutzerkennwort ein, das für den Zugriff auf den SFTP-Server erforderlich ist.
   e. Geben Sie im Feld *Konto* das Konto ein, das für den Zugriff auf den SFTP-Server erforderlich ist.
   f. Geben Sie im Feld *Verzeichnis* den Pfad zum SFTP-Verzeichnis ein, an das die Instanz gesendet werden soll.
   g. Wählen Sie unter *Dateiname* die Option *Automatisch generierten Namen verwenden* oder *Spezifischen Namen verwenden*.
   h. Geben Sie im Feld *Fingerabdruck* den Hostschlüssel-Fingerabdruck des SFTP-Servers ein.
9. Klicken Sie auf *Zeitgesteuert verarbeiten*.

20.6 Zeitgesteuertes Verarbeiten eines Objekts für E-Mails

Wenn Sie das *E-Mail*-Ziel auswählen, speichert die BI-Plattform die Ausgabeinstanz auf dem Output File Repository Server und sendet eine Kopie der Instanz als Anlage an die von Ihnen angegebenen E-Mail-Adressen.

Bevor Sie dieses Ziel verwenden können, muss das *E-Mail*-Ziel (SMTP) auf den Adaptive Job Servern aktiviert und konfiguriert werden.

Crystal-Reports-Berichte und andere Objektinstanzen werden über die E-Mail-Unterstützung für Simple Mail Transfer Protocol (SMTP) an E-Mail-Ziele gesendet.

Die BI-Plattform unterstützt die MIME-Kodierung (Multipurpose Internet Mail Extensions).

1. Wählen Sie in der CMC den Bereich *Ordner* aus.
2. Wählen Sie ein Objekt für die zeitgesteuerte Verarbeitung aus.
3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie auf *Ziele*.
5. Wählen Sie in der Liste *Ziel* die Option *E-Mail* aus.
6. Aktivieren oder deaktivieren Sie das Kontrollkästchen *Instanz im Verlauf beibehalten*.
7. Aktivieren oder deaktivieren Sie das Kontrollkästchen *Standardeinstellungen verwenden*.

   Wenn Sie das Kontrollkästchen *Standardeinstellungen verwenden* aktiviert haben, wechseln Sie zu Schritt 9.
8. Wenn Sie das Kontrollkästchen *Standardeinstellungen verwenden* deaktiviert haben, führen Sie folgende Aktionen durch:
   a. Geben Sie im Feld *Von* die E-Mail-Adresse des Absenders ein.
   b. Geben Sie im Feld *An* die E-Mail-Adressen der Empfänger ein, an die die Instanz gesendet werden soll.
   c. Geben Sie im Feld *Cc* die E-Mail-Adresse der Empfänger ein, an die eine Kopie der E-Mail und der Instanz gesendet werden soll.
   d. Geben Sie im Feld *Bcc* die E-Mail-Adresse der Empfänger von Blindkopien ein, an die eine Kopie der E-Mail und der Instanz gesendet werden soll.
   e. Geben Sie im Feld *Betreff* den Betreff der E-Mail ein.
   f. Im Feld *Nachricht* (Nachrichtentext der E-Mail) können Sie mithilfe des Rich-Text-Editors und einer eigenen Symbolleiste nun den Inhalt Ihrer Nachricht mittels verschiedener Formatierungsoptionen anpassen.

      > **Hinweis**
      >
      > Wenn Sie ein Bild in die E-Mail einfügen, wird das Bild automatisch heruntergeladen, wenn sowohl der Absender als auch der Empfänger Zugriff auf den Bild-Link haben.

   g. Aktivieren oder deaktivieren Sie das Kontrollkästchen *Anlage hinzufügen*.
   h. Wählen Sie unter *Dateiname* die Option *Automatisch generierten Namen verwenden* oder *Spezifischen Namen verwenden*.
9. Klicken Sie auf *Zeitgesteuert verarbeiten*.

Weitere Informationen

Aktivieren oder Deaktivieren von Zielen für einen Job Server [Seite 296]

Einrichten von SMTP über SSL

Um SMTP über SSL einzurichten, muss dasselbe Zertifikat in den Server- und Client-Systemen vorhanden sein.

Um SMTP über SSL einzurichten, führen Sie die folgenden Schritte aus:

1. Wechseln Sie unter Windows zu `<InstallVerz>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. Wechseln Sie zusätzlich für mit der BI-Plattform verbundene Clients zu `<Installverz>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.

   > **Hinweis**
   >
   > Navigieren Sie bei allen anderen unterstützten Plattformen zum entsprechenden Ordner.

2. Geben Sie dem Zertifikat den Namen „certificate.crt“.

   Beispielsweise sendet der Server beim Verbinden mit dem SMTP-Server die Zertifikatsinformationen. Die Zertifikatsinformationen müssen in eine Nur-Text-Datei kopiert werden, die in „certificate.crt“ umbenannt wird. Diese muss im Ordner 'win64_x64' für die Windows-Plattform und für die Clients im Ordner 'win32_86' abgelegt werden.

SMTP über SSL ist nun eingerichtet.

> **Hinweis**
>
> Wenn der Benutzer das Kontrollkästchen *SSL aktivieren* markiert, wird ein sicherer Kanal aktiviert. Damit ist eine sichere SMTP-Übertragung über SSL möglich.

20.7 Zeitgesteuertes Senden von Objekten an BI-Posteingänge von Benutzern

Beim zeitgesteuerten Verarbeiten von Objekten können Sie ein Objekt so konfigurieren, dass seine Instanzen an einen oder mehrere BI-Posteingänge von Benutzern gesendet werden. Die BI-Plattform speichert die Instanz auf dem Output File Repository Server (FRS) und sendet eine Kopie der Instanz an die von Ihnen angegebenen BI-Posteingänge.

Standardmäßig ist das BI-Posteingangsziel auf den Adaptive Job Servern aktiviert und konfiguriert.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Objekt für die zeitgesteuerte Verarbeitung aus.

3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie auf *Ziele*.
5. Wählen Sie in der Liste *Ziel* die Option *BI-Posteingang*.
6. Aktivieren oder deaktivieren Sie das Kontrollkästchen *Instanz im Verlauf beibehalten*.
7. Aktivieren oder deaktivieren Sie das Kontrollkästchen *Standardeinstellungen verwenden*.

   Wenn Sie das Kontrollkästchen *Standardeinstellungen verwenden* aktiviert haben, wechseln Sie zu Schritt 9.
8. Wenn Sie das Kontrollkästchen *Standardeinstellungen verwenden* deaktiviert haben, führen Sie folgende Aktionen durch:
   a. Wählen Sie unter *Verfügbare Empfänger* die Benutzer aus, an die die Instanz gesendet werden soll.
   b. Wählen Sie unter *Zielname* die Option *Automatisch generierten Namen verwenden* oder *Spezifischen Namen verwenden* aus.
   c. Wählen Sie unter *Senden als* die Option *Verknüpfung* oder *Kopieren* aus.
9. Klicken Sie auf *Zeitgesteuert verarbeiten*.

20.8 Aktivieren oder Deaktivieren von Zielen für einen Job Server

Wenn die BI-Plattform einen zeitgesteuerten Bericht oder ein Programmobjekt ausführt, speichert sie die erstellte Ausgabeinstanz standardmäßig auf dem Output File Repository Server (FRS). Wenn Sie ein Ziel (ein anderes als den Enterprise-Standardspeicherort) wählen, für das Sie ein Objekt zeitgesteuert verarbeiten oder an das Sie ein Objekt senden möchten, speichert die BI-Plattform die Ausgabeinstanz auf dem Output FRS und speichert eine Kopie in dem von Ihnen angegebenen Ziel.

Vor der Wahl eines Ziels muss dieses auf den Adaptive Job Servern aktiviert und konfiguriert werden.

Standardmäßig ist das BI-Posteingangsziel auf den Adaptive Job Servern aktiviert und konfiguriert, so dass Sie Berichte und Dokumente verteilen können. Sie können weitere Ziele auf dem Adaptive Job Server aktivieren und konfigurieren.

1. Wechseln Sie zum Verwaltungsbereich *Server* der CMC.
2. Wählen Sie den Adaptive Job Server aus, für den ein Ziel aktiviert oder deaktiviert werden soll.
3. Wählen Sie *Verwalten* > *Eigenschaften*.
4. Klicken Sie im Dialogfeld *Eigenschaften* auf *Ziele*.
5. Führen Sie eine der folgenden Aktionen aus:
   - Um ein Ziel zu aktivieren, wählen Sie es in der Liste *Ziel* aus, klicken auf *Hinzufügen* und konfigurieren es.
   - Um ein Ziel zu deaktivieren, wählen Sie es in der Liste *Ziel* aus und klicken auf *Entfernen*.
6. Klicken Sie auf *Speichern* oder *Speichern und schließen*.

20.9 Zeitgesteuerte Verarbeitung von Objekten auf der Grundlage von Ereignissen

Führen Sie diese Aufgabe durch, damit ein zeitgesteuerter Auftrag nach dem Auftreten eines Ereignisses ausgelöst wird.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das Objekt aus, das auf Grundlage eines Ereignisses ausgeführt werden soll.
3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie in der Navigationsliste auf *Wiederholung*.
5. Wählen Sie in der Liste *Objekt ausführen* eine Ausführungsoption aus.
6. Legen Sie die übrigen Wiederholungsoptionen für das Objekt (Stardatum, Enddatum usw.) nach Bedarf fest.
7. Klicken Sie in der Navigationsliste auf *Ereignisse*.
8. Wählen Sie unter *Verfügbare Ereignisse* mind. ein Ereignis aus, und klicken Sie auf >, um die Ereignisse der Liste *Abzuwartende Ereignisse* hinzuzufügen.

   > **Hinweis**
   >
   > Wählen Sie im Dropdown-Menü die Option *Beliebiges Ereignis*, wenn Sie das zeitgesteuerte Objekt auslösen möchten, nachdem eines der Ereignisse eintritt.

9. Klicken Sie auf *Zeitgesteuert verarbeiten*.

Weitere Informationen

Wiederholungsmuster [Seite 288]
Ausführungsoptionen für Wiederholungsmuster [Seite 289]
Ereignisse und zeitgesteuerte Verarbeitung [Seite 313]

20.10 Zeitgesteuerte Verarbeitung von Objekten zum Auslösen eines Ereignisses

Führen Sie diese Aufgabe durch, damit bei der Ausführung eines zeitgesteuerten Auftrags ein Ereignis ausgelöst wird.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das Objekt aus, das das Ereignis auslösen soll.
3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie in der Navigationsliste auf *Wiederholung*.

5. Wählen Sie in der Liste *Objekt ausführen* eine Ausführungsoption aus.
6. Legen Sie die übrigen Wiederholungsoptionen für das Objekt (Stardatum, Enddatum usw.) nach Bedarf fest.
7. Klicken Sie in der Navigationsliste auf *Ereignisse*.
8. Wählen Sie unter *Verfügbare Ereignisse* mind. ein Ereignis aus, und klicken Sie auf >, um die Ereignisse der Liste *Bei Beendigung auszulösende Ereignisse* hinzuzufügen.

   Sie können nur Zeitsteuerungsereignisse auswählen.
9. Klicken Sie auf *Zeitgesteuert verarbeiten*.

Weitere Informationen

Wiederholungsmuster [Seite 288]
Ausführungsoptionen für Wiederholungsmuster [Seite 289]

20.11 Konfigurieren von Erfolgs- oder Fehlerbenachrichtigungen für eine Instanz

Wenn eine Benachrichtigungsoption verfügbar, aber nicht ausgewählt ist, wird sie als "Nicht verwendet" gekennzeichnet. Wenn ein Benachrichtigungstyp verwendet wird, ist er als "Aktiviert" gekennzeichnet.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Objekt, für das eine Benachrichtigung festgelegt werden soll.
3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie in der Navigationsliste auf *Benachrichtigung*.
5. Um die Audit-Benachrichtigung zu verwenden, klicken Sie auf *Audit-Benachrichtigung* und führen die folgenden Aktionen durch:
   - Um bei erfolgreicher Ausführung eines Auftrags einen Datensatz an die Audit-Datenbank zu senden, aktivieren Sie das Kontrollkästchen *Ein Auftrag wurde erfolgreich ausgeführt*.
   - Um bei Fehlschlagen eines Auftrags einen Datensatz an die Audit-Datenbank zu senden, aktivieren Sie das Kontrollkästchen *Ein Auftrag konnte nicht ausgeführt werden*.
6. Um die E-Mail-Benachrichtigung zu verwenden, klicken Sie auf *E-Mail-Benachrichtigung* und führen folgende Aktionen durch:
   - Um bei erfolgreicher Ausführung eines Auftrags eine E-Mail zu versenden, aktivieren Sie das Kontrollkästchen *Ein Auftrag wurde erfolgreich ausgeführt*.
     Um den Inhalt und die Empfänger der E-Mail anzugeben, wählen Sie *Zu verwendende Werte hier festlegen*, geben Sie die E-Mail-Adressen in die Felder *Von* und *An* ein sowie den Betreff und die Nachricht. Trennen Sie mehrere Adressen oder Verteilerlisten durch Semikolon.
   - Um bei Fehlschlagen eines Auftrags eine E-Mail zu versenden, aktivieren Sie das Kontrollkästchen *Ein Auftrag konnte nicht ausgeführt werden*.

Um den Inhalt und die Empfänger der E-Mail anzugeben, wählen Sie *Zu verwendende Werte hier festlegen*, geben Sie die E-Mail-Adressen in die Felder *Von* und *An* ein sowie den Betreff und die Nachricht. Trennen Sie mehrere Adressen oder Verteilerlisten durch Semikolon.

In der Standardeinstellung wird die Benachrichtigung an die Standard-E-Mail-Adresse des Servers gesendet.

20.12 Einstellen einer Warnungsbenachrichtigung

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Berichtsobjekt, für das Warnungen festgelegt werden sollen.
3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie im Fenster *Zeitgesteuert verarbeiten* auf *Benachrichtigung*.
5. Aktivieren Sie das Kontrollkästchen *Warnungsbenachrichtigung aktivieren*.
6. Wählen Sie *Standardeinstellungen verwenden*, um die Warnungsbenachrichtigung unter Verwendung der Standardeinstellungen des Adaptive Job Servers zu versenden, oder wählen Sie *Benutzerdefinierte Einstellungen* und geben die E-Mail-Einstellungen an.

   Die Standardeinstellungen für den Adaptive Job Server können im Bereich *Server* der CMC geändert werden. Weitere Informationen finden Sie im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.
7. Geben Sie die URL des Viewers ein, den die Empfänger für den Bericht verwenden sollen, oder wählen Sie den Standard-Viewer aus.

   Sie sollten die W3C-Kodierung (World Wide Web Consortium) für die Viewer-URL verwenden. Ersetzen Sie beispielsweise Leerzeichen im Pfad durch `%20`. Weitere Informationen finden Sie unter http://www.w3.org/ .

   Um eine Viewer-URL als Standard festzulegen,wählen Sie *Central Management Console* im Bereich *Anwendungen* des CMC aus, wählen Sie *Aktionen* > *Verarbeitungseinstellungen*, und geben Sie die URL im Feld *URL (muss URL-kodiert sein)* ein.

   Die Viewer-URL wird als Hyperlink in der Warnungsbenachrichtigungs-E-Mail angezeigt.
8. Geben Sie die Höchstanzahl an Warnungsdatensätzen ein, die in einer Warnungsbenachrichtigung eingeschlossen werden sollen.

   Ein Hyperlink in der Warnungsbenachrichtigung führt auf eine Berichtsseite, die die Datensätze enthält, die die Warnung ausgelöst haben.

   Sie geben den Warnungsname und -status in SAP Crystal Reports ein.
9. Klicken Sie auf *Zeitgesteuert verarbeiten*.

20.13 Auswahl eines Ausgabeformats.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.

2. Wählen Sie ein Berichtsobjekt, für das ein Ausgabedateiformat ausgewählt werden soll.
3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie auf *Formate*
5. Wählen Sie ein Ausgabeformat.
   Wählen Sie beispielsweise für einen Crystal-Reports-Bericht unter *Formatoptionen für ausgewähltes Dokument* und für ein Web-Intelligence-Dokument unter *Ausgabeformat* ein Format aus.
6. Legen Sie die übrigen Optionen für die zeitgesteuerte Verarbeitung nach Bedarf fest.
7. Klicken Sie auf *Zeitgesteuert verarbeiten*.

20.14 Wählen eines Cache-Formats für Web-Intelligence-Dokumente

Beim Ausführen eines zeitgesteuerten Web-Intelligence-Dokuments durch die BI-Plattform wird die generierte Instanz auf dem Output File Repository Server (FRS) gespeichert. Wenn Sie ein Cache-Format auswählen, wird die Instanz auf dem entsprechenden Berichtsserver zwischengespeichert. Wenn Sie kein Cache-Format auswählen, kann das System keinen Cache für die Instanz erzeugen.

Die Auswahl eines Cache-Formats ist nur für Web-Intelligence-Dokumente und nicht für Crystal-Reports-Berichte relevant.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Web-Intelligence-Dokumentobjekt aus, für das ein Cache-Format ausgewählt werden soll.
3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie auf *Zwischenspeichern*.
5. Wählen Sie unter *Für die Zwischenspeicherung verfügbare Formate* die Option *Microsoft Excel*, *Standard-HTML* und/oder *Adobe Acrobat* aus.

   Sie können mehrere Formate auswählen.

   Der Cache wird mit den von Ihnen ausgewählten Formaten vorab geladen.
6. Wählen Sie unter *Verfügbare Gebietsschemas* das Gebietsschema aus, mit dem der Cache vorab geladen werden soll, und klicken Sie auf , um das Gebietsschema in die Liste *Ausgewählte Gebietsschemas* zu verschieben.

   Sie können mehrere Gebietsschemas auswählen. Wenn Sie dieses Web-Intelligence-Dokument zeitgesteuert verarbeiten, generiert die Plattform zwischengespeicherte Versionen des Dokuments in diesen Gebietsschemas.

   Der Cache wird mit den von Ihnen ausgewählten Gebietsschemas vorab geladen.
7. Legen Sie die übrigen Optionen für die zeitgesteuerte Verarbeitung nach Bedarf fest.
8. Klicken Sie auf *Zeitgesteuert verarbeiten*.

20.15 Zeitgesteuerte Verarbeitung eines Berichtsobjekts für einzelne Benutzer

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie ein Berichtsobjekt aus, das zeitgesteuert verarbeitet werden soll.
3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie auf *Zeitgesteuerte Verarbeitung für*.
5. Wählen Sie *Nur für mich zeitgesteuert verarbeiten* oder *Für angegebene Benutzer und Benutzergruppen zeitgesteuert verarbeiten*.
6. Wenn Sie *Für angegebene Benutzer und Benutzergruppen zeitgesteuert verarbeiten* ausgewählt haben, navigieren Sie zu den Benutzern oder Benutzergruppen, für die eine zeitgesteuerte Verarbeitung ausgeführt werden soll, treffen Sie eine Auswahl, und klicken Sie auf >, um sie der Liste *Ausgewählt* hinzuzufügen.

   Um einen Benutzer oder eine Gruppe aus der Liste *Ausgewählt* zu entfernen, wählen Sie den Benutzer oder die Gruppe aus, und klicken Sie auf <.
7. Legen Sie die übrigen Optionen für die zeitgesteuerte Verarbeitung fest, und klicken Sie auf *Zeitgesteuert verarbeiten*.

Weitere Informationen

Wiederholungsmuster [Seite 288]
Ausführungsoptionen für Wiederholungsmuster [Seite 289]

20.16 Auswählen eines Servers oder einer Servergruppe für die zeitgesteuerte Verarbeitung von Objekten

Sie können den Server oder die Servergruppe auswählen, auf dem ein zeitgesteuert verarbeitetes Objekt ausgeführt wird. So können Sie den Lastausgleich besser beeinflussen.

Sie können die Servergruppe auswählen, die von der BI-Plattform verwendet wird, wenn ein Benutzer während der Anzeige einer Crystal-Reports-Berichtsinstanz bzw. einer Web-Intelligence-Dokumentinstanz diese regeneriert. Zusätzlich können Sie beispielsweise Programmaufträge auf einer bestimmten Servergruppe ausführen, um die Systemressourcen nicht vollständig auszulasten.

Die Optionen dieser Aufgabe finden Sie unter *Verwalten* > *Standardeinstellungen* nach Auswahl von *Anzeigeserver-Gruppe* (Crystal-Reports-Berichte) bzw. *Web-Intelligence-Prozesseinstellungen* (Web-Intelligence-Dokumente).

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das Objekt aus, das zeitgesteuert verarbeitet werden soll.

3. Wählen Sie *Aktionen* > *Zeitgesteuert verarbeiten*.
4. Klicken Sie in der Navigationsliste auf *Zeitsteuerungsserver-Gruppe*.
5. Wählen Sie den Servertyp aus:
   - Wählen Sie *Ersten verfügbaren Server verwenden*, um das Objekt unabhängig von der verwendeten Servergruppe so schnell wie möglich auszuführen.
   - Wählen Sie *Server der ausgewählten Gruppe bevorzugen*, um einen bestimmten Server in einer Servergruppe zu verwenden, wenn mehr als ein Server verfügbar ist.
   - Wählen Sie *Nur Server der ausgewählten Gruppe verwenden*, um die angegebene Servergruppe zu verwenden, und geben Sie die Servergruppe ein.

   Wenn Sie ein Programmobjekt zeitgesteuert verarbeiten, für das der Zugriff auf lokal gespeicherte Dateien auf einem Adaptive Job Server erforderlich ist, der den Dienst zur zeitgesteuerten Verarbeitung von Programmen hostet, jedoch mehrere Adaptive Job Server vorhanden sind, müssen Sie angeben, auf welchem der Server das Programm ausgeführt werden soll.
6. Aktivieren Sie das Kontrollkästchen *Auf ursprünglicher Website ausführen*, um das Objekt auf der Website, wo es sich befindet, auszuführen.
7. Legen Sie die übrigen Optionen für die zeitgesteuerte Verarbeitung nach Bedarf fest, und klicken Sie auf *Zeitgesteuert verarbeiten*.

20.17 Verwalten von Instanzen für ein Objekt

Führen Sie diese Aufgabe aus, um Instanzen für ein spezifisches Objekt anzuzeigen und zu verwalten. Um Instanzen für alle Objekte anzuzeigen und zu verwalten, verwenden Sie den Instanzen-Manager.

1. Wechseln Sie in den Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das Objekt aus, für das Sie Instanzen verwalten möchten.
3. Wählen Sie *Aktionen* > *Verlauf*.
4. Wählen Sie eine oder mehrere Instanzen.

   Um die Liste zu regenerieren, klicken Sie auf *Regenerieren*. In diesem Fall muss vorab keine Instanz ausgewählt werden.
5. Wählen Sie *Jetzt ausführen*, *Anhalten*, *Fortsetzen*, *Senden an*, *Erneut zeitgesteuert verarbeiten* oder *Löschen*.

   Wenn Sie *Jetzt ausführen* auswählen, wird das Objekt von der BI-Plattform für die sofortige Ausführung verarbeitet. Der zeitgesteuerte Auftrag hat den Status "Ausstehend".

Weitere Informationen

Instanzen-Manager [Seite 303]

20.18 Instanzen-Manager

Mit dem Instanzen-Manager können Sie alle Instanzen in Ihrer BI-Plattform-Implementierung über einen zentralen Ort anzeigen und verwalten.

Mit dem Instanzen-Manager können Sie die folgenden Aufgaben durchführen:

- Suchen spezifischer Instanzen
- Auswählen mehrerer Instanzen und Durchführen von Stapelvorgängen (z. B. unterbrechen, fortsetzen oder löschen)
- Anzeigen ausführlicher Informationen zu einer Instanz
- Diagnostizieren und Beheben von Systemproblemen, die zu Fehlern von Instanzen führen

Die Standardansicht des Instanzen-Managers zeigt alle ausstehenden Instanzen nach Titel sortiert an. Um detaillierte Informationen über eine Instanz anzuzeigen, wählen Sie die Instanz aus und klicken in der Symbolleiste auf das Symbol *Instanzendetails*.

Beispiel: Verwenden des Instanzen-Managers bei der Fehlerbehebung

Ein Administrator meldet sich bei der CMC an, überprüft den Instanzen-Manager und stellt dabei fest, dass mehrere Aufträge fehlgeschlagen sind. Der Administrator filtert die Liste, um nur fehlgeschlagene Aufträge der letzten zwei Tage anzuzeigen, und stellt fest, dass alle scheinbar auf demselben Server ausgeführt wurden. Der Administrator sortiert die Liste nach Server und stellt fest, dass alle fehlgeschlagenen Aufträge auf demselben Server ausgeführt wurden. Der Fehlercode der einzelnen Fehlermeldungen ist identisch. Der Administrator zeigt detaillierte Informationen für eine Instanz an und stellt fest, dass eine Datenbankverbindung unsachgemäß neu konfiguriert wurde. Der Administrator konfiguriert die Datenbankverbindung ordnungsgemäß neu und kehrt zum Instanzen-Manager zurück, um alle fehlgeschlagenen Aufträge neu auszuführen.

20.19 Anzeigen einer Instanz

Sie können auch den Instanzen-Manager für die Anzeige einer Liste der Instanzen nach Status oder Benutzer verwenden.

1. Wechseln Sie in den Verwaltungsbereich *Ordner* der CMC.
2. Wählen Sie das Objekt aus, für das Sie eine Instanz anzeigen möchten.
3. Wählen Sie *Aktionen* > *Verlauf*.
4. Klicken Sie in der Spalte *Instanzenzeit* auf die Instanz, die angezeigt werden soll.

Um alle Spalten in der Standardbreite anzuzeigen, führen Sie einen Bildlauf nach rechts durch. Instanzen können nicht nach den Spalten "Übergabezeit", "Startzeit", "Dauer", "Wiederholung" oder "Ablauf" sortiert werden.

Weitere Informationen

Instanzen-Manager [Seite 303]

20.20 Anhalten einer Instanz

1. Öffnen Sie das Dialogfeld *Verlauf* eines Objekts.
2. Wählen Sie die zeitgesteuerte Instanz, die angehalten werden soll, aus und klicken Sie auf *Anhalten*.

20.21 Fortsetzen einer angehaltenen Instanz

1. Öffnen Sie das Dialogfeld *Verlauf* eines Objekts.
2. Wählen Sie die zeitgesteuerte Instanz, die fortgesetzt werden soll, aus und klicken Sie auf *Fortsetzen*.

20.22 Löschen von Instanzen

Instanzen können bei Bedarf aus einem Objekt gelöscht werden. Sie können sowohl zeitgesteuerte Instanzen – mit dem Status "Wiederkehrend" oder "Ausstehend" – als auch Bericht- oder Programminstanzen löschen, die den Status "Erfolgreich" oder "Fehlgeschlagen" haben.

1. Öffnen Sie das Dialogfeld *Verlauf* eines Objekts.
2. Wählen Sie die zu löschende(n) Instanz(en) aus, und klicken Sie auf *Löschen*.

20.23 Beschränkungen für Instanzen festlegen

Indem Sie Beschränkungen auf Objekt- oder Ordnerebene festlegen, können Sie die regelmäßige Bereinigung veralteter Instanzen automatisieren.

Auf Ebene der Berichtsobjekte können Sie die Anzahl der in der BI-Plattform verbleibenden Instanzen für ein Objekt, einen Benutzer oder eine Benutzergruppe beschränken, und Sie können die Anzahl der Tage des Verbleibs einer Instanz in der Plattform für einzelne Benutzer oder Benutzergruppen beschränken. Auf Objektebene festgelegte Beschränkungen haben Vorrang vor Beschränkungen auf Ordnerebene. (Für den Ordner geltende Beschränkungen gelten somit nicht automatisch für das Objekt.)

Auf Ordnerebene festgelegte Beschränkungen gelten für alle Objekte innerhalb des betreffenden Ordners einschließlich aller Unterordner.

1. Wählen Sie im Verwaltungsbereich *Ordner* der CMC ein Objekt aus.
2. Klicken Sie auf *Aktionen* > *Beschränkungen*.
3. Führen Sie im Dialogfeld *Beschränkungen* einen der folgenden Schritte aus:
   - Um die Anzahl der Instanzen pro Objekt zu beschränken, aktivieren Sie das Kontrollkästchen *Überzählige Instanzen löschen, wenn die Anzahl der Objektinstanzen mehr als N beträgt*, und geben Sie die maximale Anzahl an Instanzen ein, die im System verbleiben sollen.
     Der Standardwert ist 100.
   - Um die Anzahl an Instanzen für bestimmte Benutzer oder Benutzergruppen zu beschränken, aktivieren Sie das Kontrollkästchen *Überzählige Instanzen für die folgenden Benutzer/Gruppen löschen*, klicken auf *Hinzufügen* und wählen die gewünschten Benutzer oder Gruppen aus. Dann klicken Sie auf >, um die ausgewählten Benutzer oder Gruppen in die Liste zu verschieben, klicken auf *OK* und geben in der Spalte *Beschränkung für Instanz* die maximale Anzahl an Instanzen ein.
     Der Standardwert ist 100.
   - Um die Anzahl der Tage, die Instanzen für bestimmte Benutzer oder Benutzergruppen gespeichert werden, zu beschränken, aktivieren Sie das Kontrollkästchen *Instanzen nach N Tagen für die folgenden Benutzer/Gruppen löschen*, klicken auf *Hinzufügen* und wählen die gewünschten Benutzer oder Gruppen aus. Dann klicken Sie auf >, um die ausgewählten Benutzer oder Gruppen in die Liste zu verschieben, klicken auf *OK* und geben in der Spalte *Maximale Anzahl der Tage* das das Höchstalter der Instanzen ein.
     Der Standardwert ist 100.
4. Klicken Sie auf *Aktualisieren*.

Weitere Informationen

Beschränken von Berichtinstanzen auf Ordnerebene [Seite 259]

20.24 Sofortiges Ausführen mehrerer Objekte

Statt einzelne Objekte zeitgesteuert zu verarbeiten, können Sie mit *Jetzt ausführen* von der CMC aus mehrere Objekte ausführen. Wenn Sie Objekte sofort ausführen, werden sie unter Verwendung der standardmäßigen Einstellungen für die zeitgesteuerte Verarbeitung unverzüglich ausgeführt.

1. Wechseln Sie zum Verwaltungsbereich *Ordner* der CMC.
2. Suchen Sie die auszuführenden Objekte, und wählen Sie sie aus.
3. Klicken Sie auf *Aktionen* > *Jetzt ausführen*.

20.25 Auswählen von Sprachen für Berichtsinstanzen

> **Hinweis**
>
> Diese Aufgabe gilt nur für SAP-Crystal-Reports-Berichte.

Befolgen Sie diese Anleitung, wenn Sie Berichtsinstanzen in verschiedenen Sprachen generieren möchten.

1. Klicken Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* auf *Sprachen*.
2. Wählen Sie eine Sprachoption aus.
   - *Bericht im bevorzugten Anzeigegebietsschema zeitgesteuert verarbeiten*
     Mit dieser Option wird der Bericht gemäß dem in den Einstellungen festgelegten bevorzugten Anzeigegebietsschema zeitgesteuert verarbeitet. Außerdem werden Instanzen erstellt, die ausschließlich dieses Gebietsschema verwenden.
   - *Bericht in mehreren Gebietsschemas zeitgesteuert verarbeiten*
     Mit dieser Option wird der Bericht in mehreren Sprachen zeitgesteuert verarbeitet. Bei Wahl dieser Option müssen Sie auch Gebietsschemas auswählen, indem Sie diese aus der Liste *Alle Gebietsschemas* in die Liste *Ausgewählte Instanzgebietsschemas* verschieben.
3. Legen Sie ggf. weitere Parameter für die zeitgesteuerte Verarbeitung fest, und klicken Sie dann auf *Zeitgesteuert verarbeiten*.

21 Kalender

21.1 Erstellen eines Kalenders

Es empfiehlt sich, einen Kalender für Benutzer zu erstellen, der als Vorlage zum Erstellen neuer Kalender verwendet wird. Sie können diesen Vorlagekalender kopieren und bei Bedarf ändern. Sie können beispielsweise einen Standardkalender für Werktage erstellen, der alle Tage als Ausführungstage enthält, die nicht als Wochenende oder Unternehmensferien markiert sind.

1. Wechseln Sie zum Verwaltungsbereich *Kalender* der CMC.
2. Wählen Sie *Verwalten* > *Neu* > *Neuer Kalender*.
3. Geben Sie einen Namen und eine Beschreibung für den Kalender ein, und klicken Sie auf *OK*.

Der Kalender wird zum System hinzugefügt, und Sie können auf der Registerkarte *Datumsangaben* Ausführungstermine hinzufügen.

Weitere Informationen

Termine zum Kalender hinzufügen [Seite 307]

21.2 Termine zum Kalender hinzufügen

Nach dem Erstellen eines Kalenders können Sie Termine im Jahres-, Vierteljahres- oder Monatsformat anzeigen, bevor Sie sie zum Kalender hinzufügen, und Sie können wiederkehrende Termine basierend auf dem Tag des Monats oder der Woche auswählen.

Wenn Sie einen vorhandenen Kalender ändern, prüft die BI-Plattform alle aktuell für die zeitgesteuerte Verarbeitung eingeplanten Instanzen in Ihrem System und aktualisiert automatisch die Objekte, die den Kalender verwenden. Diese werden automatisch aktualisiert und anschließend gemäß der geänderten Terminzeitsteuerung ausgeführt.

1. Wechseln Sie in den Verwaltungsbereich *Kalender* der CMC.
2. Wählen Sie den Kalender aus, dem Termine hinzugefügt werden sollen.
3. Wählen Sie *Aktionen* > *Datumsangaben auswählen*.
4. Wählen Sie das Kalenderformat *Jährlich*, *Quartalsweise* oder *Monatlich* aus.
5. Um einen Kalender mit wiederkehrenden Terminen zu erstellen, wählen Sie*Nach Tag des Monats* oder *Nach Wochentag* aus.
6. Wählen Sie die Tage des Monats aus, an denen der Kalender ausgeführt werden soll.

Klicken Sie zum Entfernen eines Ausführungstags erneut auf den Tag. Um eine Woche oder alle Wochentage eines Monats als Ausführungstage auszuwählen, klicken Sie auf die Zeile oder den Spaltenkopf.

7. Klicken Sie abschließend auf *Speichern*.

21.3 Löschen eines Kalenders

Wenn ein Kalender gelöscht wird, führt die BI-Plattform die in dem gelöschten Kalender eingeplanten Objekte noch ein Mal aus.

Prüfen Sie vor dem Löschen des Kalenders für die Objekte, auf die der Kalender angewendet wurde, die Informationen bezüglich der zeitgesteuerten Verarbeitung. Sie möchten sicherstellen, dass die benötigten Objekte weiterhin ausgeführt werden. Bei Bedarf können Sie für die Objekte einen anderen Kalender oder ein anderes Wiederholungsmuster auswählen.

1. Wechseln Sie zum Verwaltungsbereich *Kalender* der CMC.
2. Wählen Sie den zu löschenden Kalender aus.

   Zur Auswahl mehrerer Kalender halten Sie die `Strg`- oder `Umschalt`-Taste gedrückt und klicken auf die einzelnen Kalender.
3. Wählen Sie *Verwalten* > *Löschen* aus, und klicken Sie auf *OK*.

Weitere Informationen

Objekt zeitgesteuert verarbeiten [Seite 287]

22 Ereignisse

22.1 Ereignisse

Ereignisse entsprechen Kennzeichen oder Prüfpunkten, die Informationen zu Ereignissen oder Aktionen liefern, die auf dem Server auftreten. Die ereignisbasierte zeitgesteuerte Verarbeitung bietet Ihnen zusätzliche Kontrolle für die zeitgesteuerte Verarbeitung von Objekten. Sie können Ereignisse so einrichten, dass Objekte erst nach dem Eintreten eines bestimmten Ereignisses verarbeitet werden.

In der CMC sind die folgenden Ereignisse verfügbar:

Crystal-Reports-Ereignisse

Crystal-Reports-Ereignisse stoßen die Ausführung eines Berichts nur dann an, wenn der auf das Ereignis wartende Bericht bereits eingeplant und zur Ausführung bereit ist. Crystal-Reports-Ereignisse können auf einer neuen Datei basieren, und es können Berichte eingeplant werden, die auf das Anstoßen durch das Ereignis warten.

Benutzerdefinierte Ereignisse

Benutzerdefinierte Ereignisse werden auch als "manuelle Ereignisse" bezeichnet. Jedes benutzerdefinierte Ereignis hat zwei Eigenschaften: den Ereignisnamen und die zugehörige Beschreibung. Mithilfe benutzerdefinierter Ereignisse werden Warnmeldungen an den BI-Posteingang und die E-Mail-ID eines Benutzers gesendet. Benutzerdefinierte Ereignisse geben Ihnen auch die Möglichkeit, die zeitgesteuerte Verarbeitung von Objekten nach dem Anstoßen durch Ereignisse einzuplanen, indem Sie die erforderlichen Bedingungen festlegen.

Überwachungsereignisse

Überwachungsereignisse sind vom System generierte Ereignisse, die sich auf den Servicestatus beziehen. Die Überwachung ist eine in die CMC eingebundene Anwendung, mit deren Hilfe Administratoren den Zustand des Systems überwachen können. Die wichtigsten Aspekte der Überwachung sind Kontrollmodule und Diagnosen.

Mit Kontrollmodulen können Sie Schwellenwerte für mehr als 250 Kennzahlen im System festlegen. Sie werden benachrichtigt, wenn die festgelegten Schwellenwerte über- bzw. unterschritten werden.

> Beispiel
>
> Wenn Sie über ein Kontrollmodul verfügen, das den vom Output FRS beanspruchten Speicherplatz überwacht, werden Sie benachrichtigt, wenn der festgelegte Speicherplatz erreicht wird.

Systemereignisse

Es gibt zwei Arten von Systemereignissen:

- **Dateiereignisse**
  Dateiereignisse basieren auf unter einem bestimmten Pfad gespeicherten Dateien. Ist eine Datei z. B. unter einem der Serverpfade gespeichert, können Sie Berichte gemäß der Einplanung anhand des Dateipfades ausführen. Aus betriebswirtschaftlicher Sicht: Wenn die erforderlichen Tabellen für das Reporting monatlich/wöchentlich/täglich geladen werden, wird durch das Speichern einer Textdatei unter einem Pfad nach dem Laden der Berichte ein Dateiereignis angestoßen.
- **Zeitsteuerungsereignisse**
  Mithilfe von Zeitsteuerungsereignissen werden Berichte oder BI-Objekte sequenziell ausgeführt. Diese Ereignisdefinition enthält drei Aktionen: Erfolg, Misserfolg und Erfolg oder Misserfolg. Der Grund dafür ist, dass des Status eines gerade ausgeführten Objekts zu jedem Zeitpunkt entweder Erfolgreich oder Fehler sein kann.

Benutzerbenachrichtigungen

Benutzerbenachrichtigungen werden von Administratoren dazu verwendet, BI-Endbenutzer, die mit dem BI-Launchpad arbeiten, über wichtige Ereignisse zu bachrichtigen. Administratoren können ausgewählte Benutzer zur geplanten Zeit über kritische Meldungen und andere zugehörige Informationen (z.B. Systemausfallzeiten) benachrichtigen. Die Warnmeldungen werden als Benachrichtigungs-Popup im BI-Launchpad angezeigt, wenn sich der Benutzer anmeldet.

BW-Ereignisse

Auslösende BOE-Ereignisse (Prozessart in einer BW-Prozesskette) stoßen in einem BW-System BW-Ereignisse für Business Intelligence an. Jedes BW-Ereignis enthält einen Ereignisnamen und eine zugehörige Beschreibung. BW-Ereignisse werden verwendet, um die ereignisbasierte zeitgesteuerte Verarbeitung von Berichten zu konfigurieren, die auf BW-Datenquellen basieren. Ein BW-System stößt ein BW-Ereignis an, wenn Systemdaten geändert werden. Mithilfe von BW-Ereignissen werden außerdem Warnmeldungen an den BI-Posteingang und die E-Mail-ID eines Benutzers gesendet.

22.1.1 Benutzerbenachrichtigungen

Mit der Benachrichtigungsfunktion kann ein Administrator von der CMC aus Warnmeldungen an den Benutzer senden. Mit dieser Funktion können Administratoren ausgewählte Benutzer über kritische Meldungen und andere zugehörige Informationen (z. B. Systemausfallzeiten) benachrichtigen. Die Warnmeldungen werden als Benachrichtigungs-Popup oben rechts im BI-Launchpad angezeigt, wenn sich der Benutzer anmeldet.

22.1.1.1 Erstellen eines Benachrichtigungsereignisses

Die Benachrichtigung ist ein zeitgesteuertes Plug-In. Beim Erstellen eines neuen Benachrichtigungsereignisses muss der Administrator das "Start"- und das "End"-Datum sowie die entsprechenden Zeiten angeben.
Der für die Zeitsteuerung zuständige Adaptive-Job-Server erstellt zur festgelegten "Start"-Zeit eine Zeitsteuerungsinstanz. Der AJS sendet die Warnmeldung dann an den Warnungsposteingang im Launchpad. Diese Benachrichtigungen werden oben rechts im BI-Launchpad angezeigt.

Um ein Benachrichtigungsereignis zu erstellen, gehen Sie folgendermaßen vor:

1. Melden Sie sich bei der CMC an.
2. Wählen Sie auf der CMC-Startseite die Option *Ereignisse* aus dem Dropdown-Menü.
3. Führen Sie im Bereich *Ereignisse* links einen Rechtsklick auf *Benutzerbenachrichtigungen* aus, und navigieren Sie zu *Neu* > *Neue Benachrichtigung*.

   Das Popupfenster *Neue Benachrichtigung* wird angezeigt.
4. Um ein Benachrichtigungsmeldung einzuplanen, gehen Sie folgendermaßen vor:
   a. Wählen Sie im Dropdown-Menü *Zeitzone* die entsprechende Zeitzone aus.
   b. Nehmen Sie die erforderlichen Eingaben für *Startdatum/-zeit* vor.
   c. Nehmen Sie die erforderlichen Eingaben für *Enddatum/-zeit* vor.

   > **Hinweis**
   >
   > - Die *End*-Zeit kann nicht vor der *Start*-Zeit liegen.
   > - Die Differenz zwischen der *Start*- und der *End*-Zeit darf 14 Tage nicht überschreiten.
   > - Ungeachtet der gewählten Zeitzone darf die *Start*-Zeit nicht vor der CMS-Serverzeit liegen. Wenn die *Start*-Zeit vor der CMS-Serverzeit liegt, wird die Benachrichtigung nicht angestoßen.

   d. Geben Sie im Feld *Benachrichtigungstitel* einen Titel für die Benachrichtigung ein.

   > **Hinweis**
   >
   > Der *Benachrichtigungstitel* darf nicht länger als 256 Zeichen sein.

   e. Geben Sie im Feld *Beschreibung* eine passende Beschreibung für die Benachrichtigung ein.

   > **Hinweis**
   >
   > Die *Beschreibung* darf nicht länger als 1024 Zeichen sein.

   > **Hinweis**
   >
   > Sie können die Benachrichtigung an die E-Mail-Adresse des Benutzers senden, indem Sie das Kontrollkästchen *Diese Meldung als Benachrichtigung an die E-Mail-ID des Benutzers senden* aktivieren.
5. Wählen Sie *OK*.

Sie haben nun ein Benachrichtigungsereignis angelegt.

> **Hinweis**
>
> Auf der Seite "Benachrichtigungseinstellungen" werden der Zeitpunkt der Erstellung und der Zeitpunkt der Änderung auf der Grundlage der CMS-Serverzeit angezeigt.

Der Administrator kann das automatische Popup des Benachrichtigungsbanners über die Modifizierung der Datei `BIlaunchpad.properties` deaktivieren und die Abfrage deaktivieren, indem er das Feld `Notification.enabled` auf `false` setzt. Um die Benachrichtigungsabfrage standardmäßig zu aktivieren, muss die Eigenschaft `pinger.enabled` in der Datei `global.properties` aktiviert werden. Wenn Abfrage und Pinger nicht aktiviert sind, wird das Benachrichtigungs-Popup nur dann angezeigt, wenn ein Benutzer die Seite aktualisiert, sich zum ersten Mal anmeldet oder sich bei aktivierter Benachrichtigung erneut anmeldet.

Die Abfrage wird im Intervall von 3 Minuten über das BI-Launchpad ausgeführt.

22.1.1.2 Auswahl einer Benachrichtigungs-Zielgruppe

Die Benachrichtigungsfunktion gibt Ihnen die Möglichkeit, die erforderliche Zielgruppe für jede von Ihnen erstellte Benachrichtigung auszuwählen.

Um die Zielgruppe für eine Benachrichtigung auszuwählen, gehen Sie folgendermaßen vor:

1. Führen Sie einen Rechtsklick auf die erstellte Benachrichtigung aus, und wählen Sie im Kontextmenü *Abonnenten verwalten*.

   Das Popup-Fenster *Abonnenten verwalten* wird angezeigt.
2. Wählen Sie *Hinzufügen* im Bereich *Abonnentenliste*.

   Das Popup-Fenster *Abonnenten hinzufügen* wird angezeigt.
3. Wählen Sie die Benutzer bzw. Benutzergruppen aus, die Sie benachrichtigen möchten.
4. Wählen Sie *Standardabonnements hinzufügen*.

   Das Popup-Fenster *Abonnenten hinzufügen* wird ausgeblendet.
5. Wählen Sie *Sichern und Schließen* im Popup-Fenster *Abonnenten verwalten*.

Sie haben damit die Zielgruppe für eine Benachrichtigung ausgewählt.

ⓘ Hinweis

- Nachdem die Benachrichtigung angestoßen wurde, können Sie die Abonnentenliste nicht mehr ändern.
- Sie können nun Benachrichtigungen an die OpenDocument-Benutzer senden.

22.1.1.3 Bearbeiten eines Benachrichtigungsereignisses

Um ein Benachrichtigungsereignis zu bearbeiten, gehen Sie folgendermaßen vor:

1. Melden Sie sich bei der CMC an.
2. Wählen Sie auf der CMC-Startseite die Option *Ereignisse* aus dem Dropdown-Menü.
3. Wählen Sie im Bereich *Ereignisse* links *Benutzerbenachrichtigungen*.
4. Klicken Sie mit der rechten Maustaste auf die Benachrichtigung, die Sie bearbeiten möchten, und wählen Sie im Kontextmenü *Ereignis bearbeiten*.

Das Dialogfeld *Ereignis bearbeiten* wird angezeigt.

5. Bearbeiten Sie die erforderlichen Parameter des Benachrichtigungsereignisses.

> **Hinweis**
>
> Sie können die folgenden Parameter eines Benachrichtigungsereignisses bearbeiten:
>
> - Zeitzone
> - Startdatum/-zeit
> - Enddatum/-zeit
> - Titel der Benachrichtigung
> - Beschreibung
> - Abonnenten verwalten

6. Wählen Sie *OK*.

Sie haben nun ein Benachrichtigungsereignis angelegt.

> **Hinweis**
>
> Wenn Sie eine Benachrichtigung bearbeiten, indem Sie zu *Ereignisse* > *Benutzerbenachrichtigungen* > *Eigenschaften* navigieren, wird die Benachrichtigung nur dann angestoßen, wenn Sie *OK* auf der Seite *Ereignis bearbeiten* wählen.

22.2 Ereignisse und zeitgesteuerte Verarbeitung

Ereignisse sind Objekte, die Vorkommen im System darstellen.

Sie können abhängig vom Ereignistyp für die Zeitsteuerung, Warnmeldungen oder die Überwachung des Systemstatus verwendet werden. Im Verwaltungsbereich für *Ereignisse* der CMC werden alle Ereignisse nach Ereignistyp in Ordnern organisiert. In jedem Ereignistypordner können Sie Unterordner erstellen, um Ereignisse besser speichern und verwalten zu können.

Die ereignisbasierte zeitgesteuerte Verarbeitung bietet Ihnen zusätzliche Kontrolle über die zeitgesteuerte Verarbeitung von Objekten: Sie können Ereignisse so einrichten, dass Objekte erst nach dem Eintreten eines bestimmten Ereignisses verarbeitet werden. Die Arbeit mit Ereignissen umfasst zwei Schritte: Erstellen eines Ereignisses und zeitgesteuerte Verarbeitung eines Objekts mit Ereignissen. Nachdem Sie also ein Ereignis erstellt haben, können Sie es bei der zeitgesteuerten Verarbeitung eines Objekts als Abhängigkeit auswählen. Der zeitgesteuerte Auftrag wird nur dann verarbeitet, wenn das Ereignis eintritt.

Sie können folgende Ereignistypen für die Verwendung in Verbindung mit der zeitgesteuerten Verarbeitung erstellen:

Ereignistyp	Beschreibung
Dateiereignisse	Wenn Sie ein Dateiereignis festlegen, geben Sie einen Dateinamen an, den der *Event Server* für eine bestimmte Datei überwacht. Wenn die Datei generiert wird, löst der *Event Server* das Ereignis aus. Beispiel: Sie möchten, dass einige Berichte von der regelmäßigen Dateiausgabe anderer Programme oder Skripte abhängig sind. Dateiereignisse werden im Ordner *Systemereignisse* gespeichert.
Zeitsteuerungsereignisse	Wenn Sie ein Zeitsteuerungsereignis festlegen, wählen Sie ein Objekt aus, dessen vorhandenes Wiederholungsintervall als Auslöser für das Ereignis dient. Auf diese Weise können Sie mit Zeitsteuerungsereignissen Eventualitäten oder Bedingungen zwischen zeitgesteuerten Objekten einrichten. Beispiel: Sie möchten, dass bestimmte umfangreiche Berichte nacheinander ausgeführt werden oder dass ein bestimmter Verkaufsgruppenergebnisbericht nur ausgeführt wird, nachdem ein detaillierter Verkaufsbericht erfolgreich ausgeführt wurde. Ereignisse der zeitgesteuerten Verarbeitung werden im Ordner *Systemereignisse* gespeichert.
Benutzerdefinierte Ereignisse	Wenn Sie ein benutzerdefiniertes Ereignis erstellen, erstellen Sie eine Verknüpfung, um ein Ereignis manuell auszulösen. Benutzerdefinierte Ereignisse werden im Ordner *Benutzerdefinierte Ereignisse* gespeichert.

Bei der zeitgesteuerten Verarbeitung mit Ereignissen müssen Sie beachten, dass das Wiederholungsintervall eines Objekts weiterhin bestimmt, wie häufig das Objekt ausgeführt wird. Beispiel: Ein täglicher Bericht, der von einem Dateiereignis abhängt, wird einmal am Tag ausgeführt (sofern die von Ihnen angegebene Datei jeden Tag generiert wird). Darüber hinaus muss das Ereignis innerhalb des Zeitrahmens eintreten, der bei der eigentlichen Planung des ereignisbasierten Berichts aufgestellt wird.

Verwenden Sie Dateiereignisse für Warnmeldungen.

Automatisch erstellte Ereignisse

Das System erstellt automatisch entsprechende Ereignisse, wenn bestimmte Objekttypen (z. B. Crystal-Reports-Berichte) zum Repository hinzugefügt werden.

> ⓘ Hinweis
>
> Sie können diese Ereignistypen im Bereich *Ereignisse* anzeigen. Um diese Ereignistypen zu verwalten oder zu ändern, müssen Sie jedoch Zugriff auf die entsprechende Ereignisquelle oder die relevante Anwendung haben.

Überwachungsereignisse

Um den Gesamtsystemstatus zu überwachen, verfügt die BI-Plattform auch über Audit-Ereignisse. Diese Ereignisse entsprechen den Überwachungsdiagnosen, die im Bereich *Überwachung* erstellt und verwaltet werden.

22.2.1 Erstellen eines dateibasierten Ereignisses

Dateibasierte Ereignisse werden im Ordner *Systemereignisse* gespeichert und verwaltet.

1. Wechseln Sie in den Verwaltungsbereich *Ereignisse* der CMC.
2. Suchen und öffnen Sie den Ordner `Systemereignisse`.
3. Wählen Sie den Pfad *Verwalten* > *Neu* > *Neues Ereignis*.
4. Wählen Sie in der Liste *Typ* die Option *Datei* aus.
5. Geben Sie in das Feld *Ereignisname* einen Namen für das Ereignis ein.
6. Geben Sie in das Feld *Beschreibung* eine Beschreibung ein.
7. Wählen Sie aus der Liste *Server* den Event Server aus, der die angegebene Datei überwachen soll.
8. Geben Sie in das Feld *Dateiname* einen Dateinamen ein.

   Geben Sie den absoluten Pfad zu der Datei, nach der der Event Server suchen soll, ein (Beispiel: `C:\<Ordner>\<Dateiname>` oder `/Home/<Ordner>/<Dateiname>`). Das eingegebene Laufwerk und das Verzeichnis müssen für den Event Server erkennbar sein. Im Idealfall sollte sich das Verzeichnis auf einem lokalen Laufwerk vorhanden sein.
9. Um Warnmeldungen für das Ereignis zu aktivieren, wählen Sie *Warnmeldungen aktiviert* und geben eine Meldung in das Feld *Warnmeldung* ein.

   Bei Auslösung des Ereignisses wird diese Meldung in die gesendete Warnungsbenachrichtigung eingefügt.
10. Klicken Sie auf *OK*.

22.2.2 Erstellen eines Zeitsteuerungsereignisses

Zeitsteuerungsereignisse werden im Ordner *Systemereignisse* gespeichert und verwaltet.

1. Wechseln Sie in den Verwaltungsbereich *Ereignisse* der CMC.
2. Suchen und öffnen Sie den Ordner `Systemereignisse`.
3. Wählen Sie den Pfad *Verwalten* > *Neu* > *Neues Ereignis*.
4. Wählen Sie im Dialogfeld *Neues Ereignis* aus der Liste *Typ* die Option *Zeitgesteuerte Verarbeitung* aus.
5. Geben Sie in das Feld *Ereignisname* einen Ereignisnamen ein.
6. Geben Sie in das Feld *Beschreibung* eine Beschreibung des Ereignisses ein.
7. Wählen Sie für den Ereignisstatus eine der folgenden Optionen:

Ereignisstatus	Beschreibung
Erfolg	Das Ereignis wird nur bei erfolgreichem Abschluss eines angegebenen Objekts ausgelöst.
Fehler	Das Ereignis wird nur bei erfolglosem Abschluss eines angegebenen Objekts ausgelöst.
Erfolg oder Fehler	Das Ereignis wird bei Abschluss eines angegebenen Objekts ausgelöst.

8. Um für das Ereignis die Warnfunktion zu aktivieren, wählen Sie *Warnungen aktiviert* aus.

   Bei Auslösung des Ereignisses wird den Benutzern eine Warnungsbenachrichtigung gesendet.
9. Klicken Sie auf *OK*.

22.2.3 Erstellen eines benutzerdefinierten Ereignisses

Erstellen Sie zuerst ein benutzerdefiniertes Ereignis, nehmen Sie anschließend die zeitgesteuerte Verarbeitung eines Objekts vor, das von dem Ereignis abhängt, bevor Sie darauf das Ereignis auslösen.

1. Wechseln Sie zum Verwaltungsbereich *Ereignisse* der CMC.
2. Suchen und öffnen Sie den Ordner `Benutzerdefinierte Ereignisse`.
3. Wählen Sie den Pfad *Verwalten* > *Neu* > *Neues Ereignis*.
4. Geben Sie in das Feld *Ereignisname* einen Namen für das Ereignis ein.
5. Geben Sie in das Feld *Beschreibung* eine Beschreibung des Ereignisses ein.
6. Um Warnmeldungen für das Ereignis zu aktivieren, wählen Sie *Warnmeldungen aktiviert* und geben eine Meldung in das Feld *Warnmeldung* ein.

   Bei Auslösung des Ereignisses wird diese Meldung in die Warnungsbenachrichtigung eingefügt.
7. Klicken Sie auf *OK*.

Weitere Informationen

Objekt zeitgesteuert verarbeiten [Seite 287]
Aktivieren der Warnmeldungsfunktion für ein Ereignis [Seite 317]

22.2.4 Auslösen eines benutzerdefinierten Ereignisses

1. Wechseln Sie in den Verwaltungsbereich *Ereignisse* der CMC.
2. Suchen und öffnen Sie den Ordner `Benutzerdefinierte Ereignisse`.
3. Wählen Sie ein benutzerdefiniertes Ereignis aus.
4. Wählen Sie den Pfad *Aktionen* > *Auslösendes Ereignis*.

23 Warnmeldungen

23.1 Suchen von Warnungsquellobjekten in der CMC

Warnmeldungsquellen werden je nach Objekttyp an verschiedenen Speicherorten abgelegt. In der folgenden Tabelle wird dargestellt, wie Sie verschiedene Warnmeldungsquellen auffinden.

Objekt (Warnmeldungsquelle)	Speicherort in der CMC
Crystal-Reports-Berichte	Bereich *"Ordner"* oder *"Persönliche Ordner"* Eine Liste aller Crystal-Reports-Berichte im System, die Warnmeldungen unterstützen, steht im Ordner `Crystal-Reports-Ereignisse` im Bereich *Ereignisse* der CMC zur Verfügung. Um eine Warnmeldung zu abonnieren, suchen Sie nach dem jeweiligen Crystal-Reports-Bericht im Bereich *Ordner* oder *Persönliche Ordner*.
Ereignisse (dateibasiert, zeitsteuerungsbasiert und benutzerdefiniert)	Bereich *Ereignisse* Ereignisse sind nach Ereignistyp organisiert. Ereignisse, bei denen Warnmeldungen aktiviert sind, werden durch das Symbol gekennzeichnet.

23.2 Aktivieren der Warnmeldungsfunktion für ein Ereignis

Die Warnmeldungsfunktion ist für Crystal-Reports-Berichte, die Warnmeldungen enthalten, automatisch aktiviert. Das bedeutet, Benutzer können Warnmeldungen zu bestimmten Berichten abonnieren, sobald der betreffende Bericht dem Repository hinzugefügt wurde.

Die Aktivierung von Warnmeldungen für Ereignisse erfordert zusätzliche Schritte, wie etwa die Aktivierung einer Warnmeldung, wenn ein neues Ereignis erstellt wird.

1. Wechseln Sie in den Verwaltungsbereich *Ereignisse* der CMC.
2. Suchen Sie das Ereignis, für das die Warnmeldungsfunktion aktiviert werden soll, und wählen Sie es aus.
3. Wählen Sie *Verwalten* > *Eigenschaften*.
4. Klicken Sie im Dialogfeld *Eigenschaften* im Navigationsbereich auf *Ereigniseinstellungen*.
5. Aktivieren Sie das Kontrollkästchen *Warnungen aktiviert*, und geben Sie im Feld *Warnmeldungstext* eine Nachricht ein, die beim Auslösen der Warnmeldung an die Abonnenten gesendet wird.

   Für Zeitsteuerungsereignisse können Sie keine Nachrichten eingeben.
6. Klicken Sie auf *Speichern und schließen*.

23.3 Abonnieren einer Warnmeldung

1. Wechseln Sie in den Verwaltungsbereich *Ereignisse* der CMC.
2. Suchen Sie die Warnungsquelle, und markieren Sie sie.
3. Wählen Sie *Aktionen* > *Abonnieren*.
4. Wählen Sie im Dialogfeld *Veröffentlichung abonnieren* unter *Ziele* einen Zielort für die Warnmeldung:

Option	Beschreibung
Meine Warnmeldungen	Aktivieren Sie dieses Kontrollkästchen, um die Warnungsbenachrichtigung an ein Ziel im Business-Intelligence-System zu senden (beispielsweise BI-Launchpad).
E-Mail	Aktivieren Sie dieses Kontrollkästchen, um die Warnungsbenachrichtigung an die für Ihr Benutzerkonto in der BI-Plattform festgelegte E-Mail-Adresse zu senden. Dieses Ziel ist nur verfügbar, wenn für Ihr Benutzerkonto eine E-Mail-Adresse angegeben wurde. Vergewissern Sie sich, dass Ihre E-Mail-Adresse gültig und korrekt eingegeben ist. Anderenfalls erhalten Sie die Warnmeldung nicht.

5. Wenn unter *Warnung* mehrere Dokumente aufgeführt sind, aktivieren Sie das Kontrollkästchen für alle Warnungen, die Sie erhalten möchten.
6. Um einen Parameter für die Warnung festzulegen, klicken Sie unter *Parameter* auf *Bearbeiten* und modifizieren den Parameterwert.

   Wenn ein Dokument personalisiert ist, werden die Personalisierungsdetails angezeigt, wenn Sie den Mauszeiger über ein Warnungskontrollkästchen bewegen.
7. Konfigurieren Sie die übrigen Warnungsabonnementoptionen nach Bedarf.

   Je nach Warnungsquelle werden weitere Abonnementoptionen angezeigt. Für Crystal-Reports-Berichte, die mehrere Warnmeldungen enthalten, müssen Sie beispielsweise auswählen, welche Warnmeldungen Sie abonnieren möchten.
8. Klicken Sie auf *OK*.

Wenn die Warnung das nächste Mal ausgelöst wird, wird eine Benachrichtigung an das von Ihnen ausgewählt Ziel gesendet. Um die Warnungsbenachrichtigung an ein anderes Ziel zu senden, wählen Sie die Warnungsquelle und dann *Aktionen* > *Abonnement ändern* aus. Sie können diese Option auch verwenden, um den Crystal-Reports-Bericht auszuwählen, für den eine Warnmeldung abonniert wurde.

Benachrichtigungen werden anhand der Standardzieleinstellung für die Warnungsanwendung versendet, es sei denn, Sie legen benutzerdefinierte Einstellungen für die Warnungsquelle fest.

Weitere Informationen

Verwalten von Warnmeldungseinstellungen für eine Warnungsquelle [Seite 321]
Suchen von Warnungsquellobjekten in der CMC [Seite 317]

23.4 Abonnement einer Warnmeldung aufheben

1. Wechseln Sie in den Verwaltungsbereich *Ereignisse* der CMC.
2. Suchen Sie die Warnungsquelle, und markieren Sie sie.
3. Wählen Sie *Aktionen* > *Abonnement aufheben*.
4. Klicken Sie bei Aufforderung zur Bestätigung im Dialogfeld *Abonnement von Warnmeldungen aufheben* und klicken auf *Abonnement aufheben*.

23.5 Abonnieren einer Warnmeldung für andere Benutzer

1. Wechseln Sie in den Verwaltungsbereich *Ereignisse* der CMC.
2. Suchen Sie die Warnungsquelle, und markieren Sie sie.
3. Wählen Sie *Aktionen* > *Abonnenten verwalten*.
4. Klicken Sie im Dialogfeld *Abonnenten verwalten* im Navigationsbereich auf *Abonnentenliste*.
5. So fügen Sie neue Abonnenten hinzu:
   a. Klicken Sie auf *Hinzufügen*.
   b. Verschieben Sie im Dialogfeld *Abonnenten hinzufügen* Benutzer und Gruppen mithilfe der Schaltfläche > aus der Liste *Verfügbar* in die Liste *Abonniert*, und klicken Sie auf *Standardabonnement(s) hinzufügen*.
   c. Konfigurieren Sie im Dialogfeld *Abonnements bearbeiten* die Warnmeldungs- und Zieloptionen nach Bedarf.

      Sie können beispielsweise angeben, dass andere Warnmeldungen abonniert werden sollen (wenn die Warnmeldungsquelle mehrere Warnmeldungen enthält). Abhängig von der Warnmeldungsquelle können weitere Einstellungen verfügbar sein.
   d. Klicken Sie auf *Speichern und schließen*.
6. So bearbeiten Sie die Einstellungen für einen Abonnenten:
   a. Wählen Sie in der Spalte *Abonnent* einen Benutzer aus, und klicken Sie auf *Bearbeiten*.
   b. Um anzugeben, welche Warnmeldungen der Benutzer erhalten soll, klicken Sie im Dialogfeld *Abonnements bearbeiten* auf *Warnmeldungen* in der Navigationsliste und aktivieren das Kontrollkästchen für alle Warnmeldungen, die Sie für den Benutzer abonnieren möchten.

      Falls die Warnmeldungsquelle mehrere Warnmeldungen enthält, wird jede Warnmeldung aufgelistet. Andernfalls wird nur eine Warnmeldung angezeigt.
   c. Um anzugeben, an welche Ziele eine Warnmeldung gesendet wird, klicken Sie in der Navigationsliste auf *Ziele*, und aktivieren das Kontrollkästchen für jedes Ziel, an das die Warnmeldung gesendet werden soll.

      Nur E-Mail-Ziele, die auf dem Adaptive Job Server aktiviert und konfiguriert sind, sind verfügbar. Falls kein E-Mail-Ziel konfiguriert ist, wird nur das Kontrollkästchen *Meine Warnmeldungen* angezeigt.
   d. Falls verfügbar, konfigurieren Sie nach Bedarf weitere Warnmeldungsoptionen.

      Abhängig von der Warnmeldungsquelle können weitere Optionen verfügbar sein.
   e. Klicken Sie auf *Speichern und schließen*.

7. Klicken Sie im Dialogfeld *Abonnenten verwalten* auf *Speichern & schließen*.

23.6 Aufheben des Abonnements einer Warnung für andere Benutzer

1. Wechseln Sie in den Verwaltungsbereich *Ereignisse* der CMC.
2. Suchen Sie die Warnungsquelle, und markieren Sie sie.
3. Wählen Sie *Aktionen* > *Abonnenten verwalten*.
4. Klicken Sie im Dialogfeld *Abonnenten verwalten* im Navigationsbereich auf *Abonnentenliste*.
5. Wählen Sie einen Benutzer oder eine Benutzergruppe, für den bzw. die das Abonnement von Warnungen aufgehoben werden soll, und klicken Sie auf *Abonnement aufheben*.

23.7 Ausschließen von Benutzern von einer Warnungmeldung

Das Ausschließen von Benutzern ist nützlich, wenn Sie nur einen Teil der Benutzer in einer Gruppe als Abonnenten festlegen möchten. Zuerst abonnieren Sie die gesamte Gruppe, dann schließen Sie Benutzer aus, die keine Warnungsbenachrichtigungen erhalten müssen.

Die Liste *Ausgeschlossen* übersteuert alle anderen Abonnementeinstellungen für einen Benutzer.

1. Wechseln Sie in den Verwaltungsbereich *Ereignisse* der CMC.
2. Suchen Sie die Warnungsquelle, und markieren Sie sie.
3. Wählen Sie *Aktionen* > *Abonnenten verwalten*.
4. Wählen Sie im Navigationsbereich des Dialogfelds *Abonnenten verwalten* die *Abonnentenliste*.
5. Verwenden Sie die Schaltfläche >, um Benutzer oder Gruppen aus der Liste *Verfügbar* in die Liste *Ausgeschlossen* zu verschieben.
6. Klicken Sie auf *Speichern und schließen*.

Weitere Informationen

Suchen von Warnungsquellobjekten in der CMC [Seite 317]

23.8 Verwalten von Warnmeldungseinstellungen für eine Warnungsquelle

Sofern Sie die Warnmeldungseinstellungen für eine Warnungsquelle nicht ändern, werden die Benachrichtigungen mit den Einstellungen für das Standardziel der Warnungsanwendung versendet.

1. Wechseln Sie in den Verwaltungsbereich *Ereignisse* der CMC.
2. Suchen Sie die Warnungsquelle, und markieren Sie sie.
3. Wählen Sie *Aktionen* > *Warnmeldungseinstellungen verwalten*.
4. Um das BI-Launchpad als Ziel zu aktivieren, markieren Sie im Dialogfeld *Warnmeldungseinstellungen verwalten* das Kontrollkästchen *Meine Warnmeldungen aktivieren*.

   Mit dieser Option werden Warnungsbenachrichtigungen an die BI-Launchpad-Konten der Abonnenten gesendet und können von diesen im BI-Launchpad unter *Meine Warnmeldungen* angezeigt werden.
5. Um E-Mail als Ziel zu aktivieren, markieren Sie das Kontrollkästchen *E-Mail aktivieren* und wählen dann *Standard-E-Mail-Einstellungen verwenden* oder *Benutzerdefinierte E-Mail-Einstellungen*.

   Wenn Sie *Standard-E-Mail-Einstellungen verwenden* ausgewählt haben, werden die Standardeinstellungen von den im Bereich *Anwendungen* festgelegten Warnmeldungswerten abgeleitet.
6. Wenn Sie *Benutzerdefinierte E-Mail-Einstellungen* ausgewählt haben, führen Sie folgende Aktionen nach Bedarf durch:
   a. Geben Sie im Feld *Von* eine E-Mail-Absenderadresse ein, oder wählen Sie aus der Liste *Platzhalter hinzufügen* Variablen für die E-Mail-Adresse aus.
   b. Geben Sie im Feld *An* alle E-Mail-Adressen ein, an die Sie Warnungsbenachrichtigungen senden möchten, oder wählen Sie aus der Liste *Platzhalter hinzufügen* Variablen für die E-Mail-Adresse aus.
   c. Geben Sie im Feld *Cc* alle E-Mail-Adressen ein, an die Sie Warnungsbenachrichtigungen senden möchten, oder wählen Sie aus der Liste *Platzhalter hinzufügen* Variablen für die E-Mail-Adresse aus.
   d. Geben Sie im Feld *Bcc* die E-Mail-Adressen aller Empfänger ein, an die Sie Warnungsbenachrichtigungen als Blindkopie senden möchten, oder wählen Sie aus der Liste *Platzhalter hinzufügen* Variablen für die E-Mail-Adresse aus.
   e. Geben Sie im Feld *Betreff* das Thema der Warnungsbenachrichtigung ein, oder wählen Sie aus der Liste *Platzhalter hinzufügen* Variablen für den Betreff aus.
   f. Geben Sie im Feld *Meldung* den Text für den Körper der Warnungsbenachrichtigung ein, oder wählen Sie aus der Liste *Platzhalter hinzufügen* Variablen für die Meldung aus.
   g. Aktivieren Sie das Kontrollkästchen *Anlage hinzufügen*, um eine Anlage zur Warnungsbenachrichtigung hinzuzufügen.
   h. Wählen Sie unter *Dateiname* die Option *Automatisch generierten Namen verwenden* oder *Spezifischen Namen verwenden*. Wenn Sie *Spezifischen Namen verwenden* wählen, geben Sie einen Dateinamen ein, oder wählen Sie einen Platzhalter aus der Liste.
   i. Aktivieren Sie das Kontrollkästchen *Dateierweiterung hinzufügen*, um den Dateinamen automatisch eine Dateierweiterung hinzuzufügen.

      Wenn Sie dem Dateinamen keine Dateierweiterung hinzufügen, kann das Dokument nicht geöffnet werden.
7. Klicken Sie auf *Speichern und schließen*.

Weitere Informationen

Suchen von Warnungsquellobjekten in der CMC [Seite 317]

24 Profile

24.1 Erstellen eines Profils

1. Wechseln Sie zum Verwaltungsbereich *Profile* der CMC.
2. Wählen Sie den Pfad *Verwalten* > *Neu* > *Neues Profil*.
3. Geben Sie im Dialogfeld *Neue Profile erstellen* im Feld *Titel* einen Namen für das Profil ein.
4. Geben Sie im Feld *Beschreibung* eine Beschreibung des Profils ein, und klicken Sie auf *OK*.

24.2 Angeben eines globalen Profilziels für ein Profil

Lokale Profilziele werden während des Veröffentlichungsprozesses angegeben.

1. Wechseln Sie in den Verwaltungsbereich *Profile* der CMC.
2. Suchen Sie nach dem Profil, für das Sie ein Profilziel angeben möchten, und wählen Sie es aus.
3. Wählen Sie *Aktionen* > *Profilziele* aus.
4. Klicken Sie im Dialogfeld *Profilziele* auf *Hinzufügen*.
5. Wählen Sie aus der Liste *Universumname* ein Universum aus.
6. Geben Sie im Feld *Klassenname* einen Klassennamen ein, oder klicken Sie auf *Objekt aus Universum auswählen*.
7. Geben Sie im Feld *Variablenname* einen Variablennamen ein, oder klicken Sie auf *Objekt aus Universum auswählen*.
8. Klicken Sie auf *OK*.

24.3 Angeben eines Profilwerts für einen Benutzer oder eine Gruppe

Sie erzielen dasselbe Ergebnis, wenn Sie mit dem Profil beginnen, für das Sie einen Wert angeben möchten.

Sie können verschiedene Typen von Profilwerten verwenden, z. B. einen statischen Profilwert, einen Ausdruck oder variable Profilwerte für Drittbenutzer und gruppen, die dem System zugeordnet sind.

1. Wechseln Sie zum Verwaltungsbereich *Profile* oder *Benutzer und Gruppen* der CMC.
2. Wählen Sie das Profil aus, für das Sie einen Wert angeben möchten, oder wählen Sie den Benutzer bzw. die Benutzergruppe aus, für den/die Sie einen Profilwert angeben möchten.

3. Wählen Sie *Aktionen* > *Profilwerte* aus.
4. Klicken Sie im Dialogfeld *Profilwerte* auf *Hinzufügen*.
5. Klicken Sie auf *Wählen*.
6. Wählen Sie einen Benutzer oder eine Gruppe bzw. mehrere Benutzer oder Gruppen aus, und klicken Sie auf >, um sie in die Liste auf der rechten Seite zu verschieben.
7. Klicken Sie auf *OK*.
8. Geben Sie einen Profilwert für den ausgewählten Benutzer oder die ausgewählte Gruppe bzw. mehrere Benutzer oder Gruppen ein.
   - Um einen Wert hinzuzufügen, klicken Sie auf *Wert*, geben im Feld *Neuer Wert* einen Wert ein und klicken auf *Hinzufügen*.
     Sie können für einen Benutzer oder eine Gruppe mehrere statische Werte hinzufügen und **%NULL%** als statischen Profilwert verwenden, wenn ein Benutzer oder eine Gruppe nicht über Werte verfügt, die das Profil für die Personalisierung filtern kann.
   - Um einen Filterausdruck zu verwenden, klicken Sie auf *Filterausdruck* und geben im Feld *Web-Intelligence-Formelausdruck* oder *Crystal-Reports-Ausdruck* einen Ausdruck ein. Um das Profil auf mehrere Dokumenttypen anzuwenden, geben Sie in allen drei Feldern Filterausdrücke ein.
     Um einen Web-Intelligence-Ausdruck zu verwenden, geben Sie zuerst ein globales Profilziel für das Profil an.
9. Klicken Sie auf *OK*.

Weitere Informationen

Verwenden von Variablen als Profilwerte [Seite 324]

24.4 Verwenden von Variablen als Profilwerte

Wenn Sie einem Profil einen Benutzer oder eine Benutzergruppe hinzufügen, können Sie einen variablen Profilwert für den vollständigen Namen des Benutzers, den Kontonamen oder die E-Mail-Adresse eingeben.

In der folgenden Tabelle werden die Platzhaltervariablen beschrieben, die Sie für die Externalisierung von Profilen verwenden können.

Variable	Beschreibung
Titel	Verknüpft mit dem Kontonamen eines Benutzers oder einer Benutzergruppe
Vollständiger Name des Benutzers	Verknüpft mit dem vollständigen Namen eines Benutzers oder einer Benutzergruppe

Variable	Beschreibung
E-Mail-Adresse	Verknüpft mit der E-Mail-Adresse eines Benutzers oder einer Benutzergruppe. Wenn Sie die Variable *E-Mail-Adresse* der gemeinsamen E-Mail-Adresse einer Benutzergruppe zuordnen, löst die BI-Plattform die Variable auf und ruft für jedes Mitglied der Gruppe die individuelle E-Mail-Adresse ab.

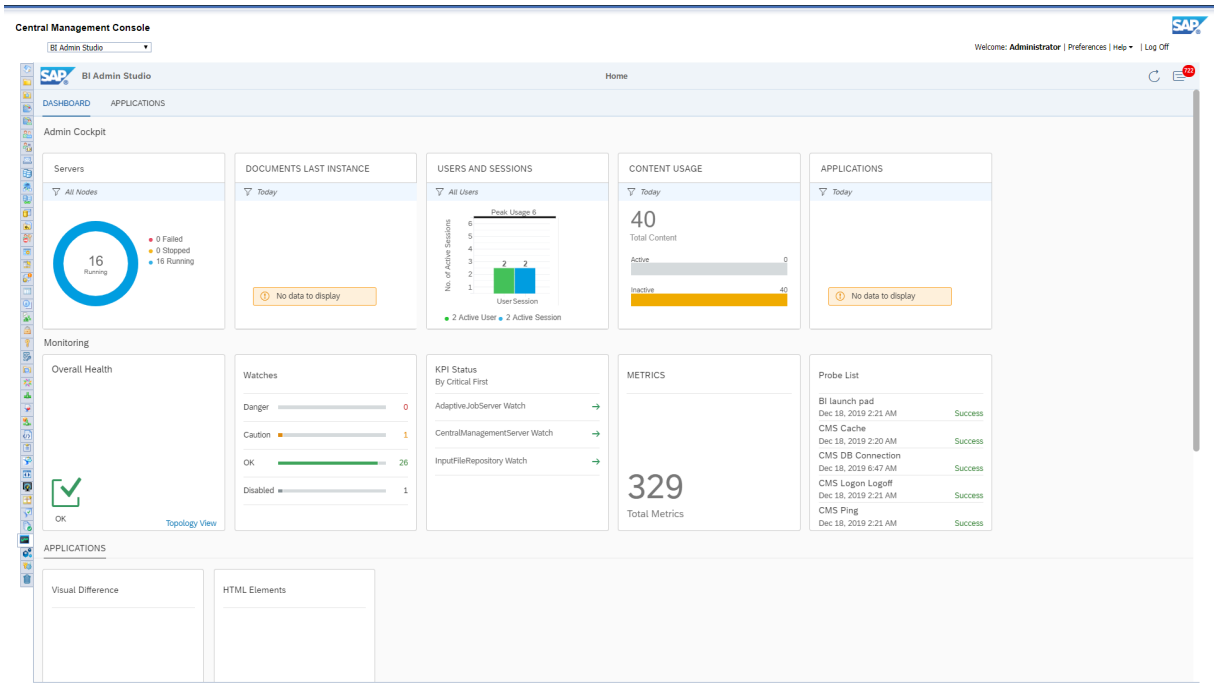
1. Wechseln Sie in den Verwaltungsbereich *Profile* der CMC.
2. Suchen Sie das Profil, dem Sie einen Benutzer oder eine Benutzergruppe hinzufügen möchten, und wählen Sie es aus.
3. Wählen Sie *Aktionen* > *Profilwerte* aus.
4. Klicken Sie im Dialogfeld *Profilwerte* auf *Hinzufügen*.
5. Klicken Sie auf *Wählen*.
6. Wählen Sie den Benutzer oder die Benutzergruppe aus der links angezeigten Liste aus, und klicken Sie auf >, um den Benutzer oder die Gruppe in die rechts angezeigte Liste zu verschieben.
7. Klicken Sie auf *OK*.
8. Klicken Sie auf *Wert*.
9. Wählen Sie aus der Liste *Platzhalter hinzufügen* eine Platzhaltervariable aus, und klicken Sie auf *Hinzufügen*.
   Der Platzhalter wird im Feld *Vorhandene Werte* angezeigt.
10. Klicken Sie auf *OK*.

Wenn Sie das Profil zur Personalisierung einer Veröffentlichung verwenden, wird der Profilwert für den Drittthersteller-Benutzer automatisch anhand der neusten Benutzerinformationen aktualisiert. Wenn sich die E-Mail-Adresse des Benutzers seit der letzten Ausführung der Veröffentlichung geändert hat, ändert sich die für den Profilwert verwendete E-Mail-Adresse beispielsweise bei der nächsten Ausführung der Veröffentlichung.

25 BI-Admin-Studio

BI-Admin-Studio (ehemals BI Administrator Cockpit) ist eine Anwendung in der CMC, die die Überwachung, Warnmeldungen und das Admin-Cockpit kombiniert.

Die Anwendung umfasst zwei Registerkarten: *Dashboard* und *Anwendungen*.



Dashboard

Die Registerkarte *Dashboard* bietet eine Übersicht über die Dashboards, die im *Admin-Cockpit* und in der *Überwachung* zur Verfügung stehen. Sie können auf jedes Dashboard klicken, um detaillierte Informationen darüber zu erhalten. Sie können beispielsweise das *Server*-Dashboard auswählen, um die Liste der Server zu erhalten, die den *Status Wird ausgeführt*, *Gestoppt* und *Fehlgeschlagen* aufweisen, sowie die zugehörigen Details wie *Servername*, *PID* und *Typ*. Weitere Informationen zum Admin-Cockpit erhalten Sie unter Admin-Cockpit [Seite 327], und mehr über die Überwachung erfahren Sie unter Überwachung.

Anwendungen

Über die Registerkarte *Anwendungen* können Sie auf *Grafischer Vergleich* und *Autorisierte HTML-Elemente* zugreifen. Weitere Informationen zu *Grafischer Vergleich* finden Sie unter Grafischer Vergleich [Seite 360], und mehr über *HTML-Elemente* erfahren Sie unter Autorisieren von HTML-Elementen.

Warnmeldungen

Sie können 🗨 auswählen, um auf den Benachrichtigungsbereich für Warnmeldungen zuzugreifen. Im Benachrichtigungsbereich können Sie die Option *Zu Warnmeldungsseite* auswählen, um mehr über die von Ihnen erstellten Warnmeldungen zu erfahren.

25.1 Admin-Cockpit

Das Admin-Cockpit ist eine neue Anwendung, die der CMC hinzugefügt wurde. Mit ihr kann der Administrator grundlegende Daten zur BI-Umgebung sammeln. Das bedeutet, Business-Intelligence-Daten aus den Daten in Ihrer Business-Intelligence-Umgebung abzuleiten. Über das Admin-Cockpit erhalten Sie Informationen über Server, zeitgesteuerte Aufträge, Benutzer und Sitzungen, die Nutzung von Inhalten sowie über Anwendungen.

> ⓘ Hinweis
>
> Damit das Admin-Cockpit genutzt werden kann, müssen folgende Voraussetzungen erfüllt sein:
>
> - Der Überwachungsdienst muss aktiviert sein.
> - Das Auditing und das relevante Ereignis müssen aktiviert sein, damit korrekte Daten abgerufen werden.
> - Der RESTful-Webdienst der BI-Plattform muss für Clients verfügbar sein.
> - WACS muss ausgeführt werden, es sei denn, der RESTful-Webdienst ist auf Tomcat implementiert.
> - Stellen Sie bei der Konfiguration von SSL für die CMS sicher, dass Sie SSL auch für WACS konfigurieren, es sei denn, der RESTful-Web-Service ist auf Tomcat implementiert.
> - Der domänenübergreifende Zugriff muss aktiviert sein.
> - Benutzer müssen zur Administratorengruppe oder einer ihrer Untergruppen gehören, um auf das Admin-Cockpit zugreifen zu können.

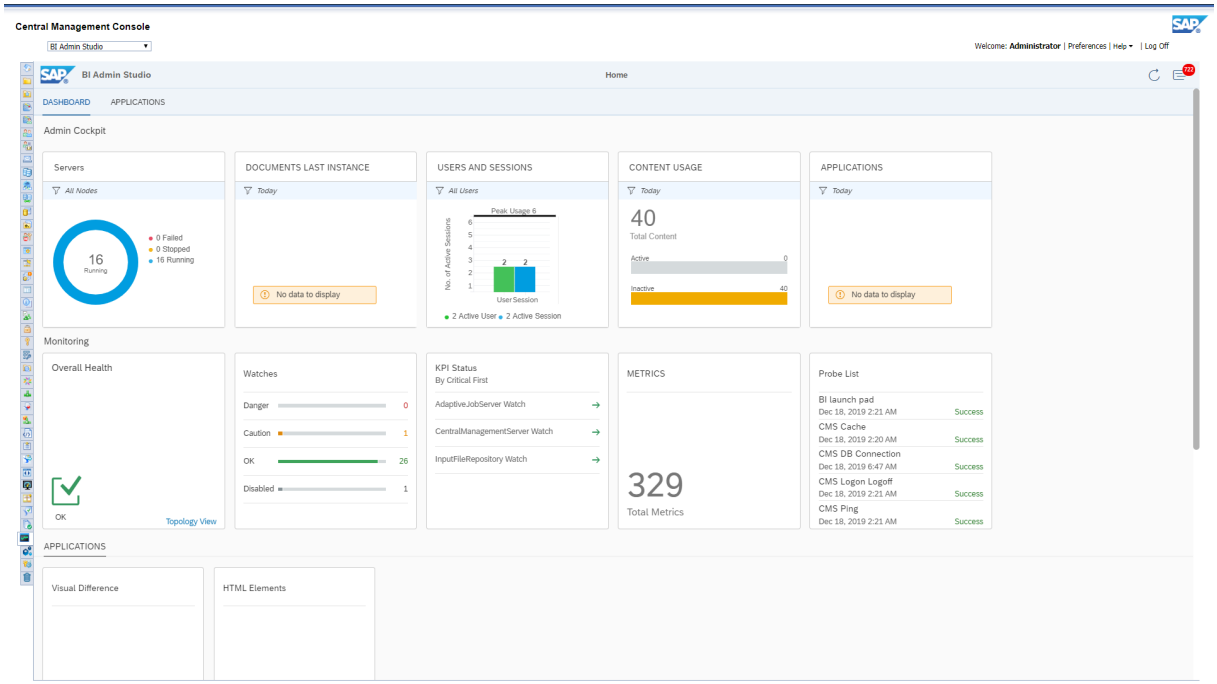
25.1.1 Admin-Cockpit

Das Admin-Cockpit bietet eine umfassende bildhafte Analyse von Daten zu den folgenden Komponenten:

- Server
- Letzte Instanz der Dokumente

- Benutzer und Sitzungen
- Inhaltsverwendung
- Anwendung

> **Hinweis**
>
> Die Audit-Datenbank muss aktiviert sein, um die Analyse für die *Nutzung des Inhalts* und die *Anwendung* anzuzeigen.



Sie können die Daten aktualisieren, die auf jeder Seite innerhalb des Admin-Cockpit angezeigt werden, indem Sie oben rechts auf der Startseite wählen.

25.1.2 BI für Server

Das Admin-Cockpit hilft Ihnen dabei, Echtzeitdaten über den Status und die jeweiligen Details zu sämtlichen Servern in Ihrer BI-Umgebung zu erhalten.

Auf der Startseite können Sie die folgenden Details einsehen:

- Gesamtzahl der Server
- Anzahl der Server mit Fehlern
- Anzahl der gestoppten Server

Sie können die auf der Kachel *Server* angezeigten Daten filtern, indem Sie das ausgewählte Server-Cluster auswählen.

Wenn Sie die Kachel *Server* wählen, werden Sie zur entsprechenden Serverseite weitergeleitet, auf der die Details zur Gesamtzahl der Server, der Fehler produzierenden Server sowie der gestoppten Server angezeigt werden. Auf der Serverseite können Sie auch den *Status*, den *Servernamen*, die *PID* (Prozess-ID), den *Typ*, den *Zustand* und die *Letzte Änderung* zu jedem Fehler produzierenden Server anzeigen.

Über die Seite *Server* können Sie Daten durch die Auswahl des gewünschten Server-Clusters anhand spezifischer Server-Cluster filtern.

Sie können weitere Details zum Fehler produzierenden Server anzeigen, indem Sie auf die entsprechende Zeile klicken. Dadurch werden Sie zu einer neuen Seite weitergeleitet, auf der der Grund des Fehlers angegeben wird. Sie können den Fehler produzierenden Server von der Seite aus neu starten, indem Sie *START* wählen.

25.1.3 BI-Informationen zu Dokumentinstanzen

Über das Admin-Cockpit können Sie den Status und die zugehörigen Details zu sämtlichen Instanzen der zeitgesteuert verarbeiteten Dokumente in Ihrer BI-Umgebung abrufen.

Auf der "Startseite" werden für jedes zeitgesteuert verarbeitete Dokument die folgenden Informationen angezeigt:

- Gesamtanzahl der letzten Instanzen des zeitgesteuert verarbeiteten Dokuments
- Anzahl der letzten ausgeführten Instanzen des zeitgesteuert verarbeiteten Dokuments
- Anzahl der Fehler produzierenden Instanzen des zeitgesteuert verarbeiteten Dokuments
- Anzahl der letzten ausstehenden Instanzen des zeitgesteuert verarbeiteten Dokuments

Auf der Kachel *Letzte Instanz der Dokumente* können Sie die Daten nach einem bestimmten Zeitraum filtern, indem Sie den gewünschten Zeitraum im Dropdown-Menü auswählen. Folgende Zeiträume sind verfügbar:

- Heute
- Letzte 7 Tage
- Letzte 30 Tage
- Quartal
- Jahr

Wenn Sie die Kachel *Letzte Instanz der Dokumente* wählen, werden Sie zur Seite "Letzte Instanzen" weitergeleitet, auf der für jedes zeitgesteuert verarbeitete Dokument die Gesamtanzahl der letzten Instanzen des Dokuments (aufgeschlüsselt nach Status: Wird ausgeführt, Fehler, Ausstehend) angezeigt wird. Auf der Registerkarte *Statistik* werden in den Bereichen *Dokumente mit den meisten Instanzen* und *Instanzen mit der längsten Laufzeit* die entsprechenden Details angezeigt. Auf der Seite "Dokumentinstanzen" werden zu jedem Fehlerstatus außerdem der *Instanzname*, der *Status*, der *Typ*, der *Eigentümer* sowie die *Endzeit* angezeigt.

Sie können die auf der Seite *Letzte Instanzen* angezeigten Daten als CSV-Datei exportieren, indem Sie auf die Schaltfläche für den Export-Link klicken. Sie haben außerdem die Möglichkeit, ausgewählte Instanzen zu exportieren, indem Sie das zugehörige Kontrollkästchen aktivieren und in der Dropdown-Liste für den Export die Option *Ausgewählte exportieren* auswählen.

Sie können weitere Details zu einer Fehler produzierenden Instanz anzeigen, indem Sie auf die entsprechende Zeile klicken. Sie können den Auftrag über die Seite neu starten, indem Sie *AUSFÜHREN* wählen.

Auf der Registerkarte "Statistik" ist ein neuer Diagrammfilter aktiviert, mit dem Sie die Top-5-, Top-10-, Top-15- und Top-20-Dokumente filtern und anzeigen können.

25.1.4 BI: Benutzer und Sitzungen

Das Admin-Cockpit hilft Ihnen dabei, Daten über Benutzer und Sitzungen in Ihrer BI-Umgebung abzurufen.

Auf der Startseite können Sie beispielsweise die folgenden Details einsehen:

- Anzahl der aktiven Benutzer
- Anzahl der aktiven Sitzungen

Über die Kachel *Benutzer und Sitzungen* können Sie Daten für folgende Benutzergruppen filtern:

- Alle Benutzer
- Vordefinierte Benutzer
- Zugriffslizenzbenutzer

Beim Klicken auf die Kachel *Benutzer und Sitzungen* werden Sie zur Seite "Benutzer und Sitzungen" weitergeleitet, die Details für "Alle Benutzer", "Top-Benutzer" und "Statistik" enthält. Auf der Registerkarte "Statistik" finden Sie Details zu den aktivsten und den inaktivsten Benutzern.

Auf der Seite "Benutzer und Sitzung" finden Sie Details zu *Benutzername*, *Gesamtzahl der Sitzungen*, *Zeitpunkt der letzten Anmeldung* und *Längste ausgeführte Sitzung*.

Um weitere Details zu einem bestimmten Benutzer anzuzeigen, klicken Sie auf die entsprechende Zeile. Dadurch werden Sie zu einer neuen Seite weitergeleitet, auf der Details zu den wichtigsten Sitzungen des betreffenden Benutzers angezeigt werden. Sie können jede beliebige Sitzung des betreffenden Benutzers über die Seite beenden, indem Sie die gewünschte Sitzung auswählen und anschließend auf *SITZUNG BEENDEN* klicken.

25.1.5 BI für die Nutzung von Daten

Das Admin-Cockpit hilft Ihnen dabei, Daten über die Nutzung der Inhalte in Ihrer BI-Umgebung zu erhalten.

Auf der Startseite können Sie beispielsweise die folgenden Details einsehen:

- Anzahl der aktiven Dokumente
- Anzahl der inaktiven Dokumente

Sie können in der Kachel *Inhaltsverwendung* die Daten nach einem bestimmten Zeitraum filtern, indem Sie im Dropdown-Menü den gewünschten Zeitraum auswählen.

> **Hinweis**
>
> Wenn Sie aktive Inhalte gelöscht haben und dann Daten nach einem bestimmten Zeitraum filtern, werden die gelöschten Einträge nach wie vor unter den aktiven Inhalten aufgeführt, wenn diese im gewählten Zeitraum aktiv waren.

Folgende Zeiträume sind verfügbar:

- Heute
- Letzte 7 Tage
- Letzte 30 Tage

- Quartal
- Jahr

Beim Klicken auf die Kachel *Inhaltsverwendung* werden Sie zu einer Seite über die Inhaltsverwendung weitergeleitet, auf der die Details zum aktiven Inhalt, inaktiven Inhalt und zu den Statistiken aufgeführt sind. Auf der Registerkarte "Statistiken" können Sie die Details zu den Posteingängen mit dem meisten inaktiven Inhalt, Universen mit dem meisten Inhalt sowie Ordnern mit dem meisten Inhalt einsehen.

Sie können die auf der Seite *Inhaltsverwendung* angezeigten Daten in eine CSV-Datei exportieren, indem Sie auf die Schaltfläche für den Export-Link klicken. Sie haben außerdem die Möglichkeit, ausgewählte Aufträge zu exportieren, indem Sie das entsprechende Kontrollkästchen aktivieren und in der Dropdown-Liste für den Export die Option *Ausgewählte exportieren* auswählen.

Auf der Seite über die Nutzung der Inhalte können Sie auch die *Bezeichnung des Inhalts*, den *Typ* und die *Laufzeit* anzeigen.

Auf der Registerkarte "Statistik" ist ein neuer Diagrammfilter aktiviert, mit dem Sie die Top-5-, Top-10-, Top-15- und Top-20-Dokumente filtern und anzeigen können.

25.1.6 BI für Anwendungen

Das Admin-Cockpit liefert Ihnen Daten über die Anzahl der Anwendungen in Ihrer BI-Umgebung, sortiert nach Anwendungsnamen.

Sie können in der Kachel *Anwendung* die Daten nach einem bestimmten Zeitraum filtern, indem Sie im Dropdown-Menü den gewünschten Zeitraum auswählen. Folgende Zeiträume sind verfügbar:

- Heute
- Letzte 7 Tage
- Letzte 30 Tage
- Quartal
- Jahr

Beim Klicken auf die Kachel *Anwendungen* werden Sie zu einer Anwendungsseite weitergeleitet, auf der die Details zu *Allen Anwendungen* und den *Top-Anwendungen* aufgeführt sind.

Auf der Registerkarte *Top-Anwendungen* werden die 5 Top-Anwendungen aufgeführt, in denen im ausgewählten Zeitraum die meisten Dokumente erstellt wurden. Auf der Anwendungsseite können Sie auch den *Anwendungsnamen*, die *Anzahl der Benutzer* sowie die *Anzahl der Artefakte* anzeigen.

25.2 Überwachung

Das Überwachungstool in SAP BusinessObjects Business Intelligence bietet die Möglichkeit, die Laufzeit- und Verlaufsmetriken von BI-Plattform-Servern für die Berichterstellung und Benachrichtigung zu erfassen. Das Überwachungstool zeigt außerdem an, ob die Anwendung ordnungsgemäß funktioniert.

Der Zugriff auf das Überwachungstool kann über die CMC-Startseite erfolgen. Das Überwachungstool umfasst folgende Registerkarten:

- *Dashboard*: Enthält den Gesamtstatus, den KPI-Status, den Kontrollmodulstatus, aktuelle Warnmeldungen und Direktlinks.
- *Metriken*: Führt alle Metriken auf, die im BI-Plattform-System gefunden wurden. Stellt eine Option zur Erstellung einer neuen Metrik bereit.
- *Kontrollmodulliste*: listet die Anzahl der Kontrollmodule nach Status wie z. B. *Gefahr*, *Achtung*, *OK*, *Deaktiviert* und *Fehlgeschlagen* auf.
- *Diagnosen*: Führt die Diagnosen mit dem jeweiligen Status und den entsprechenden Diagrammen auf.
- *Warnmeldungen*: Enthält alle im Überwachungstool generierten Warnmeldungen.

25.2.1 Dashboard

Über die Seite "Dashboard" kann der Benutzer von einem einzelnen Bildschirm aus den Systemstatus verfolgen. Sie bietet Echtzeitinformationen über KPIs, aktuelle Warnmeldungen und den Status der BI-Implementierung.

25.2.1.1 Dashboard-Warnmeldungen

Im Dashboard-Bereich *Aktuelle Warnmeldungen* werden maximal sechs aktuelle Warnmeldungen und die Uhrzeiten angezeigt, zu denen die Warnmeldungen aufgezeichnet wurden. Sie können auf eine Warnmeldung klicken, um die mögliche Problemursache und die durchgeführte Aktion anzuzeigen. Klicken Sie auf die Kachelüberschrift "Warnmeldungen", um zur Seite *Warnmeldungen* zu navigieren.

> ⓘ Hinweis
>
> Die Ursache und die Aktion werden nur angezeigt, wenn sie aufgezeichnet wurden, als eine Warnmeldung bestätigt wurde.

Weitere Informationen zu den Aktivitäten, die auf der Seite *Warnmeldungen* ausgeführt werden können, erhalten Sie unter Warnmeldungen [Seite 358].

25.2.1.2 Dashboard-KPIs

25.2.1.2.1 Anpassen des Bereichs "KPI-Status"

Im Bereich *KPI-Status* werden die KPIs basierend auf Ihrer Auswahl angezeigt. Sie können die im Bereich *KPI-Status* anzuzeigenden KPIs anpassen, indem Sie folgende Schritte durchführen:

1. Klicken Sie auf *KPI auswählen*. Die Liste der verfügbaren KPIs wird angezeigt.
2. Wählen Sie die anzuzeigenden KPIs im Bereich *KPI-Status* aus. Hier können Sie bis zu acht KPIs auswählen. Um einen KPI zu entfernen, heben Sie die Auswahl des KPIs in der Dropdown-Liste auf. Klicken Sie auf die KPI-Kachelüberschrift, um zur Seite *Kontrollmodulliste* zu gelangen, auf der Sie KPIs hinzufügen oder entfernen können.

> **Hinweis**
>
> Sie können die aktuellen Aktualisierungen der KPIs anzeigen, indem Sie im Bereich "KPI-Status" mit den angezeigten KPIs auf den Hyperlink *Letzte Aktualisierung* klicken.

25.2.1.2.2 Ursachenanalysen im Bereich "KPI-Status" ausführen

Mit dem Bereich "KPI-Status" können Sie die Ursache für den Fehler einer Metrik ermitteln.

1. Klicken Sie auf eine im Bereich *KPI-Status* angezeigte KPI.
   Der Bildschirm *Kontrollmoduldetails* wird angezeigt.
2. Im Bereich *Kontrollmoduldetails* können Sie unter *Allgemeine Eigenschaften* und *Kontrollmodulregel* die Ursache für einen Fehler oder Erfolg einer Metrik anzeigen.

25.2.1.3 Gesamtstatusanzeige

Im Bereich *Gesamtstatus* wird der Gesamtstatus der BI-Plattform-Implementierung angezeigt.

Beispiel: Ist der Status einer bzw. eines der Dienstkategorien, Enterprise-Knoten oder Servergruppen rot, so ist der Gesamtstatus-Indikator ebenfalls rot.

Klicken Sie im Bereich *Gesamtstaus* auf *Topologieansicht*, um die BI-Plattform-Implementierung auf der Basis der folgenden Kriterien anzuzeigen:

- Enterprise-Knoten
- Servergruppen
- Dienstkategorien

Topologieansicht

Über die *Topologieansicht* haben Sie folgende Möglichkeiten:

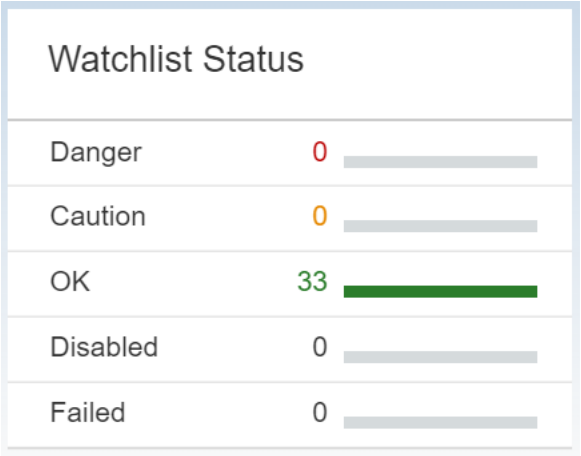
- Anzeige der ausgewählten BI-Plattform-Implementierung in grafischer oder tabellarischer Form, indem Sie das Symbol wählen.
  - Das mit dem grafischen Format eingeblendete Fenster zeigt das direkt übergeordnete Element sowie gleichgeordnete Elemente eines aufgeklappten Knotens nach einem Drilldown an. Klicken Sie auf das eingeblendete Fenster, um zum übergeordneten Knoten zurückzukehren. Im Fall von Servergruppen können Sie den Root-Knoten der Hierarchie anzeigen.
    Bewegen Sie beim grafischen Format den Mauszeiger über den jeweiligen Knoten, um den Status anzuzeigen. Doppelklicken Sie auf einen Knoten, um die Kontrollmoduldetails dieses Knotens anzuzeigen.

    - Bei der tabellarischen Ansicht wird der Status in der Spalte *Gesamtstatus* angezeigt.
- Filtern der Implementierung nach Typ über die Dropdown-Liste *Typ anzeigen*.
- Filtern der ausgewählten Implementierung nach Status über die Dropdown-Liste *Status*.
- Abrufen des aktuellen Status über das Symbol *Regenerieren* ( ) im *Filterbereich*.

25.2.1.4 Status der Kontrollmodulliste

Der *Status der Kontrollmodulliste* gibt die Gesamtanzahl der Kontrollmodule an und zeigt die Anzahl der Kontrollmodule mit dem jeweiligen Status an:

- Gefahr
- Achtung
- OK
- Deaktiviert
- Fehlgeschlagen



25.2.1.5 Direktlinks

Über die Kachel *Direktlinks* können Sie direkt vom Dashboard aus die folgenden Aufgaben durchführen:

- *Neue Metrik erstellen*
- *Neues Kontrollmodul erstellen*
- *Java-basierte Diagnose erstellen*
- *Skriptdiagnose erstellen*

25.2.2 Diagramme

Mit den Diagrammen des Überwachungstools können Sie die Systemleistung in verschiedenen Zeitintervallen überwachen. Auf der Seite "Diagnosen" basieren die Diagramme auf der Roundtrip-Zeit und dem Diagnosestatus. Die Diagramme der übrigen Seiten basieren auf den Metrikdaten.

> **Hinweis**
>
> Die in den Diagrammen angezeigte Zeit entspricht der im Feld *Zeitzone* unter *CMC-Einstellungen* festgelegten Zeit. Wenn Sie *Standard – Ortszeit des Webservers* wählen, wird die Zeitzone des Ortes verwendet, an dem sich der Server befindet.

Diagramme können in den folgenden zwei Modi angezeigt werden:

- Live-Modus: Dieser Modus zeigt den Diagnosestatus der letzten 2 Minuten an und wird kontinuierlich aktualisiert. Die Optionen "Histogramm", "Vergrößern", "Verkleinern" und "Kalender" sind in diesem Modus deaktiviert.
- Verlaufsmodus: In diesem Modus können Sie Diagramme mit Verlaufsdaten anzeigen. Die Optionen "Histogramm", "Vergrößern", "Verkleinern" und "Kalender" sind in diesem Modus aktiviert. Das Diagramm kann für maximal 6 Monate im Verlaufsmodus angezeigt werden.

Die Hauptbereiche des Diagramms sind folgende:

- Kopf – Zeigt den Metriktitel und den Modus zusammen mit dem Zeitbereich an, für den das Diagramm angezeigt wird. Im Kopf wird außerdem der aktuelle Wert im Live-Modus angezeigt.
- Hauptdiagramm – Zeigt den aktuellen Status der Metrik oder der ausgeführten Diagnose mit Datum und Uhrzeit an.
- Symbolleiste – Die Symbolleiste enthält die folgenden Schaltflächen:

  : Diese Umschaltfläche ermöglicht das Umschalten zwischen Live-Modus und Verlaufsmodus.

  : Mit der Kalenderoption können Sie Uhrzeit und Datum für Start und Ende auswählen.

  : Ermöglicht die Anzeige des Diagramms im Vollbild.

Synchronisieren der Zeitachse

Für Diagramme wird die Funktionalität zum Synchronisieren von Zeitachsen im Überwachungstool bereitgestellt. Beim Anzeigen von mehreren Diagrammen in demselben Fenster können Sie auf *Zeitachsen synchronisieren* klicken, um denselben Zeitbereich für alle Diagramme festzulegen. Wenn Sie den Zeitbereich in einem Diagramm ändern, verändert sich der Zeitbereich in allen Diagrammen entsprechend. Das Synchronisieren von Zeitachsen ist sowohl im Verlaufsmodus als auch im Live-Modus möglich.

25.2.3 Diagnosen

Mit der Diagnosefunktion kann das SAP-BusinessObjects-System unter Verwendung einer simulierten Anwendung überwacht werden. Die von diesen Diagnosen generierten Ergebnisse und Diagramme enthalten wichtige Eingabeinformationen über Systemverfügbarkeit, -status und -stabilität sowie eine Leistungsstatistik verschiedener SAP-BusinessObjects-Dienste und -Funktionen. Diese Daten können auch zur Kapazitätsplanung verwendet werden.

Sie können jederzeit eine Diagnose zur Überprüfung des Systemzustands ausführen. Die Ausführung von Diagnosen kann für vorgegebene Intervalle zeitgesteuert verarbeitet werden. Für eine einzelne Diagnose können mehrere zeitgesteuerte Verarbeitungen bestehen. Nach der Ausführung einer Diagnose wird das Diagnoseergebnis und die Roundtrip-Zeit angezeigt und darüber hinaus grafisch dargestellt. Von Diagnosen generierte Metriken werden als "virtuelle Metriken" bezeichnet. Diese virtuellen Metriken können bei der Erstellung von Kontrollmodule verwendet werden.

Mit den Überwachungsdiagnosen der BI-Plattform können Sie folgende Aktivitäten ausführen:

- Simulation von Endbenutzer-Workflows wie etwa Benutzeranmeldevorgänge und Berichtausführung von Web-Intelligence- und Crystal-Reports-Anwendungen.
- Testen von Verfügbarkeit, Funktionalität und Performance von SAP-BusinessObjects-Diensten.
- Testen der Kernfunktionen des Central Management Servers (CMS), des CMS-Cache-Diensts und der CMS-Datenbankverbindung.

Diagnosen können in folgenden Szenarios verwendet werden:

- Zum Überprüfen der Überlastung im CMS können Sie die Diagnose für die CMS-Datenbankverbindungen ausführen. Anhand des Diagnoseergebnisses und der Roundtrip-Zeit in verschiedenen Zeitintervallen können Sie eine Implementierung planen oder die Berichterstellung in großem Umfang effektiv zeitgesteuert verarbeiten.
- Um die Verfügbarkeit eines Servers zu prüfen, können Sie eine CMS-Diagnose in verschiedenen Zeitintervallen ausführen und erhalten den Serverdatenverkehr zu jedem beliebigen Zeitpunkt.

25.2.3.1 Diagnosetypen

Die Diagnosen können folgendermaßen eingeteilt werden:

- Diagnoseberichte: Diagnosen, die Ergebnisse generieren, in denen aktuelle Systeminformationen enthalten sind. Zu den Diagnoseberichten gehört der Serverstart/-stopp. Diese Diagnose prüft alle Server, zeichnet den Status aller Server auf, startet die Server neu und sammelt erneut Informationen über die Server.
- Diagnosemetriken: Diagnosen, die Metriken von Datentypen generieren, wie etwa ganzzahlig, Boolesch oder Zeichenfolge. Dazu zählt die CMS-Anmeldung und -Abmeldung. Diese Diagnose prüft, ob die Benutzer sich erfolgreich am Central Management Server (CMS) anmelden und abmelden können.
- Hybrid-Diagnosen: Diagnosen, die als Diagnosebericht und -metrik fungieren. Mit Ausnahme der Serverstart/-Serverstopp-Diagnosen, die zu den Diagnoseberichten gehören, sind alle anderen von der BI-Plattform bereitgestellten Diagnosen Hybrid-Diagnosen.

Standardmäßig werden folgende Überwachungsdiagnosen mit der BI-Plattform ausgeliefert:

CMS-Anmeldung/-Abmeldung

Die Diagnose für die CMS-Anmeldung/-Abmeldung prüft die Verfügbarkeit des CMS und die Möglichkeit des Benutzers zur Anmeldung am System über Clientanwendungen. Die Diagnose meldet sich als Benutzer an, prüft die Sitzungsgültigkeit und meldet sich dann ab.

Crystal-Reports-Dienst über Page Server und Cache-Server

Die Diagnose des Crystal Reports-Dienstes über Page Server und Cache-Server prüft die Verfügbarkeit des Crystal-Reports-Diensts über Page Server und Cache-Server von Crystal Reports. Die Diagnose verwendet die Crystal Reports Page Server und Cache-Server, um einen Bericht zu öffnen, ihn ggf. zu regenerieren, in das PDF-Format zu exportieren und den Bericht zu schließen.

Crystal-Reports-Dienst über Report Application Server

Die Diagnose des Crystal-Reports-Dienstes über Report Application Server prüft die Verfügbarkeit des Crystal-Reports-Dienstes über Report Application Server. Die Diagnose verwendet die Report Application Server, um einen Bericht zu öffnen, ihn ggf. zu regenerieren, in das PDF-Format zu exportieren und den Bericht zu schließen.

Web-Intelligence-Dienst

Die Diagnose des Web-Intelligence-Dienstes prüft die Verfügbarkeit des Web-Intelligence-Dienstes über Web Intelligence Report Server. Die Diagnose öffnet ein Web Intelligence-Dokument, regeneriert und exportiert es ggf. in XLS- und PDF-Formate und schließt das Dokument.

CMS-Ping

Das CMS-Ping sendet eine leere Abfrage an den CMS. Diese Diagnose gilt als erfolgreich, wenn der CMS einen Analysefehler zurückgibt. Diese Diagnose sollte schnell abgeschlossen sein, da die Abfrageanalyse zu den CMS-Kernfunktionen gehört.

CMS-Cache

Die Diagnose des CMS-Caches prüft die Verfügbarkeit und den Zustand des CMS-Caches durch das Senden folgender Abfrage:

```
select SI_NAME from
```

```
          CI_SYSTEMOBJS where SI_OBTYPE=4
```

Diese Abfrage gibt das System-InfoObject zurück, das den CMS-Clusternamen enthält. Der CMS ruft das System-InfoObject eher aus dem Cache als aus der Repository-Datenbank ab. Wenn der Cache nicht ordnungsgemäß funktioniert oder die Cluster-Definition nicht korrekt ist, kann die Abfrage nicht ausgeführt werden.

CMS-Datenbankverbindung

Die Diagnose der CMS-Datenbankverbindung prüft die Verfügbarkeit der Repository-Datenbank durch die Ausführung folgender Abfrage:

```
select SI_NAME from CI_SYSTEMOBJS
          where SI_OBTYPE=13
```

Diese Abfrage gibt das System-InfoObject zurück, das dem Desktop-Plugin-Objekt des Benutzers entspricht. Der CMS ruft das System-InfoObject von der Repository-Datenbank ab. Wenn die Verbindung zwischen dem CMS-Server und der Repository-Datenbank nicht ordnungsgemäß hergestellt wird, kann die Abfrage nicht ausgeführt werden.

BI-Launchpad

Mit der BI-Launchpad-Diagnose wird der Gesamtstatus des BI-Launchpads geprüft. Dazu gehört die Anmeldung beim BI-Launchpad mit ausgewählten Authentifizierungstypen (z.B. Enterprise, LDAP, SAP oder Windows AD) und die anschließende Abmeldung.

Beachten Sie folgende Einschränkungen:

- Wenn das BI-Launchpad so konfiguriert ist, dass die Authentifizierungsmethode während der Anmeldung ausgeblendet wird, wird der auf der Eigenschaftenseite der Diagnose ausgewählte Authentifizierungstyp ignoriert.
- Wenn Sie einen benutzerdefinierten Einsprungspunkt für das BI-Launchpad eingerichtet haben (eine andere Webseite, die zur Umleitung auf die BI-Launchpad-Anmeldeseite dient, z.B. die Seite `http://localhost:8080/BOE/BI/custom.jsp`, die auf `http://localhost:8080/BOE/BI` umleitet), verwenden Sie den benutzerdefinierten Einsprungspunkt nicht mit der BI-Launchpad-Diagnose.
- Auf der Eigenschaftenseite der BI-Launchpad-Diagnose wird die Einstellung "InfoView-Anwendungsname" nicht verwendet (sie ist veraltet).

Server stoppen/starten

Die Diagnose zum Stoppen/Starten der Server prüft den Status der Server, die der Benutzer überprüfen möchte. Dazu gehört das Stoppen und Starten der zu überwachenden Server.

25.2.3.2 Verwalten von Diagnosen

Auf der Seite *Diagnosen* des Überwachungstools werden alle Diagnosen zusammen mit dem Status der zeitgesteuerten Verarbeitung, der nächsten geplanten Ausführung und dem Ergebnis der vorherigen Ausführung einschließlich Uhrzeit angezeigt. Beim Auswählen einer Diagnose werden zwei Diagramme angezeigt: *Ergebnis* und *Roundtrip-Zeit*. Diese Diagramme werden standardmäßig im Verlaufsmodus angezeigt. Auf der Seite *Diagnosen* können Sie Diagnosen ausführen und zeitgesteuert verarbeiten, die Eigenschaften oder den Verlauf von Diagnosen prüfen, Einschränkungen festlegen und Diagnosen regenerieren.

Um die automatische Regenerierung der Diagnosen festzulegen, klicken Sie auf . Wenn Sie eine Diagnose manuell regenerieren möchten, klicken Sie auf .

25.2.3.2.1 Ausführen von Diagnosen

Diagnosen können zu jeder beliebigen Zeit durchgeführt werden. Wählen Sie aus der Liste der Diagnosen eine Diagnose aus, und klicken Sie auf *Jetzt ausführen* . Nach Durchführung der Diagnose zeigt die Spalte *Ergebnis und Uhrzeit der vorherigen Ausführung* den Status der Diagnose als *Wird ausgeführt* an, sowie die Uhrzeit des Diagnosestarts. Wenn die Aktivitäten der Diagnose abgeschlossen sind, werden in der Spalte *Ergebnis und Uhrzeit der vorherigen Ausführung* die Roundtrip-Zeit in Millisekunden sowie Startdatum und -uhrzeit der Diagnose angezeigt. Die Diagramme für das Ergebnis und die Roundtrip-Zeit der Diagnose werden angezeigt.

> **Hinweis**
>
> Der Status einer Diagnose kann Erfolgreich, Fehler oder Zeitüberschreitung lauten. Klicken Sie auf den Diagnosestatus, um die Details zur Diagnose anzuzeigen. Der Status `Keine Daten verfügbar` wird angezeigt, wenn die Diagnose nie ausgeführt oder die Diagnosedaten gelöscht wurden.

25.2.3.2.2 Zeitgesteuertes Verarbeiten von Diagnosen

Sie können einzelne Diagnosen so zeitgesteuert verarbeiten, dass sie zu bestimmten Zeiten ausgeführt werden. Zeitgesteuertes Verarbeiten einer Diagnose:

1. Wählen Sie aus der Spalte *Diagnose* eine Diagnose aus, und klicken Sie dann auf

   Schedule .

2. Klicken Sie im linken Bereich des Dialogfeldes *Zeitgesteuert verarbeiten* auf *Wiederholung*, und wählen Sie im Dropdown-Menü *Objekt ausführen* ein Wiederholungsmuster aus.
   Bei der Auswahl eines Wiederholungsmusters werden Sie von der Anwendung aufgefordert, zusätzliche Informationen anzugeben. In der folgenden Tabelle werden die zusätzlichen Informationen aufgelistet, die Sie für jedes Wiederholungsmuster angeben müssen:

Optionen zur Objektausführung	Zusätzliche Informationen erforderlich
Jetzt	Keine
Einmal	Definieren Sie Start- und Enddatum/-zeit
Stündlich	Definieren Sie Stunde und Minute, und anschließend Start- und Endatum/-zeit
Täglich	Definieren Sie die Anzahl der Tage, und dann Start- und Enddatum/-uhrzeit
Wöchentlich	Wählen Sie die Wochentage, und legen Sie anschließend Start- und Enddatum/-zeit fest
Monatlich	Definieren Sie die Anzahl der Monate, und anschließend Start- und Enddatum/-zeit
Am n-ten Tag des Monats	Wählen Sie den Tag im Monat, und legen Sie anschließend Start- und Enddatum/-zeit fest
Am ersten Montag des Monats	Definieren Sie Start- und Enddatum/-zeit
Am letzten Tag des Monats	Definieren Sie Start- und Enddatum/-zeit
Tag x der n-ten Woche des Monats	Wählen Sie Woche und Tag, und legen Sie anschließend Start- und Enddatum/-zeit fest
Kalender	Sie können einen benutzerdefinierten Kalender auswählen, und dann Start- und Enddatum/-uhrzeit definieren.

3. Geben Sie eine Zahl im Feld *Zulässige Anzahl der Wiederholungen* sowie die erforderliche Zeit im Feld *Wiederholungsintervall in Sekunden* ein.
4. Klicken Sie auf *Zeitgesteuerte Verarbeitung für* und wählen Sie auf Grundlage Ihrer Anforderungen entweder *Nur für mich zeitgesteuert verarbeiten* oder *Für angegebene Benutzer und Benutzergruppen zeitgesteuert verarbeiten*.
   Wenn Sie *Für angegebene Benutzer und Benutzergruppen zeitgesteuert verarbeiten* auswählen, werden Sie von der Anwendung aufgefordert, den Namen des Benutzers oder der Benutzergruppe einzugeben. Wählen Sie die Benutzer oder die Benutzergruppe aus der in der Spalte *Verfügbar* enthaltenen Liste aus, und klicken Sie auf . Klicken Sie auf , um die Benutzergruppe aus der Auswahl zu entfernen.
5. Klicken Sie auf *Zeitgesteuert verarbeiten*.

Standardzeitsteuerung

Mit den Einstellungen zur zeitgesteuerten Standardverarbeitung können Sie mehrere Diagnosen auf einem ähnlichen Zeitplan ausführen. Zum Festlegen der Standardzeitsteuerung gehen Sie wie folgt vor:

1. Wählen Sie aus der Spalte *Diagnose* eine Diagnose aus, und klicken Sie dann auf *Zeitgesteuert verarbeiten*.
2. Klicken Sie auf *Standardeigenschaften*.
3. Führen Sie dieselben Schritte wie bei der Zeitsteuerung einzelner Diagnosen aus.

25.2.3.2.3 Anzeigen von Diagnoseeigenschaften

Auf der Seite *Diagnosen* können Sie die Eigenschaften von Diagnosen anzeigen sowie bestimmte Felder ändern. Alle Diagnosen haben einige gemeinsame Eigenschaften sowie bestimmte individuelle Eigenschaften. Um die Eigenschaften einer Diagnose anzuzeigen und zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie eine Diagnose aus, und klicken Sie auf *Eigenschaften*.
2. Ändern Sie die Felder nach Bedarf, und klicken Sie auf *Speichern & schließen*.

In der folgenden Tabelle werden die allgemeinen Eigenschaften von Diagnosen aufgelistet:

Parameter	Beschreibung	Typ
Titel	Titel der Diagnose	Zeichenfolge
CUID	CUID der Diagnose	
Beschreibung	Kurze Beschreibung die Diagnosefunktionen	Zeichenfolge
Erstellt	Datum und Uhrzeit der Diagnoseerstellung	
Zuletzt geändert:	Datum und Uhrzeit der letzten Änderung an der Diagnose	
Zuletzt ausgeführt am:	Datum und Uhrzeit der letzten Ausführung der Diagnose	
Zeitüberschreitung (s)	Zeitbeschränkung (in Sekunden), nach der die Ausführung der Diagnose gestoppt wird	Ganzzahl

In den folgenden Tabellen werden die für bestimmte Diagnosen erforderlichen Eingabeparameter aufgelistet:

Crystal Reports-Dienst über Page Server und Cache-Server

Eingabeparameter	Beschreibung	Typ
CUID	CUID des Dokuments	Zeichenfolge
export	Wenn Sie dies aktivieren, wird das Dokument in das PDF-Format exportiert Wenn Sie dies deaktivieren, wird das Dokument nicht in das PDF-Format exportiert	Boolesch
refresh	Wenn Sie dies aktivieren, wird das Dokument regeneriert Wenn Sie dies deaktivieren, wird das Dokument nicht regeneriert	Boolesch

Crystal Reports-Dienst über Report Application Server

Eingabeparameter	Beschreibung	Typ
CUID	CUID des Dokuments	Zeichenfolge
export	Wenn Sie dies aktivieren, wird das Dokument in das PDF-Format exportiert Wenn Sie dies deaktivieren, wird das Dokument nicht in das PDF-Format exportiert	Boolesch

Eingabeparameter	Beschreibung	Typ
refresh	Wenn Sie dies aktivieren, wird das Dokument regeneriert Wenn Sie dies deaktivieren, wird das Dokument nicht regeneriert	Boolesch

BI-Launchpad

Eingabeparameter	Beschreibung	Typ	Beispielwert
Authentifizierungstyp	Authentifizierungstyp	Zeichenfolge	Enterprise
CMS-Name	Name des im BI-Launchpad verwendeten CMS	Zeichenfolge	localhost:6400
Kennwort	BI-Launchpad-Kennwort	Zeichenfolge (verschlüsselt)	Kennwort1
URL-Basis	Basis-URL der BI-Launchpad-Anwendung, mit der der Benutzer eine Verbindung herstellt	Zeichenfolge	http://localhost:8080/BOE/BI
Benutzername	BI-Launchpad-Benutzername	Zeichenfolge	Administrator

Serverstart/-stopp

Eingabeparameter	Beschreibung	Typ	Beispielwert
whereclause	Mit diesem Eingabeparameter können die Benutzer definieren, welche Server überwacht werden sollen	Zeichenfolge	`Where SI_PROGID='CrystalEnterprise.Server' AND SI_SERVER_KIND NOT IN ('aps') AND SI_NAME NOT LIKE '%AdaptiveProcessingServer%' AND SI_NAME NOT LIKE '%AdaptiveJobServer%'`

Web Intelligence-Dienst

Eingabeparameter	Beschreibung	Typ
CUID	CUID des Dokuments	Zeichenfolge
pdfexport	Wenn Sie dies aktivieren, wird das Dokument in das PDF-Format exportiert Wenn Sie dies deaktivieren, wird das Dokument nicht in das PDF-Format exportiert	Boolesch
refresh	Wenn Sie dies aktivieren, wird das Dokument regeneriert Wenn Sie dies deaktivieren, wird das Dokument nicht regeneriert	Boolesch

Eingabepa-rameter	Beschreibung	Typ
xlsexport	Wenn Sie dies aktivieren, wird das Dokument in das Excel-Format exportiert Wenn Sie dies deaktivieren, wird das Dokument nicht in das Excel-Format exportiert	Boolesch

25.2.3.2.4 Anzeigen des Diagnoseverlaufs

Das Überwachungstool protokolliert die Ergebnisse von ausgeführten Diagnosen. Um den Verlauf einer Diagnose anzuzeigen, wählen Sie sie aus der Spalte *Diagnose* aus, und klicken dann auf *Verlauf*.

Das Dialogfeld *Verlauf* wird angezeigt, in dem die ausgeführten Instanzen der Diagnosen aufgelistet werden. Das Dialogfeld "Verlauf" stellt die folgenden Details für alle Instanzen bereit:

Feld	Beschreibung
Zeit der Instanz	Zeigt den Zeitpunkt an, an dem die Diagnose gestartet wurde
Titel	Zeigt den Titel der Diagnose an
Status	Zeigt an, ob die Zeitsteuerung erfolgreich war
Erstellt Von	Zeigt an, wer die Diagnose erstellt hat
Typ	Zeigt den Typ der Diagnose an Wie z.B. Diagnosebericht, Diagnoseauswertung oder Diagnosebericht und -auswertung
Ergebnis des Laufs	Zeigt an, ob die Diagnose ein positives, negatives oder kein Ergebnis erbracht hat

Im Dialogfeld *Verlauf* können Sie folgende Aktionen ausführen:

- Klicken Sie zur Regenerierung der Instanzenliste auf , oder klicken Sie auf *Verwalten* und wählen Sie dann *Regenerieren*.
- Wählen Sie zum Löschen einer Instanz die entsprechende Instanz aus, und klicken Sie auf *Verwalten*, und wählen Sie dann *Löschen*.
- Wählen Sie zur Anzeige von Instanzdetails die entsprechende Instanz aus, und klicken Sie auf . Die *Instanzendetails* werden in einem neuen Fenster geöffnet.
- Um eine Instanz anzuhalten oder eine angehaltene Instanz wieder aufzunehmen, wählen Sie die Instanz aus und klicken auf *Aktionen*. Dann wählen Sie entsprechend *Anhalten* oder *Fortsetzen*. Sie können auch die verfügbaren Symbole verwenden.
- Um eine Instanz erneut auszuführen, wählen Sie die Instanz aus und klicken auf , oder Sie klicken auf *Aktionen* und wählen *Jetzt ausführen*.

> **Hinweis**
>
> Sie können die Filter verwenden, die für die Spalten *Instanzenzeit*, *Titel*, *Status* und *Erstellt von* bereitgestellt wurden.

- Klicken Sie zum Anzeigen der Ergebnisse auf das Diagnoseergebnis. Das Dialogfeld *Diagnoseergebnis* wird geöffnet. Die Seite *Diagnoseergebnis* zeigt Folgendes an:

  Diagnosename
  Ergebnis
  Dauer
  Diagnosemeldungen

25.2.3.2.5 Festlegen von Beschränkungen für die zeitgesteuerte Verarbeitung

Die Funktion zur Diagnosebeschränkung ermöglicht Ihnen die Verwaltung der Diagnoseinstanzen. Mit dieser Funktion können Sie die Anzahl der Instanzen festlegen, die im Dialogfeld *Verlauf* angezeigt werden soll, oder die Anzahl der Tage, die die Verlaufsinstanzen aufbewahrt werden sollen. Nachdem Sie die Anzahl der Instanzen oder Tage festgelegt haben, werden die überzähligen Instanzen aus der Datenbank gelöscht. Um die Beschränkungen für den Diagnoseverlauf festzulegen, gehen Sie wie folgt vor:

1. Wählen Sie aus der Spalte *Diagnose* eine Diagnose aus, und klicken Sie dann auf *Verlauf*.
2. Klicken Sie im linken Bereich auf *Beschränkungen*. Wählen Sie im Dialogfeld "Beschränkungen" die Option *Überzählige Instanzen löschen, wenn die Anzahl der Objektinstanzen mehr als N beträgt* aus, und geben Sie die erforderliche Zahl ein.
3. Wenn die von Ihnen festgelegte Instanzenbeschränkung nur für ausgewählte Benutzer oder Benutzergruppen gelten soll, klicken Sie auf *Hinzufügen* für *Überzählige Instanzen für die folgenden Benutzer/Gruppen löschen*. Wählen Sie aus *Verfügbare Benutzer/Gruppen* die entsprechenden Benutzer oder Benutzergruppen aus, und klicken Sie auf , oder klicken Sie auf , um alle Benutzer und Benutzergruppen auszuwählen.
4. Wenn die Instanzenbeschränkung für die Anzahl der Tage nur für ausgewählte Benutzer oder Benutzergruppen gelten soll, klicken Sie auf *Hinzufügen* für *Instanzen nach N Tagen für die folgenden Benutzer/Gruppen löschen*. Wählen Sie aus *Verfügbare Benutzer/Gruppen* die entsprechenden Benutzer oder Benutzergruppen aus, und klicken Sie auf , oder klicken Sie auf , um alle Benutzer und Benutzergruppen auszuwählen.

25.2.3.2.6 Verwalten von Diagnosen über die Befehlszeile

Mit dem Überwachungstool der BI-Plattform können Sie Diagnosen über die Befehlszeilenschnittstelle hinzufügen, ausführen und löschen.

> **Hinweis**
>
> Für jede Parameterdefinition lautet das Format `<Name>:<Typ>:<Wert>`. Hinzu kommt ein optionaler vierter Parameter: `true`, zur Verschlüsselung des Werts. Wenn Sie `true` angeben, wird der Wert in der Central-Management-Server-Datenbank verschlüsselt und außerdem auf der Eigenschaftenseite der Diagnose in der Central Management Console maskiert.

> **Hinweis**
>
> In der Befehlssyntax werden Doppelpunkte und Semikolons als Trennzeichen verwendet. Aus diesem Grund können Sie einen Parameter wie `urlbase` nicht als `localhost:8080` festlegen. Sie müssen die Diagnose zuerst erstellen und dann in der CMC die URL für die Diagnose festlegen.

Hinzufügen einer neuen Diagnose über die Befehlszeilenschnittstelle

1. Geben Sie den folgenden Pfad in die Befehlszeilenschnittstelle ein: `cd C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise 4.0\win64_x64\scripts`.
2. Geben Sie den Befehl **`probeAdd`** gemeinsam mit den erforderlichen Attributen und Parametern wie in der folgenden Tabelle beschrieben ein:

Attribute/Parameter	Beschreibung	Beispiel:
`-auth`	Authentifizierungstyp (zum HINZUFÜGEN der Diagnose)	secEnterprise
`-classname`	Vollständig qualifizierter Klassenname der Diagnose	-classname com.businessobjects.monitoring.probe.ProbeInfoView
`-cms`	CMS-Name	localhost:6400
`-help`	Hilfe für diese Anwendung drucken	
`-inputparam`	Eingabeparameter für die vorliegenden Diagnose	-inputparam "authtype:string:enterprise;urlbase:string:localhost;cmsname:string:host_machine_name;username:string:administrator;password:string:Password1:true"
`-name`	Diagnosename	BI-Launchpad
`-password`	Kennwort (zum HINZUFÜGEN der Diagnose) (Groß- und Kleinschreibung beachten)	Kennwort1
`-timeout`	Zeitüberschreitungsintervall in Sekunden	10
`-username`	Benutzername (zum HINZUFÜGEN der Diagnose)	Administrator

> **Hinweis**
>
> Die obigen Parameter `-auth`, `-username` und `-password` werden zum HINZUFÜGEN einer Diagnose verwendet. Der Authentifizierungstyp, der Benutzername und das Kennwort zum AUSFÜHREN der Diagnose sind im Parameter `-inputparam` enthalten.

Ausführen einer Diagnose über die Befehlszeilenschnittstelle

1. Geben Sie den folgenden Pfad in die Befehlszeilenschnittstelle ein: `cd C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise 4.0\win64_x64\scripts`.
2. Geben Sie den Befehl **`probeRun`** gemeinsam mit den erforderlichen Attributen und Parametern wie in der folgenden Tabelle beschrieben ein:

Attribute/Parameter	Beschreibung	Beispiel:
`-auth`	Authentifizierungstyp	secEnterprise
`-cms`	CMS-Name	localhost:6400
`-cuid`	CUID der Diagnose	
`-help`	Hilfe für diese Anwendung drucken	
`-id`	ID der Diagnose	
`-name`	Diagnosename	BI-Launchpad
`-password`	Kennwort zum Ausführen der Diagnose (Groß- und Kleinschreibung beachten)	Kennwort1
`-resultdir`	Speicherverzeichnis für das Diagnoseergebnis	C:\Diagnoseergebnisse
`-username`	Benutzername zum Ausführen der Diagnose	Administrator

> **Hinweis**
>
> Wenn Sie eine Diagnose durchführen, brauchen Sie lediglich einen der folgenden Parameter anzugeben: `-cuid`, `-id`, `-name`. Wird mehr als einer dieser Parameter angegeben, tritt ein Fehler auf.

Löschen einer Diagnose über die Befehlszeilenschnittstelle

1. Geben Sie den folgenden Pfad in die Befehlszeilenschnittstelle ein: `cd C:\Programme (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise 4.0\win64_x64\scripts`.
2. Geben Sie den Befehl **`probeDelete`** gemeinsam mit den erforderlichen Attributen und Parametern wie in der folgenden Tabelle beschrieben ein:

Attribute/Parameter	Beschreibung	Beispiel:
`-auth`	Authentifizierungstyp	secEnterprise
`-cms`	CMS-Name	localhost:6400
`-cuid`	CUID der Diagnose	
`-help`	Hilfe für diese Anwendung drucken	
`-id`	ID der Diagnose	

Attribute/Parameter	Beschreibung	Beispiel:
`-name`	Diagnosename	BI-Launchpad
`-password`	Kennwort zum Löschen der Diagnose (Groß- und Kleinschreibung beachten)	Kennwort1
`-username`	Benutzername zum Löschen der Diagnose	Administrator

> **Hinweis**
>
> Wenn Sie eine Diagnose löschen, brauchen Sie lediglich einen der folgenden Parameter anzugeben: `-cuid`, `-id`, `-name`. Wird mehr als einer dieser Parameter angegeben, tritt ein Fehler auf.

25.2.3.2.7 Hinzufügen neuer Diagnosen

Das Überwachungstool der BI-Plattform wird mit mehreren Standarddiagnosen ausgeliefert. Zusätzlich zu diesen Standarddiagnosen können Sie Ihre eigenen benutzerdefinierten Diagnosen erstellen und zum Überwachungstool hinzufügen. Durch Verwenden der bereitgestellten SDKs können Sie eine neue Diagnose erstellen.

Weitere Informationen zum Erstellen einer neuen Diagnose finden Sie im *SAP BusinessObjects Java Developer Guide*.

25.2.3.2.8 Registrieren von Java-basierten Diagnosen

Sie können Java-basierte Diagnosen registrieren, indem Sie die folgenden Schritte durchführen:

1. Wählen Sie unter *Diagnosen* die Option + und anschließend Java Based Probe .
   Der Bildschirm *Diagnosen registrieren* wird angezeigt.
2. Geben Sie die Details in den Feldern *Diagnosename*, *Beschreibung*, *Zeitüberschreitung* und *Klassenname* ein.

   > **Hinweis**
   >
   > Geben Sie im Feld *Klassenname* den vollständigen Klassennamen, einschließlich des Paketnamens, ein. Beispiel: **`com.businessobjects.monitoring.probe.CMSLogOnOffProbe`**.

3. Wählen Sie den *Diagnosetyp* aus.
4. Klicken Sie auf *Hinzufügen*, um die Eingabeparameter, wie z.B. Benutzername und Kennwort, zum Ausführen der Diagnose einzugeben. Der Name und der Typ dieser Eingabeparameter sollte mit dem Namen und dem Eingabetyp der Implementierungsklasse übereinstimmen.

25.2.3.2.9 Registrieren von skriptbasierten Diagnosen

Um skriptbasierte Diagnosen zu registrieren, führen Sie folgende Schritte aus:

1. Klicken Sie auf der Registerkarte *Diagnosen* auf *Registrieren* > *Skriptdiagnose*.
   Das Fenster *Diagnoseregistrierung* wird angezeigt.
2. Geben Sie den *Diagnosenamen* ein.
3. Wählen Sie den *Diagnose-Eingabetyp* aus. Wenn der ausgewählte Diagnose-Eingabetyp "Befehlszeile" ist, geben Sie den Befehl in das Feld *Befehl* ein; andernfalls führen Sie eine Suche aus und wählen den Speicherort der Skriptdatei im Feld *Skriptdatei* aus.
4. Um eine virtuelle Metrik zu definieren, aktivieren Sie das Kontrollkästchen *Virtuelle Metrik definieren*.
   - *Begrenzungszeichen definieren* – Geben Sie hier das zum Analysieren der Ausgabe zu verwendende Begrenzungszeichen ein. Der Administrator sollte sicherstellen, dass das Begrenzungszeichen die Ausgabe richtig analysiert.
   - *Ausgabetyp* – Eine Diagnose kann entweder als *Tabellenausgabe* oder als *Schlüsselwertausgabe* ausgegeben werden. Wenn Sie *Tabellenausgabe* auswählen, geben Sie die *Metrik-ID-Spalte* und *Metrikwerte-Spaltennummern* ein.

25.2.4 Kontrollmodule

Kontrollmodule stellen den Echtzeit-Status sowie Verlaufstrends von Servern und Workflows innerhalb der BI-Plattform bereit. Benutzer können einem Kontrollmodul Schwellenwerte und Warnmeldungen zuordnen. Sie können ein Kontrollmodul unter Verwendung der Daten aus Diagnosemetriken, Servermetriken oder einer Kombination aus beiden erstellen. Kontrollmodule unterstützen Sie bei Verständnis und Optimierung der Systemfunktionalität und -leistung der BI-Plattform.

Die mit dem Kontrollmodul verknüpfte Ampel zeigt zu jedem beliebigen Zeitpunkt den Kontrollmodulstatus an. Sie können die Anzahl an Statuswerten in eines Kontrollmoduls auf 2 oder 3 festlegen.

- Anzahl an Statuswerten = 2: Es findet nur ein Übergang statt. Wenn der festgelegte Schwellenwert eines Kontrollmoduls überschritten wird, wechselt die verknüpfte Ampel von grün auf rot oder umgekehrt.
- Anzahl an Statuswerten = 3: Es finden zwei Übergänge statt, und die verknüpfte Ampel wechselt von grün auf gelb und dann von gelb auf rot oder umgekehrt.

Sie können Kontrollmodule sowohl auf der Seite *Kontrollmodulliste* als auch auf der Seite *Dashboard* anzeigen. Auf der Seite *Kontrollmodulliste* können Sie die Liste der Kontrollmodule sowie wichtige Informationen wie Kontrollmodulstatus, -typ, -beschreibung anzeigen. Darüber hinaus können Sie anzeigen, ob die E-Mail-Benachrichtigungen gestoppt oder fortgesetzt werden. Auf der Seite "Kontrollmodulliste" wird nur der Servername angezeigt. Positionieren Sie den Cursor über dem Knoten, um den vollständigen Servernamen anzuzeigen. Wenn ein Kontrollmodul ausgewählt wird, wird ein Diagramm auf Grundlage der Metrikdaten angezeigt. Dieses Diagramm kann sowohl im Live-Modus als auch im Verlaufsmodus angezeigt werden. Standardmäßig wird es jedoch im Live-Modus angezeigt. Auf der Seite *Kontrollmodulliste* können Sie eine neues Kontrollmodul erstellen. Sie können außerdem die Kontrollmoduldetails anzeigen, die E-Mail-Benachrichtigungseinstellungen eines vorhandenen Kontrollmoduls kopieren, bearbeiten oder ändern, E-Mail-Benachrichtigungen anhalten oder fortsetzen und Kontrollmodule den Favoriten hinzufügen.

25.2.4.1 Kontrollmodultypen

Kontrollmodule können folgendermaßen eingeteilt werden:

- Systemkontrollmodule: Kontrollmodule, die im Lieferumfang des Überwachungstools der BI-Plattform enthalten sind. Standardmäßig ist jedem Servertyp ein Systemkontrollmodul zugeordnet. Standardkontrollmodule können nicht gelöscht werden. Sie können sie jedoch anpassen, indem Sie die Metriken ändern und die Schwellenwerte bearbeiten. Sie können diese Kontrollmodule sogar kopieren und ein Kontrollmodul mit Ihren eigenen Metriken und Schwellenwerten erstellen. Die Verknüpfung eines Kontrollmoduls mit einem Server kann nicht geändert werden.
- Vom Benutzer erstellte Kontrollmodule: Kontrollmodule, die Sie selbst erstellen. Sie können ein Kontrollmodul mit Metriken Ihrer Wahl erstellen und die Schwellenwerte und Warnmeldungen festlegen. Darüber hinaus können Sie ein Systemkontrollmodul kopieren und sie an Ihre Anforderungen anpassen. Vom Benutzer erstellte Kontrollmodule können gelöscht werden. Ein vom Benutzer erstelltes Kontrollmodul kann keinem Server zugeordnet werden.

25.2.4.2 Erstellen eines neuen Kontrollmoduls

Sie können das neue Kontrollmodul entweder auf der Seite *Dashboard* oder auf der Seite *Kontrollmodulliste* erstellen. Klicken Sie auf der Seite *Dashboard* auf .

und auf der Seite "Kontrollmodulliste" auf .

1. Navigieren Sie zum Bereich *Überwachung* der CMC, und wählen Sie die Registerkarte *Kontrollmodulliste*.
2. Klicken Sie auf , und legen Sie die Eigenschaften und Optionen, wie in den folgenden Abschnitten beschrieben, fest:

   > **Hinweis**
   >
   > Die ausgewählte Metrik wird standardmäßig im Bereich *Hinzugefügte Metriken* angezeigt.

Allgemeine Eigenschaften

Auf dem Bildschirm *Neues Kontrollmodul – Allgemeine Eigenschaften* können Sie den *Namen*, die *Beschreibung*, die *Statusanzahl* und die *Einstellungen* festlegen. Um die allgemeinen Eigenschaften festzulegen, führen Sie folgende Schritte aus:

1. Geben Sie den Namen und die Beschreibung in die entsprechenden Felder ein.
2. Wählen Sie *Statusanzahl*, um die Anzahl an Schwellenwerten festzulegen.
   Wenn Sie zwei Statuswerte auswählen, ändert sich der Kontrollmodulstatus von grün in rot oder umgekehrt. Wenn Sie drei Statuswerte auswählen, ändert sich der Kontrollmodulstatus von grün in gelb, gelb in rot oder umgekehrt.

> **Hinweis**
>
> Wählen Sie *Schreiben in Trenddatenbank* aus, um das Kontrollmodulergebnis in der Trenddatenbank zu speichern. Anhand dieser Daten können Sie Trenddiagramme anzeigen.

3. Wählen Sie *Schritt 2*.

Regel für Achtung

Auf dem Bildschirm *Neues Kontrollmodul – Regel für Achtung* können Sie Metriken hinzufügen, Schwellenwerte festlegen und den aktuellen Status des zu erstellenden Kontrollmoduls anzeigen. Führen Sie folgende Schritte aus, um die Einstellungen für den Achtungsstatus festzulegen:

1. Wählen Sie die Metriken im Bereich *Verfügbare Metriken* aus, und klicken Sie auf .
   Die Option *Filter* ermöglicht Ihnen die Suche von Metriken aus der bestehenden Liste.
   Der boolesche Operator für zwei Metriken lautet standardmäßig `(AND) &&`. Sie können den booleschen Operator in `(OR) ||` ändern, indem Sie die Dropdown-Liste unter der Metrik verwenden.
   Nachdem die Metriken hinzugefügt wurden, wird der boolesche Ausdruck der hinzugefügten Metriken angezeigt. Sie können den booleschen Ausdruck bearbeiten. Der boolesche Ausdruck muss das Format `NodeName.ServerName$'MetricName'>=ThresholdValue` aufweisen. Dies ist ein Beispiel für einen booleschen Ausdruck:

   ```
   <Node_name>.CentralManagementServer$'Completed Jobs'>=1
   ```
2. Wählen Sie den Operator aus der Dropdown-Listea aus, und legen Sie anschließend den Schwellenwert fest.
   Die folgende Tabelle enthält die verfügbaren Operatoren, die Sie zum Festlegen des Schwellenwerts verwenden können:

Operatoren	Beschreibung
>=	Größer als oder gleich
<=	Kleiner als oder gleich
>	Größer als
<	Kleiner als
==	gleich
!=	ungleich

   Klicken Sie auf , um den aktuellen Status des Ausdrucks anzuzeigen.
3. Wählen Sie *Schritt 3*.

Regel für Gefahr

Der Bildschirm *Neues Kontrollmodul – Regel für Gefahr* wird nur dann angezeigt, wenn die Anzahl der ausgewählten Statuswerte drei entspricht. Auf dem Bildschirm *Neues Kontrollmodul – Regel für Gefahr* können

Sie Metriken hinzufügen, Schwellenwerte festlegen und den aktuellen Status des Kontrollmoduls anzeigen, das Sie erstellen. Die für die Achtungsstatus angegebenen Werte werden standardmäßig im Bildschirm der Gefahr-Regel beibehalten. Wenn Sie dieselbe Metrik beibehalten möchten, müssen Sie den Operator oder den Schwellenwert ändern. Sie können diese Metrik-Einstellungen auch löschen. Führen Sie folgende Schritte aus, um die Einstellungen für den Gefahrenstatus festzulegen:

1. Wählen Sie die Metriken im Bereich *Verfügbare Metriken* aus, und klicken Sie auf .
2. Wählen Sie den Operator aus der Dropdown-Listea aus, und legen Sie anschließend den Schwellenwert fest. Klicken Sie auf , um den aktuellen Status des Ausdrucks anzuzeigen.
3. Wählen Sie *Schritt 4*.

Kriterien und Benachrichtigung

Auf dem Bildschirm *Neues Kontrollmodul – Kriterien und Benachrichtigung* können Sie E-Mail-Benachrichtigungen aktivieren und festlegen, wie der Kontrollmodulstatus auf den Seiten *Dashboard* und *Kontrollmodulliste* angezeigt wird. Sie können entweder auswählen, dass der Kontrollmodulstatus für jede Schwellenwertüberschreitung geändert wird, oder Sie können Bedingungen dafür festlegen.

1. Wenn der Kontrollmodulstatus bei jeder Schwellenwertüberschreitung geändert werden soll, wählen Sie *Kontrollmodulstatus jedes Mal ändern, wenn die Auswertung der Achtung- oder Gefahr-Regel "wahr" ergibt* aus. Immer wenn die Achtung- oder Gefahr-Regel "wahr" ergibt, ändert sich der Kontrollmodulstatus in den entsprechenden Status. Wenn sowohl die Achtung- als auch die Gefahr-Regel "wahr" ergeben, ändert sich der Kontrollmodulstatus in rot.
2. Wenn sich der Kontrollmodulstatus in Abhängigkeit von einem Schwellwert ändern soll, wählen Sie *Kontrollmodulstatus anhand der im Folgenden angegebenen Schwellwerte ändern* und legen die im Folgenden beschriebenen Einstellungen für *Kriterien für Status "Achtung"* und *Kriterien für Status "Gefahr"* fest:

   Wählen Sie *Wenn die Regelauswertung "wahr" ergibt für die letzten*, und geben Sie die erforderliche Zeitdauer an. Die Zeitdauer kann in Tagen, Stunden, Minuten oder Sekunden angegeben werden. Wenn Sie zum Beispiel diese Option wählen und eine Zeitdauer von 5 Minuten für die Achtung-Regel festlegen, und wenn die Achtung-Regel "wahr" ergibt, ändert sich der Kontrollmodulstatus in gelb. Auf dieselbe Weise können Sie die Regel für Gefahr festlegen. Wenn sowohl die Achtung- als auch die Gefahr-Regel "wahr" ergeben, ändert sich der Kontrollmodulstatus in rot.

   Wenn Sie möchten, dass sich der Kontrollmodulstatus erst nach einer bestimmten Anzahl von Überschreitungen ändert, wählen Sie *Auf _ wahre Auswertung(en) in den letzten _ warten*, und geben die Anzahl von Auswertungen mit dem Ergebnis "wahr" sowie die Zeitdauer an. Wenn Sie beispielsweise die Anzahl an wahren Auswertungen auf 20 und die Dauer auf 5 Tage festlegen, ändert sich der Kontrollmodulstatus nur dann, wenn die Anzahl an wahren Auswertungen innerhalb von 5 Tagen über 20 steigt. Wenn sowohl die Achtung- als auch die Gefahr-Regel "wahr" ergeben, ändert sich der Kontrollmodulstatus in rot.
3. Wenn Sie möchten, dass Aktionen ausgeführt werden, wenn der Kontrollmodulstatus sich ändert, wählen Sie *Aktion konfigurieren* und wählen die entsprechende Diagnose in der Dropdown-Liste *Diagnose ausführen* aus. Wenn Sie beispielsweise ein Kontrollmodul mit drei Status erstellt haben, können Sie eine Diagnose konfigurieren, die ausgeführt wird, wenn der Kontrollmodulstatus gelb ist und wenn er sich in rot ändert.

4. Wählen Sie die Option *Warnungsbenachrichtigungen aktivieren* in *Benachrichtigungseinstellungen*, um Warnmeldungen zu aktivieren.
   Die Warnungen werden auf Grundlage von Änderungen des Kontrollmodulstatus generiert:

Vorheriger Kontrollmodulstatus	Aktueller Kontrollmodulstatus	Warnung generiert?
Grün	Rot	Ja
Gelb	Rot	Ja
Grün	Gelb	Ja
Rot	Grün	–
Gelb	Grün	–
Grün	Grün	–
Gelb	Gelb	Nein
Rot	Rot	Nein
Rot	Gelb	Nein

5. Klicken Sie auf *Verzeichnis*. Die Seite "Verzeichnis" wird geöffnet.
6. Wenn Sie einzelne E-Mails hinzufügen möchten, geben Sie die E-Mail-ID ein, und klicken Sie auf *E-Mail-Empfänger hinzufügen*, oder wählen Sie den Benutzer- oder Gruppennamen aus der Tabelle aus, klicken Sie auf *Warnmeldungseinstellungen*, und wählen Sie die erforderlichen Optionen aus.
7. Wenn Sie detaillierte Informationen zu den Metriken benötigen, die die Warnmeldung ausgelöst haben, wählen Sie *Metriktrendverlauf als Anlage hinzufügen*. Es wird ein Diagramm der Verlaufsmetrikdaten an die Warnmeldung angehängt. Das Diagramm enthält Daten für 10 Minuten, beginnend ab dem Zeitpunkt, zu dem die Warnmeldung ausgelöst wurde.
8. Klicken Sie auf *Überprüfen*, und wählen Sie anschließend *Speichern*, um die Erstellung eines neuen Kontrollmoduls abzuschließen.

> **Hinweis**
>
> Sie können *Kriterien für Status "Achtung"* kopieren, indem Sie das Kontrollkästchen zur Anwendung der Kriterien für den Status "Achtung" in *Kriterien für Status "Gefahr"* aktivieren.

25.2.4.3 Verwalten von Kontrollmodulen

Auf der Seite *Kontrollmodulliste* des Überwachungstools werden alle Kontrollmodule zusammen mit Status, Typ und Beschreibung angezeigt. Wenn ein Kontrollmodul ausgewählt wird, wird ein Diagramm auf Grundlage der Metrikdaten angezeigt. Sie können alle Kontrollmodule anzeigen, Kontrollmodule auf Grundlage ihres Status filtern oder Kontrollmodule anzeigen, die als Favoriten hinzugefügt werden, indem Sie die Option *Anzeigen* verwenden. Um beispielsweise Kontrollmodule anzuzeigen, die KPIs sind, wählen Sie *Anzeigen* > *KPIs*

Auf der Seite *Kontrollmodulliste* können Sie ein Kontrollmodul bearbeiten, kopieren oder löschen, Kontrollmoduldetails prüfen, E-Mail-Benachrichtigungen aktivieren oder deaktivieren, Kontrollmodule zu den Favoriten hinzufügen und regenerieren.

E-Mail-Benachrichtigungen

Sie können E-Mail-Benachrichtigungen für ein bestimmtes Kontrollmodulaktivieren oder deaktivieren, indem Sie die Schaltfläche *E-Mail-Benachrichtigungen* verwenden. Die Spalte *Attribute* zeigt an, ob die E-Mail-Benachrichtigung für ein Kontrollmodul angehalten wurde oder fortgesetzt wird.

Hinzufügen eines Kontrollmoduls zu den Favoriten

Sie können auf die Schaltfläche *Zu Favoriten hinzufügen* klicken, um Kontrollmodule zu Ihrer Favoritenliste hinzuzufügen. Anschließend können Sie nur Ihre Favoriten-Kontrollmodule anzeigen, indem Sie in der Liste *Anzeigen* die Option *Favoriten* auswählen. Die zu den Favoriten hinzugefügten Kontrollmodule sind benutzerspezifisch und können nicht von anderen Benutzern angezeigt werden.

Regenerieren von Kontrollmodulen

Mit der Option *Automatische Regenerierung aktivieren* können Sie die Kontrollmodule automatisch regenerieren. Sie können die Kontrollmodule auch manuell regenerieren, indem Sie auf klicken.

25.2.4.3.1 Bearbeiten von Kontrollmodulen

Sie können ein Kontrollmodul bearbeiten und nach Bedarf anpassen. Sie können jedoch die Serverzuordnung der Kontrollmodule nicht ändern. Führen Sie zum Bearbeiten eines Kontrollmoduls die folgenden Schritte durch:

1. Wählen Sie aus der Liste der Kontrollmodule ein Kontrollmodul aus, und klicken Sie auf .
2. Wählen Sie im Kopfbereich eine Registerkarte aus, um die Details dieser Registerkarte zu bearbeiten:

Optionen	Beschreibung
Allgemeine Eigenschaften	Sie können Informationen bezüglich Name, Beschreibung, Statusanzahl und Einstellungen des ausgewählten Kontrollmoduls bearbeiten.
Regel für Achtung	Sie können die Einstellungen für die Achtungsregel bearbeiten, die mit den verfügbaren Metriken, hinzugefügten Metriken und dem aktuellen Kontrollmodulstatus in Zusammenhang stehen.

Optionen	Beschreibung
Regel für Gefahr	Sie können die Einstellungen für die Gefahrenregel bearbeiten, die mit den verfügbaren Metriken, hinzugefügten Metriken und dem aktuellen Kontrollmodulstatus in Zusammenhang stehen.
Kriterien und Benachrichtigung	Sie können Informationen zu E-Mail-Benachrichtigungen bearbeiten.

3. Wählen Sie *Speichern*.

25.2.4.3.2 Kopieren oder Löschen von Kontrollmodulen

So kopieren Sie ein Kontrollmodul

Das Überwachungstool enthält eine Option zum Kopieren von Kontrollmodulen. Beim Kopieren eines Kontrollmoduls wird ein neues Kontrollmodul mit denselben Informationen und Einstellungen erstellt. Das kopierte Kontrollmodul erhält denselben Namen und bekommt eine Zahl angehängt. Wenn Sie beispielsweise ein Kontrollmodul mit dem Namen AdaptiveJovServer-Kontrollmodul kopieren, wird ein neues Kontrollmodul mit dem Namen AdaptiveJobServer-Kontrollmodul(2) erstellt.

Um ein Kontrollmodul zu kopieren, wählen Sie es aus der Kontrollmodulliste aus, und klicken auf *Kopieren*.

> ⓘ Hinweis
>
> Jedes Standardkontrollmodul wird einem Server zugeordnet. Beim Kopieren eines Kontrollmoduls wird die Serverzuordnung aus dem kopierten Kontrollmodul entfernt.

So löschen Sie ein Kontrollmodul

Standardkontrollmodule können nicht gelöscht werden, von Benutzern erstellte Kontrollmodule jedoch schon. So löschen Sie ein von einem Benutzer erstelltes Kontrollmodul:

1. Wählen Sie das Kontrollmodul aus, und klicken Sie auf *Löschen*.
2. Klicken Sie auf *OK* im Bestätigungsdialogfeld *Löschen*.

Sie können auch mehrere Kontrollmodule gleichzeitig löschen, indem Sie mehrere Kontrollmodule auswählen und auf *Löschen* klicken.

25.2.4.3.3 Anzeigen von Kontrollmoduldetails

1. Wählen Sie ein Kontrollmodul aus, und klicken Sie auf *Details*.

2. Im Dialogfeld *Kontrollmoduldetails* werden die "Allgemeinen Eigenschaften" und die "Kontrollmodulregel" des ausgewählten Kontrollmoduls angezeigt:

Option	Beschreibung
Allgemeine Eigenschaften	Gibt Namen, Status, Beschreibung des Kontrollmoduls, gelesene und ungelesene Warnmeldungen, die letzte Warnmeldung, die Einstellungen für den Gefahren- und Achtungsstatus und die Abonnenten des Posteingangs an.
Kontrollmodulregel	Gibt Informationen zum aktuellen Status der in den Achtungs- und Gefahreneinstellungen verwendeten Metriken sowie zum Diagramm, das auf dem Metrikstatus basiert. Sie können das Diagramm im Live- oder Verlaufsmodus anzeigen.

25.2.4.3.4 Deaktivieren von Kontrollmodulen

Im Überwachungstool der BI-Plattform stehen zahlreiche Kontrollmodule zur Verfügung. Sie haben die Möglichkeit, ein Kontrollmodul zu deaktivieren und bei Bedarf erneut zu aktivieren. Wenn ein Kontrollmodul deaktiviert wird, wird der Kontrollmodulstatus nicht berechnet. Wird ein Kontrollmodul daher für einen festgelegten Zeitraum deaktiviert:

- zeigt der Kontrollmodulstatus für diesen Zeitraum keine Daten im Diagramm an.
- zeigen Metriken, die Teil des deaktivierten Kontrollmoduls, jedoch nicht Teil eines anderen Kontrollmoduls sind, für diesen Zeitraum ebenfalls keine Daten im Diagramm an.

- Wählen Sie das Kontrollmodul aus, klicken Sie auf und anschließend auf *Kontrollmodul deaktivieren*.
- Klicken Sie im Bestätigungsdialogfeld zum *Löschen* auf *OK*.

Sie können auch mehrere Kontrollmodule gleichzeitig deaktivieren, indem Sie mehrere Kontrollmodule auswählen und auf *Kontrollmodul deaktivieren* klicken.

> **Hinweis**
>
> Nur die Administratorgruppen und die Benutzer, die das Kontrollmodul erstellt haben, verfügen über Berechtigungen zur Aktivierung oder Deaktivierung der Kontrollmodule.

25.2.4.4 Suchen nach einem Kontrollmodul

Die Seite "Kontrollmodulliste" enthält ein Suchfeld, über das Sie vorhandene Kontrollmodule suchen können.

Suchen nach einem Kontrollmodul über den Kontrollmodulnamen

1. Navigieren Sie zur Seite *Kontrollmodulliste*.
2. Wählen Sie im Suchkombinationsfeld *Nach Kontrollmodulname suchen*.
3. Geben Sie in das Suchfeld den Namen des Kontrollmodus ein, das Sie suchen möchten, und klicken Sie auf das Suchsymbol.

Suchen nach einem Kontrollmodul über den Metriknamen

1. Wählen Sie im Suchkombinationsfeld *Nach Metrikname suchen*.
2. Geben Sie den Namen der Metrik in das Suchfeld ein, und klicken Sie auf das Suchsymbol.

25.2.5 Metriken

Auf der Seite "Metriken" werden alle Metriken angezeigt, die aus den Diagnosen und Servern generiert wurden. Sie können Metriken aus dem linken Bereich auswählen, um sie im Bereich *Ausgewählte Metriken anzeigen* anzuzeigen. Mit der Option *Suche* können Sie nur die erforderlichen Metriken anzeigen.

> ⓘ Hinweis
>
> Die mit der Standarddiagnose generierten Metriken sind `Ausführungszeit` und `Erfolgreich`. Das Diagnoseergebnis wird von der Metrik `Erfolgreich` dargestellt, die einen der folgenden Werte annehmen kann:
>
> - 0 bedeutet, dass die Diagnose fehlgeschlagen ist.
> - 1 bedeutet, dass die Diagnose erfolgreich war.
> - 2 bedeutet, dass bei der Diagnose eine Zeitüberschreitung aufgetreten ist.
>
> Benutzer können jedoch beim Erstellen eines neuen Diagnosen eine beliebige Anzahl an Metriken für die Anzeige festlegen. Diese Metriken werden als virtuelle Metriken bezeichnet. Eine ausführliche Liste der Servermetriken finden im Anhang *Servermetriken*.

Im Bereich *Ausgewählte Metriken anzeigen* werden die ausgewählten Metriken gemeinsam mit dem Metrikwert sowie mit Datum und Uhrzeit angezeigt. Jede ausgewählte Metrik zeigt auch das Diagramm an, welches Sie im Live- oder Verlaufsmodus darstellen können. Wählen Sie *Alle zuklappen*, um die Diagramme auszublenden. Wählen Sie *Zeitachsen synchronisieren*, um mehrere Diagramme mit demselben Zeitbereich anzuzeigen.

Servermetriken über SAPOSCOL

Serverebenenmetriken wie etwa CPUcount, FreeMemory und PhysicalMemory können durch die Installation von SAPOSCOL angezeigt werden. Zum Abrufen dieser Metriken aktivieren Sie die Hostmetriken in den Überwachungstool-Eigenschaften und geben den Pfad zur Installation von SAPOSCOL an. Nach Aktivierung der Hostmetriken können diese Metriken auf der Seite "Metriken" und im Assistenten zur

Kontrollmodulerstellung angezeigt werden. Wählen Sie eine Servermetrik aus. Die QuickInfo zeigt nun den Dienstnamen dieser Servermetrik an.

Weitere Informationen

Info zu Servermetriken (Anhang) [Seite 537]

25.2.5.1 Abgeleitete Metriken

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.

Abgeleitete Metriken können im linken Bereich der Registerkarte *Metriken* angezeigt werden.

25.2.5.1.1 Erstellen einer abgeleiteten Metrik

1. Klicken Sie auf der Seite *Metriken* oder auf der Seite *Dashboard* auf *Metrik erstellen* oder auf .
2. Geben Sie den Metriknamen ein, und wählen Sie im linken Seitenbereich einen Server aus.
3. Wählen Sie die Metriken aus und klicken auf , um sie zur Metrikformel hinzuzufügen.
4. Geben Sie den Operator manuell in die Metrikformel ein. Die Operatoren Addition (+), Subtraktion (-), Multiplikation (*) und Division (/) werden unterstützt.
5. Prüfen Sie, ob die Metrikformel logisch korrekt ist, indem Sie auf *Auswerten* klicken.
6. Wählen Sie *Schritt 2*.
7. Wählen Sie *Metriken* > *Abgeleitete Metriken* > *OK*
8. Wählen Sie *Überprüfen*.
9. Klicken Sie auf *Speichern*.

> **Hinweis**
>
> Sie können die Metrik nur dann speichern, wenn die Metrikformel logisch korrekt ist.

Die neue abgeleitete Metrik wird unter dem entsprechenden Server auf der Seite *Metriken* angezeigt.

25.2.5.1.2 Bearbeiten einer abgeleiteten Metrik

Sie können die Formel einer abgeleiteten Metrik, aber nicht den Metriknamen oder den Server bearbeiten. Führen Sie zum Bearbeiten einer abgeleiteten Metrik die folgenden Schritte durch:

1. Wählen Sie eine Metrik im linken Bereich aus, und klicken Sie auf .
2. Überarbeiten Sie die Metrikformel wie gewünscht.
3. Prüfen Sie, ob die Metrikformel logisch korrekt ist, indem Sie auf *Auswerten* klicken.
4. Wählen Sie *Schritt 2*.
5. Wählen Sie *Metriken* > *Abgeleitete Metriken* > *OK*
6. Wählen Sie *Überprüfen*.
7. Klicken Sie auf *Speichern*.

25.2.6 Warnmeldungen

Eine Warnmeldung ist eine Benachrichtigung, die vom Überwachungstool generiert wird, wenn benutzerdefinierte Ausdrücke oder Regeln als True bewertet werden. Da Regeln und Ausdrücke mehrere Metriken und Schwellenwerte haben können, muss die gesamte Regel als True bewertet werden. Sie können auswählen, ob Sie die Warnmeldungen per E-Mail erhalten möchten, oder ob sie auf der *Dashboard*-Seite angezeigt werden sollen. In der Warnmeldungs-E-Mail werden Metriken hervorgehoben, die den Schwellwert überschritten haben und das Kontrollmodul dazu veranlasst haben, eine Warnmeldung auszugeben.

Beim Erstellen eines Kontrollmoduls können Sie Warnmeldungen aktivieren. Weitere Informationen zum Einrichten von Warnmeldungen erhalten Sie unter *Ereigniseinstellungen* in Erstellen eines neuen Kontrollmoduls [Seite 349].

Auf der Seite *Warnmeldungen* können Sie alle Überwachungs-Warnmeldungen, den Status, Namen und Text der Warnmeldung sowie die Uhrzeit, zu der die Warnmeldung generiert wurde, anzeigen. Wenn Sie auf den Warnmeldungsnamen klicken, wird die Seite *Warnmeldungsdetails* aufgerufen, die die folgenden Informationen enthält:

- Kontrollmodulname
- Warnmeldungseinstufung
- Zeitpunkt der Warnmeldung
- Die Regeln für den Achtungs- bzw. Gefahrenstatus sowie die Metriken und Metrikwerte zum Zeitpunkt der Warnmeldung.

Der Status *Ungelesen* der generierten Warnmeldungen wird zum Status *Gelesen*, nachdem Sie die Warnmeldungsdetails geprüft haben. Wenn Sie die der Warnmeldung entsprechende Aktion ausgeführt haben, können Sie den Status auf "Bestätigt" setzen.

In der folgenden Tabelle sind die Aktivitäten aufgeführt, die auf der Warnmeldungsseite ausgeführt werden können:

Option	Beschreibung
Durchsuchen	Ermöglicht die Auswahl eines Kontrollmoduls aus der Liste und die Anzeige der vom Kontrollmodul generierten Warnmeldungen.
Löschen	Ermöglicht die Anzeige der von allen Kontrollmodulen generierten Warnmeldungen.
Filter	Ermöglicht das Filtern der Warnmeldungen auf der Basis von drei Statuswerten: *Gelesen*, *Ungelesen* oder *Bestätigt*. **Hinweis** Der Warnmeldungsstatus wird auf *Gelesen* gesetzt, sobald Sie auf die Seite *Warnmeldungsdetails* dieser Warnmeldung zugreifen.
Bestätigen	Ermöglicht die Aufzeichnung der Ursache der Warnmeldung und der zu ihrer Lösung unternommenen Schritte. Nachdem Sie die der Warnmeldung entsprechende Aktion ausgeführt haben, können Sie die Warnmeldung auf den Status *Bestätigt* setzen. **Hinweis** Sobald Sie eine Warnmeldung auf *Bestätigt* setzen, wird der Warnmeldungsstatus auch auf *Gelesen* gesetzt.
Löschen	Ermöglicht das Löschen einer Warnmeldung.

Erinnerungswarnmeldungen

Sie erhalten Erinnerungswarnmeldungen, wenn Sie nicht auf die erste Warnmeldung reagiert haben. Angenommen, eine Warnmeldung wurde gesendet, nachdem ein Kontrollmodul seinen Schwellwert erreicht hat. Falls Sie die Warnmeldung nicht das erste Mal, nachdem sie gesendet wurde, bestätigt haben, erhalten Sie Erinnerungswarnmeldungen. Nach Bestätigung einer Erinnerungswarnmeldung werden alle bereits für dasselbe Kontrollmodul ausgegebenen Warnmeldungen automatisch bestätigt.

25.2.7 Erstellen von Berichten für Überwachungsdaten

Zum Erstellen von Berichten zur Überwachung können Sie das im Ordner "„Universes > Monitoring TrendData Universes“" mitgelieferte Universum `Monitoring TrendData` verwenden. Sie können intuitive Berichte erstellen, um Überwachungsinformationen anzuzeigen, wie z.B. Berichte über Kontrollmoduldaten, Trendberichte über Kontrollmodule, Kontrollmodulverhalten über einen bestimmten Zeitraum, Diagnosetrends,

Drilldown eines Kontrollmoduls zu seinen Metriken usw. Zum Erstellen solcher Berichte müssen Sie einen SAP-BusinessObjects-Desktop-Client installieren, das Universe-Design-Tool und eine Berichtsanwendung wie Web Intelligence oder Crystal Reports verwenden.

25.3 Grafischer Vergleich

Mithilfe des grafischen Vergleichs können Sie die Unterschiede zwischen zwei Versionen einer LCMBIAR-Datei oder eines Objekts oder von 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.

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.

25.3.1 Vergleich von Objekten oder Dateien mittels des Grafischen Vergleichs

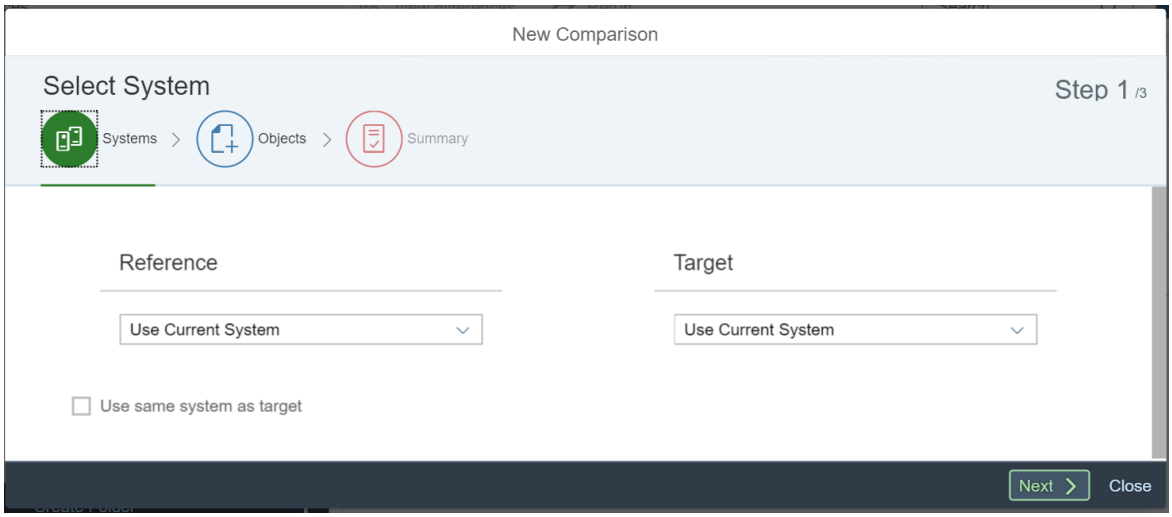
Um den Grafischen Vergleich von Dateien durchzuführen, gehen Sie folgendermaßen vor:

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**
   >
   > Wählen Sie zum Erstellen eines neuen Unterordners Create Folder +.

3. Wählen Sie +, um einen neuen Vergleich zu erstellen.

Der Assistent *Neuer Vergleich* wird angezeigt.



4. Wählen Sie in der Dropdown-Liste das *Referenz*- und das *Ziel*system aus.

   Sie können eine Verbindung zu einem der folgenden Referenz- und Zielsysteme herstellen:

   > **Hinweis**
   >
   > Beim Hinzufügen eines Objekts zum Versionsverwaltungssystem (VMS) wird im nächsten Schritt die Option zum Auswählen der Versionen angezeigt.

   - CMS
   - Lokales Dateisystem
5. Navigieren Sie auf dem Bild *Objektauswahl* zu einem Objekt oder einer Datei aus dem *Referenz*- und dem *Ziel*system, und wählen Sie das Objekt bzw. die Datei aus.
6. Ändern Sie bei Bedarf die *Bezeichnung des Vergleichs*.
7. Wählen Sie *Vergleichen*, um die Objekte zu vergleichen.

   > **Hinweis**
   >
   > - Sie können die Unterschiede überprüfen, indem Sie zuerst den Vergleich auswählen und anschließend die Option *Unterschiede anzeigen* wählen. Die Unterschiede werden in Orange hervorgehoben, und die fehlenden Objekte sind rot markiert.
   > - Sie können den Vergleich erneut vornehmen, indem Sie zuerst den Vergleich auswählen und anschließend die Option *Erneut ausführen* wählen.

   Der Vergleichsvorgang wird sofort gestartet.

   Um die verglichenen Objekte nach Typ und mit Unterschieden oder gemeinsamen Attributen anzuzeigen, können Sie auch die Filteroption verwenden.

25.3.2 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.

   > **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.
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*.

25.3.3 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.
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.

26 Auditing

26.1 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 in der SAP Community http://community.sap.com/ finden.

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 ausführen.

Einführung in das Audit

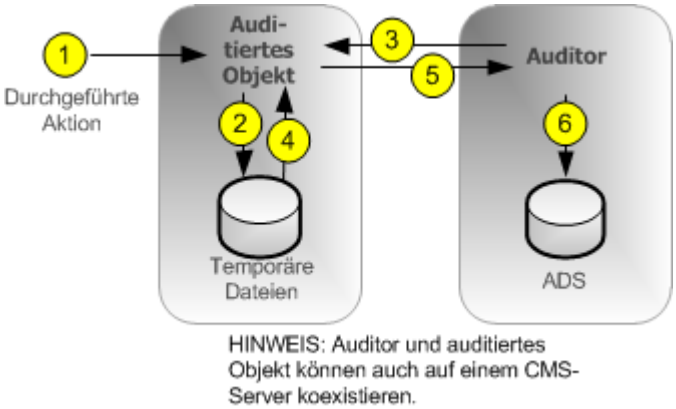
Der Central Management Server (CMS) fungiert als Systemauditor, während die einzelnen Server oder Anwendungen, die ein Audit-Ereignis auslösen, als auditiertes Objekt fungieren. Wenn ein auditiertes Ereignis ausgelöst wird, generiert das auditierte Objekt einen Datensatz und speichert ihn in einer lokalen 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

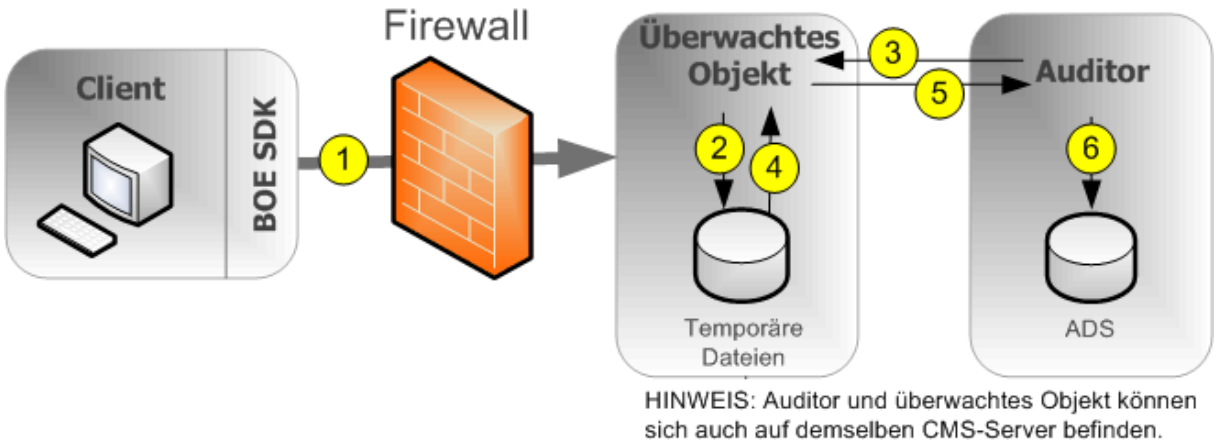
Der CMS kann bei vom Server generierten Ereignissen als auditiertes Objekt und als Auditor fungieren.



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.



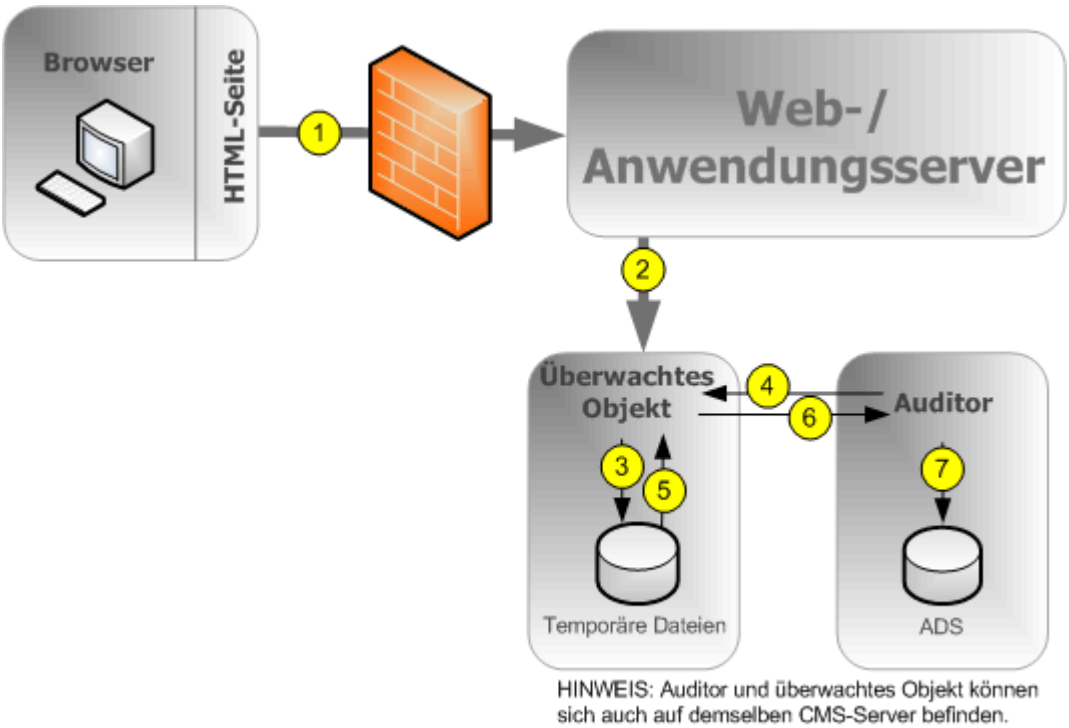
1. Der Client stellt eine Verbindung zum CMS her, der als auditiertes Objekt fungiert. Der Client stellt seine IP-Adresse und den Computernamen bereit, die vom auditierten Objekt überprüft werden.

> **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*.

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

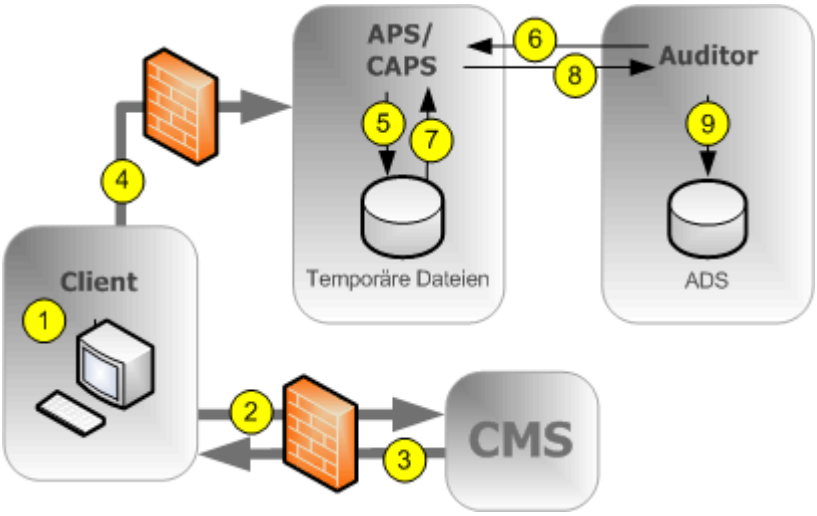
Dazu gehören Online-Anwendungen wie das BI-Launchpad, die Central Management Console, SAP BusinessObjects Web Intelligence usw.



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.

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.



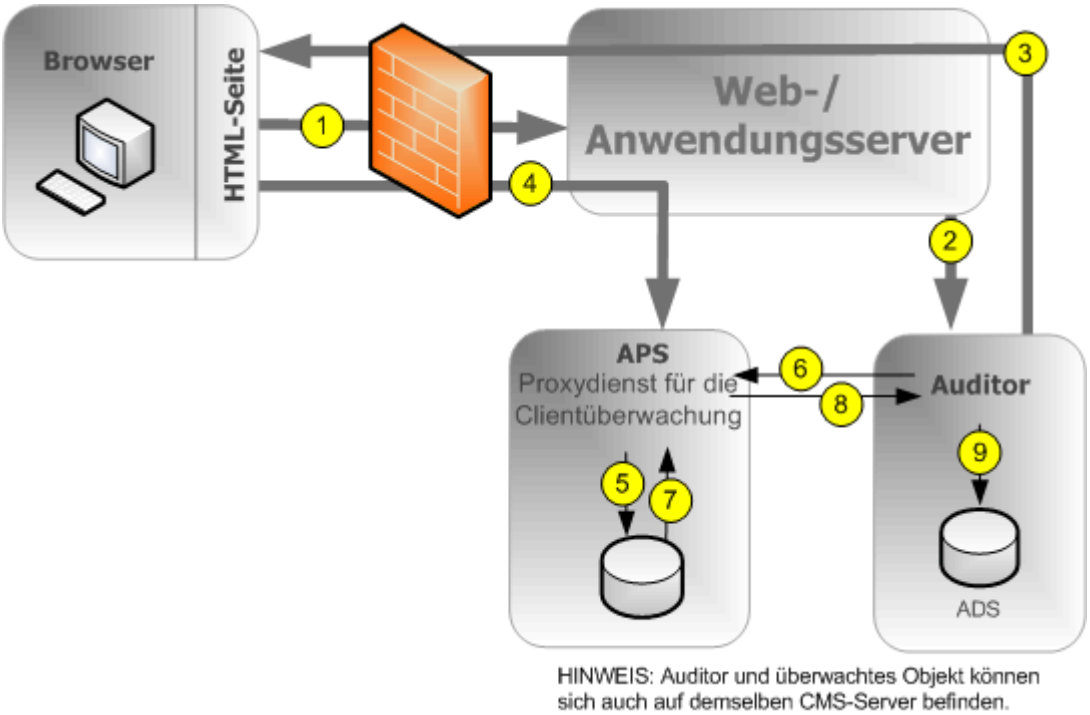
1. Der Benutzer führt einen Vorgang aus, der auditiert werden kann.
2. Der Client stellt eine Verbindung zum CMS her, um zu überprüfen, ob der Vorgang für die Auditierung konfiguriert ist.
3. Wenn die Aktion so eingestellt ist, dass sie auditiert werden muss, leitet der CMS diese Informationen an den 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**
   >
   > Zwischen jedem Client und jedem Adaptive Processing Server, der einen CAPS hostet, sowie zwischen den einzelnen Clients und dem CMS sollte ein Port in der Firewall 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.

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 das 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 das Audit an den Webanwendungsserver zurück, der diese Informationen wiederum an die Clientanwendung weitergibt.
4. Wenn das Ereignis für das Audit konfiguriert ist, sendet der Client die Ereignisinformationen an 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.

Clients, die das Auditing unterstützen

Die folgenden Clientanwendungen unterstützen das Auditing:

- Analysis, Edition for OLAP (AOLAP)
- BI-Launchpad (BILP)
- Business View Manager (BVM)
- Central Configuration Manager (CCM)
- Central Management Console (CMC)
- OpenDocument
- Information-Design-Tool (IDT)
- Live Office (LO)
- SAP BusinessObjects Mobile
- Übersetzungsmanagement-Tool (TMT)
- Web-Intelligence-Rich-Client (WIRC)
- Lumira-Desktop-Anwendung (Discovery)
- Lumira-Designer-Anwendung

> **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 maximale Auslastung. 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:

- 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 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 das Client-Audit erstellen. Dies gewährleistet die beste Systemleistung. Zum Erhöhen der Fehlertoleranz des Systems kann es sinnvoll sein, den CAPS auf mehreren APS auszuführen.

Verwandte Links

Server- und Knotenplatzhalter [Seite 556]

26.2 Seite CMC-Auditing

Die Seite *Auditing* in der CMC verfügt über folgende Bereiche:

- *Statusübersicht*
- *Ereignisse festlegen*
- *Ereignisdetails festlegen*
- *Konfiguration*

26.2.1 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 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 die Implementierung aktualisieren, damit der ADS Daten mit einer höheren Datenrate empfangen kann (z. B. durch schnellere Netzwerkverbindungen oder leistungsstärkere Datenbankhardware), oder die Anzahl der vom 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

Metrik	Details
	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. • 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.

26.2.2 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
>
> Audit-Ereignisse werden im Batchmodus und nicht einzeln an die Audit-Datenbank gesendet. Die Stapelgröße für Audit-Ereignisse beträgt derzeit 1000.

> ⓘ 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).*

26.2.2.1 Audit-Ereignisse konfigurieren

Führen Sie die folgenden Schritte aus, um die Audit-Ereignisse zu konfigurieren:

1. Wählen Sie in der Central Management Console die Registerkarte *Auditing*.
   Die Seite *Auditing* wird angezeigt.
2. Stellen Sie den Schieberegler *Ereignisse festlegen* auf die gewünschte Audit-Ebene ein, wobei jede Ebene einem bestimmten Metrikwert entspricht.
   - *Aus* – 1
   - *Minimal* – 2
   - *Standard* – 3
   - *Vollständig* – 4
   - *Benutzerdefiniert* – 0

   Die folgende Tabelle enthält die unterschiedlichen Einstellungen des Schiebereglers und die auf den einzelnen Ebenen erfassten Ereignisse.

Audit-Ebene	Erfasste Ereignisse
Aus	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

Audit-Ebene	Erfasste Ereignisse
	• 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 **Hinweis** Sie können weitere Ereignisse anzeigen, wenn die Add-Ons installiert sind.
Benutzerdefiniert	Sie wählen einen benutzerdefinierten Satz von Ereignissen aus.

Hinweis

Wenn *Ereignisse festlegen* auf *Standard* gesetzt ist, hat die *Audit-Ebene* den Wert 3.

Wenn *Ereignisse festlegen* auf *Aus* gesetzt ist, ändert sich der Wert der *Audit-Ebene* von 3 in 1.

3. Wählen Sie *Benutzerdefiniert*, und klicken Sie in der Liste unter dem Schieberegler *Ereignisse festlegen* auf die Ereignisse, die Sie erfassen möchten.
4. Klicken Sie unter *Ereignisdetails festlegen* auf die optionalen Details, die Sie zusammen mit den Ereignissen erfassen möchten. Wenn Sie weniger Details erfassen, wird die Systemleistung verbessert.

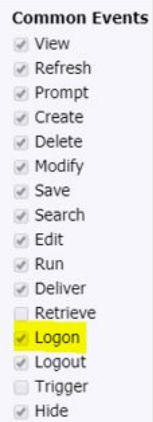
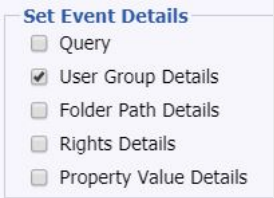
Information	Beschreibung
Abfrage	Wenn eingestellt, wird das Ereignisdetail *Abfrage* (Detail-ID 25) für jedes Ereignis aufgezeichnet, das eine Datenbank abfragt.
Ordnerpfaddetails	Wenn eingestellt, werden die folgenden Details erfasst: • *Objektordnerpfad (Detail-ID 71)* • *Name des obersten Ordners (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:

Information	Beschreibung
	• *Benutzergruppenname (Detail-ID 16)* • *Benutzergruppen-ID (Detail-ID 15)*
Eigenschaftswertdetails	Wenn eingestellt, wird das Ereignisdetail *Eigenschaftswert* (Detail-ID 29) erfasst, wenn die Eigenschaften eines Objekts aktualisiert werden. Dies wird nur für CMC-, BI-Launchpad- und SharePoint-Ereignisse generiert.

5. Klicken Sie auf *Speichern*.

> **Hinweis**
>
> Beim Client-Auditing kann es nach einer Änderung bis zu zwei Minuten dauern, bis das System beginnt, Daten für neue Ereignisse aufzuzeichnen. Berücksichtigen Sie diese Verzögerung, wenn Sie Änderungen im System implementieren.

26.2.2.2 Erweiterte Ereignisdetailaufzeichnung in Audit-Detailtabellen

> **Hinweis**
>
> - Sie müssen über ausreichende Kenntnisse in Bezug auf Seite CMC-Auditing [Seite 370] verfügen, insbesondere auf *Allgemeine Ereignisse, Ereignisdetails festlegen, Benutzergruppendetails* und *Anmelden*, um die nachfolgenden Informationen anwenden zu können.
> - Das Ereignis *Anmelden* stellt Informationen zum Benutzer bereit, der auf die Anwendung zugreift.
>
> 
>
>
> - Die *Benutzergruppendetails* stellen zu jedem Ereignis Informationen zur Benutzergruppe des zugehörigen Benutzers bereit.
>
> 
>

Die Aufzeichnung von Benutzergruppendetails in der Tabelle AUDIT_EVENT_DETAIL ist teilweise von der Auswahl abhängig, die Sie unter *Allgemeine Ereignisse* und *Ereignisdetails festlegen* auf der Auditing-Seite getroffen haben. Wenn Sie auf der *Auditing*-Seite das Ereignis *Anmelden* ohne die *Benutzergruppendetails* ausgewählt haben, werden die Benutzergruppendetails nach wie vor für das Ereignis *Anmelden* in der Tabelle AUDIT_EVENT_DETAIL aufgezeichnet. In der folgenden Tabelle wird das Verhalten von BI 4.2 SP 5 veranschaulicht.

Anmelden	Benutzergruppendetails	Verhalten
Ausgewählt	Ausgewählt	Die Benutzergruppendetails werden für alle Ereignisse aufgezeichnet, die Sie unter "Allgemeine Ereignisse" ausgewählt haben.
Ausgewählt	Nicht ausgewählt	Die Benutzergruppendetails werden nur für Ereignisse vom Typ "Anmelden" aufgezeichnet.
Nicht ausgewählt	Nicht ausgewählt	Die Benutzergruppendetails werden nicht aufgezeichnet.
Nicht ausgewählt	Ausgewählt	Die Benutzergruppendetails werden für alle Ereignisse außer für Ereignisse vom Typ "Anmelden" aufgezeichnet.

26.2.3 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.

26.2.3.1 Datenbankeinstellungen des Audit-Datenspeichers (ADS) konfigurieren

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*.

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.
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 109.200.)

> ⚠ 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.

27 Plattformsuche

27.1 Plattformsuche

Mithilfe der Plattformsuche der BI-Plattform können Benutzer den Inhalt des BI-Plattform-Repositorys durchsuchen.

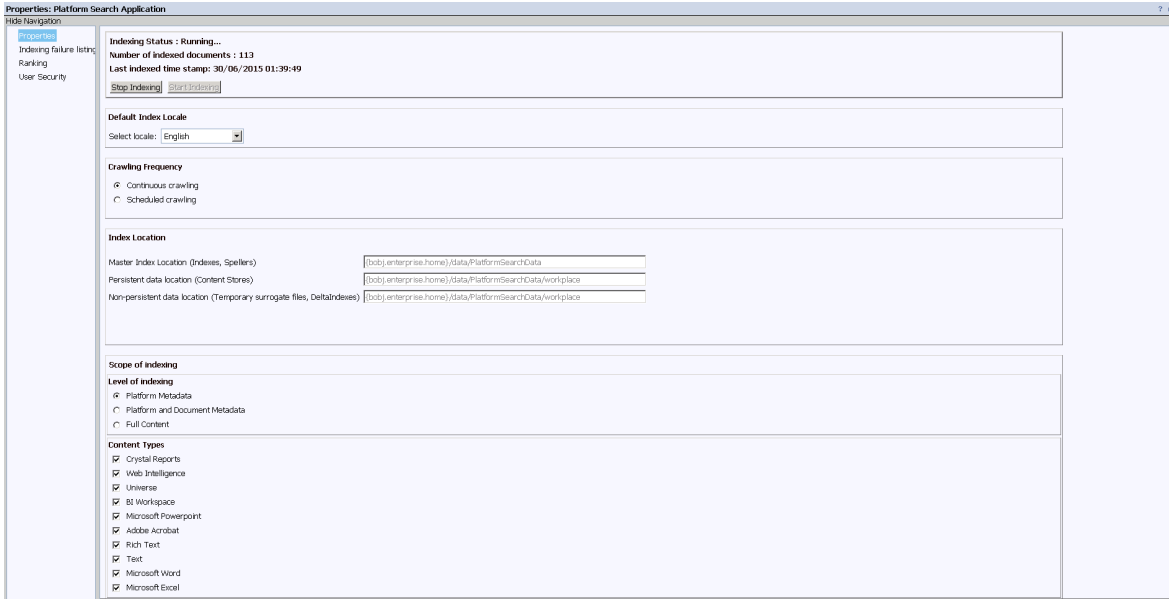
Zugriff auf die Plattformsuche besteht über die CMC-Startseite, dort können folgende Aufgaben ausgeführt werden:

- Festlegen der Anwendungseigenschaften
- Anzeigen der Indizierungsfehlerlisten
- Festlegen der Sicherheitsberechtigungen des Benutzers
- Zeitgesteuertes Verarbeiten eines Objekts

27.1.1 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. 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 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.

Option	Beschreibung
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. **Hinweis** • Der Speicherort des Hauptindex muss 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. • In den Indexdateien können personenbezogene und vertrauliche Informationen gespeichert sein, insbesondere wenn Sie Dokumentinhalte indizieren. Sie dürfen nur Systembenutzern erlauben, auf die freigegebenen Ordner zuzugreifen, und Sie sollten die freigegebenen Ordner in einer verschlüsselten Umgebung speichern, um Datendiebstahl zu verhindern.

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. Als Standard ist die Option aktiviert.
	• 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
	Bei Analysis-Office- und Lumira-Dokumenten wird die Indizierung nicht für den gesamten Inhalt unterstützt. Bei Analysis-Office- und Lumira-Dokumenten wird nur die Indizierung von Metadaten unterstützt.
	Hinweis
	Wenn Sie die Indizierungsebene ändern, wird die Indizierung für die Regenerierung des gesamten BI-Plattform-Repositorys initialisiert.

Option	Beschreibung
Inhaltstypen	Für die Indizierung stehen folgende Inhaltstypen zur Auswahl: • Crystal Reports • Web Intelligence • Universum • BI-Arbeitsbereich • Analysis Office • Lumira • Microsoft PowerPoint • Adobe Acrobat • Rich Text • Text • Microsoft Word • Microsoft Excel Der Inhaltstypenfilter ist nicht für die Indizierung von Plattform-Metadaten relevant. Unabhängig davon, welche Inhaltstypen Sie auswählen, erfolgt die Indizierung der Plattform-Metadaten für alle unterstützten Objekttypen, und die Suchergebnisse im BI-Launchpad geben alle Objekte für das mit den Plattform-Metadaten verbundene Schlüsselwort zurück. Der Inhaltstypenfilter ist für die Indizierung von Dokument-Metadaten (Dokumentautor, Dokumentkopf, Dokumentfuß usw.) und die Indizierung von Inhalten (Grafiken, Diagramme, Tabellen mit Berichten) relevant. Abhängig davon, welche Indizierungsebene und welche Inhaltstypen Sie auswählen, indiziert die Plattformsuche die Dokument-Metadaten und die Inhalte für die ausgewählten Objekttypen aus dem Repository, und bei der Suche nach einem mit Dokument-Metadaten und Inhalten verbundenen Stichwort werden nur diese Objekte in den BI-Launchpad-Suchergebnissen angezeigt.
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.

Option	Beschreibung
Von der Indizierung ausgeschlossene Dokumente	Die Option *Von der Indizierung ausgeschlossene Dokumente* schließt Dokumente von der Indizierung aus. Beispielsweise möchten Sie extrem große Crystal-Reports-Berichte von der Suche ausschließen, um die Report-Application-Server-Ressourcen nicht zu überlasten. Sie haben auch die Möglichkeit, Veröffentlichungen mit Hunderten von personalisierten Berichten zu 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
Weitere Konfiguration – Instanz überspringen	Standardmäßig werden Instanzen von Dokumenten für die Indizierung ausgewählt. Dies verursacht ein „Aufblähen“ der Indexgröße und somit einen erhöhten Speicherplatzverbrauch auf der Festplatte. Der Ordner "Lucene Index Engine" innerhalb des Ordners "PlatformSearchData" wächst aufgrund der Indizierung einer riesigen Menge von Instanzen im Repository auf eine enorme Größe an. Wenn im System Millionen von Dokumenten (oder mehr) vorliegen und zu vielen dieser Dokumente enorme Mengen an Instanzen vorhanden sind (zusammen mit in regelmäßigen Abständen erzeugten zeitgesteuerten Instanzen), wächst der Ordner "Lucene Index Engine" übermäßig stark an, selbst wenn als Indizierungsebene "Plattform-Metadaten" festgelegt ist. Mit der Funktion "Instanz überspringen" der Plattformsuche können Sie die Indizierung von Instanzen durch Aktivierung oder Deaktivierung des entsprechenden Kontrollkästchens unter "Weitere Konfiguration – Instanz überspringen" auf der Eigenschaftenseite der Plattformsuchanwendung der CMC steuern. **Hinweis** • Wenn Sie "Instanz überspringen" aktivieren bzw. deaktivieren, müssen Sie den Adaptive Processing Server der Plattformsuche neu starten. Diese Änderungen wirken sich auf alle Ebenen der Indizierung aus. • Wenn Sie "Instanz überspringen" ändern und die Änderungen auf alle vorhandenen Instanzen anwenden (d. h. alle Instanzen für die Indizierung auswählen) möchten, müssen Sie den Index neu erstellen.

Option	Beschreibung
Von der Indizierung ausgeschlossene Objekte	Die Option *Von der Indizierung ausgeschlossene Objekte* schließt Objekte von der Indizierung aus. Beispielsweise möchten Sie bestimmte Objekte von der Suche ausschließen, um die Report-Application-Server-Ressourcen nicht zu überlasten. Durch Ausschließen bestimmter Objekte können Sie den Zugriff auf diese Dokumente über die Plattformsuche verhindern. Wenn ein Objekt jedoch indiziert wurde, bevor es dieser Gruppe zugewiesen wurde, wird das Objekt ggf. in die Suche eingeschlossen. Damit sichergestellt ist, dass die Dokumente in der Gruppe *Von der Indizierung ausgeschlossene Objekte* nicht in die Suche eingeschlossen werden, müssen Sie den Index neu erstellen. Liste der Objekte, die von der Indizierung ausgeschlossen werden können: • CrystalReport • Webi • LCMJob • Universe • Excel • PDF • PowerPoint • RTF • Txt • Word • AFDashboardPage • ObjectPackage • QaaWS • Profile • Event • Discussions • InformationDesigner • MDAnalysis • Publication • Agnostic • Analytic • Hyperlink • Program • pQuery • DSL.MetaDataFile • Verknüpfung • DataDiscoveryAlbum • AO.Workbook • VISI.Story

Option	Beschreibung
	• VISI.Dataset • VISI.Lums • VISILums • User • UserGroup

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.

27.1.2 Liste der Indizierungsfehler

Die "Liste der Indizierungsfehler" enthält eine Auflistung der Dokumente, die nicht indiziert werden konnten. Die Plattformsuche bietet vier 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. Klicken Sie auf *Aktionen* > *Liste der Indizierungsfehler*.
   Das Dialogfeld *Plattformsuchanwendung*, 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.

27.1.3 Festlegen der Sicherheitsberechtigungen für Benutzer

Die Sicherheitseinstellungen für die Plattformsuche können in der CMC über die Sicherheitsoptionen im Menü *Verwalten* verwaltet werden. Mit diesen Optionen können Sie der Zugriffskontrollliste für ein Objekt Prinzipale zuweisen, die Rechte eines Prinzipals für ein Objekt anzeigen und diese ändern.

27.1.3.1 Einer Zugriffskontrollliste für ein Objekt Prinzipale zuweisen

In einer Zugriffskontrollliste werden die Benutzer angegeben, denen Rechte für ein Objekt gewährt oder verweigert werden.

Um einer Zugriffskontrollliste einen Prinzipal zuzuordnen und die Rechte festzulegen, die der Prinzipal für das Objekt haben soll, führen Sie folgende Schritte aus:

1. Wählen Sie das Objekt aus, für das Sie einen Prinzipal hinzufügen möchten.
2. Klicken Sie auf *Verwalten* > *Benutzersicherheit*.
   Das Dialogfeld *Benutzersicherheit* wird angezeigt und enthält die Zugriffskontrollliste.
3. Klicken Sie auf *Prinzipale hinzufügen*.
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.

27.1.3.2 Entfernen von Rechten für einen Prinzipal

1. Klicken Sie auf *Verwalten* > *Benutzersicherheit*.
   Das Dialogfeld *Benutzersicherheit* wird angezeigt und enthält die Zugriffskontrollliste.
2. Markieren Sie den Namen des Objekts, für das Sie die Rechte entfernen möchten.
3. Klicken Sie auf die Registerkarte *Entfernen*.
   Das Recht *Zugriff* wird in *Kein Zugriff* geändert.

27.1.3.3 Anzeigen von Rechten für einen Prinzipal

Führen Sie folgende Schritte aus, um die Rechte eines Prinzipals für ein Objekt 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
Nach Typ sortieren
Nach Recht sortieren
Von Zugriffsberechtigung

- Sortieren Sie die Liste der angezeigten Rechte aufsteigend oder absteigend nach den folgenden Kriterien:

  Sammlung
  Typ
  Name der Berechtigung
  Status der Rechte (Gewährt, Verweigert oder Nicht angegeben)
  Anwenden auf (Alle auswählen, Nur Objekt, Nur Unterobjekte, Objekt und Unterobjekte)

Zusätzlich können Sie auf eine der Verknüpfungen in der Spalte *Quelle* klicken, um die Quelle der übernommenen Rechte anzuzeigen.

27.1.3.4 Ändern der Objektsicherheit für einen Prinzipal

Allgemein wird empfohlen, dass Sie Zugriffsberechtigungen verwenden, um einem Prinzipal Rechte zuzuweisen. Es kann erforderlich sein, bestimmte, genau abgestimmte Rechte in einer Zugriffsberechtigung zu überschreiben. Über erweiterte Rechte können Sie die Rechte für einen Prinzipal anpassen, und zwar zusätzlich zu den Zugriffsberechtigungen, über die der Prinzipal bereits verfügt. Führen Sie die folgenden Schritte aus, um einem Prinzipal für ein Objekt erweiterte Rechte zuzuordnen:

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*.
4. Klicken Sie auf die Registerkarte *Erweitert*.
5. Klicken Sie auf *Rechte hinzufügen/entfernen*.
6. Ändern Sie die Rechte für den Prinzipal.

27.1.3.5 Zurücksetzen der Sicherheitseinstellungen

Durch das Zurücksetzen der Sicherheitseinstellungen zu einem Objekt werden die expliziten Zugriffsebenen oder -rechte dieses Objekts, einschließlich der ausgelieferten Einstellungen (falls vorhanden), entfernt. Das Objekt behält nur die übernommenen Ebenen und Berechtigungen.

1. Klicken Sie auf die Registerkarte *Sicherheitseinstellungen zurücksetzen*.
   Das Dialogfenster *Sicherheitseinstellungen zurücksetzen: Anwendung zur Plattformsuche* wird angezeigt.
2. Wählen Sie eine oder beide der folgenden Optionen:
   - Sicherheitseinstellungen der Anwendung zur Objekt-Plattformsuche zurücksetzen.

- Sicherheitseinstellungen für alle unter- und nachgeordneten Elemente der Anwendung Objekt-Plattformsuche zurücksetzen.

> **Hinweis**
>
> Wenn Sie beide Optionen wählen, wird ein Dialogfenster zur Bestätigung angezeigt. Wählen Sie OK, um fortzufahren.

3. Klicken Sie auf *Weiter*, um die Sicherheitseinstellungen zurückzusetzen.

27.1.4 Zeitgesteuertes Verarbeiten eines Objekts

Mit den Optionen zur zeitgesteuerten Verarbeitung können Sie ein Objekt in der Plattformsuche zeitgesteuert verarbeiten.

Um auf die Zeitsteuerungsoptionen für die Plattformsuche zuzugreifen, führen Sie folgende Schritte aus:

1. Navigieren Sie zum Bereich *Ordner* der CMC, und wählen Sie den Ordner *Zeitgesteuerte Verarbeitung der Plattformsuche*.
2. Klicken Sie mit der rechten Maustaste auf *Objekt der zeitgesteuerten Verarbeitung der Plattformsuche*, und wählen Sie *Zeitgesteuerte Verarbeitung*.
3. Legen Sie die *Dauer der zeitgesteuerten Plattformsuche* fest, indem Sie die Dauer der zeitgesteuerten Verarbeitung angeben.
4. Klicken Sie auf *Speichern*, um die Dauer der zeitgesteuerten Verarbeitung zu speichern.
5. Klicken Sie auf *Instanzentitel*, um einen Titel für die Instanz anzugeben.
6. Klicken Sie auf *Zeitgesteuert verarbeiten*.
7. Klicken Sie auf *Wiederholung*, und wählen Sie ein Wiederholungsmuster aus dem Dropdown-Menü *Objekt ausführen* aus.
   Bei der Auswahl eines Wiederholungsmusters werden Sie von der Anwendung aufgefordert, zusätzliche Informationen anzugeben. In der folgenden Tabelle werden die zusätzlichen Informationen aufgelistet, die Sie für jedes Wiederholungsmuster angeben müssen:

Optionen zur Objektausführung	Zusätzliche Informationen erforderlich
Jetzt	Keine
Einmal	Definieren Sie Start- und Enddatum/-uhrzeit
Stündlich	Definieren Sie die Stunde und Minute, und dann Start- und Endatum/-uhrzeit
Täglich	Definieren Sie die Anzahl der Tage, und dann Start- und Enddatum/-uhrzeit
Wöchentlich	Wählen Sie die Wochentage, und definieren Sie dann Start- und Enddatum/-uhrzeit
Monatlich	Definieren Sie die Anzahl der Monate, und dann Start- und Enddatum/-uhrzeit
Am n-ten Tag des Monats	Wählen Sie den Tag des Monats aus, und definieren Sie dann Start- und Enddatum/-uhrzeit

Optionen zur Objektausführung	Zusätzliche Informationen erforderlich
Am ersten Montag des Monats	Definieren Sie Start- und Enddatum/-uhrzeit
Am letzten Tag des Monats	Definieren Sie Start- und Enddatum/-uhrzeit
Am x-ten Tag der n-ten Woche des Monats	Wählen Sie die Woche und den Tag aus, und definieren Sie dann Start- und Enddatum/-uhrzeit
Kalender	Wählen Sie einen angepassten Kalender aus, und legen Sie anschließend das Start- und Enddatum/-zeit fest.

8. Geben Sie eine Zahl im Feld *Zulässige Anzahl der Wiederholungen* sowie die erforderliche Zeit im Feld *Wiederholungsintervall in Sekunden* ein.
9. Klicken Sie auf *Zeitgesteuert verarbeiten*.
10. Klicken Sie auf *Zeitgesteuerte Verarbeitung für*, und geben Sie an, für wen die zeitgesteuerte Verarbeitung eines Objekts erfolgen soll.
    - Wählen Sie "Nur für mich zeitgesteuert verarbeiten", wenn die zeitgesteuerte Verarbeitung nur für Sie erfolgen soll, und klicken Sie auf *Zeitgesteuert verarbeiten*.
    - Wählen Sie "Für angegebene Benutzer und Benutzergruppen zeitgesteuert verarbeiten" wenn die zeitgesteuerte Verarbeitung für einen bestimmte Gruppe von Benutzern bzw. eine Benutzergruppe erfolgen soll. Der Bereich *Verfügbar* wird angezeigt. Verschieben Sie die Benutzer und Gruppen, die Sie hinzufügen möchten, aus der Liste *Verfügbare Benutzer/Gruppen* in die Liste *Ausgewählte Benutzer/Gruppen*, und klicken Sie auf *Zeitgesteuert verarbeiten*.

> **Hinweis**
>
> Sie können ein Objekt für die Dauer von mindestens 1 Minute bis maximal 1 Jahr oder 525.600 Minuten zeitgesteuert verarbeiten. Die Plattformsuche legt die Dauer für die zeitgesteuerte Verarbeitung standardmäßig auf 20 Minuten fest.

28 Arbeiten mit Föderation

28.1 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-, Word, Text-, RTF- und Shockwave-Dateien	
Benutzer	Benutzer, Gruppen, Posteingang, Favoriten und Persönliche Kategorie	

Kategorie	Replizierbare Objekttypen	Zusätzliche Hinweise
BI-Plattform	Ordner, Ereignisse, Kategorien, Kalender, Zugriffsberechtigungen, 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.

28.2 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.
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. Aktualisierungen auf der ursprünglichen Website werden auf die einzelnen Zielwebsites repliziert. Aktualisierungen und neue Objekte auf einer Zielwebsite werden an die ursprüngliche Website gesendet.

28.3 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.

28.3.1 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.	• „Ansichts“- und „Replikationsrechte“ für alle zu replizierenden Objekte • „Ansichtsrecht“ für die Replikationsliste

Aktion	Beschreibung	Erforderliche Rechte
	ⓘ Hinweis „Ansichts“- und „Replikationsrechte“ sind für alle replizierten Objekte erforderlich, einschließlich Objekte, die durch Abhängigkeitsberechnungen automatisch repliziert werden.	
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 395]

28.3.2 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

Aktion	Beschreibung	Erforderliche Rechte
		• „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

Weitere Informationen

Für die ursprüngliche Website erforderliche Rechte [Seite 394]

28.3.3 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	• Verweigern Sie dem Benutzerkonto, unter dem der Replikationsauftrag ausgeführt wird, für die beizubehaltenden Objekte „Löschrechte“.

Aktion	Beschreibung	Erforderliche Rechte
	erstellen, soll das Universum auf der Zielwebsite erhalten bleiben, wenn es auf der ursprünglichen Website gelöscht wird.	
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 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.	• Verweigern Sie dem für die Verbindung verwendeten Benutzerkonto im Remoteverbindungsobjekt die „Bearbeitungsrechte“.

28.3.4 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.

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.

28.3.5 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.

28.4 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

28.4.1 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.

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

28.4.2 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 420]

28.4.3 "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.

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.

> **ⓘ 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.

28.5 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.

> **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.

28.6 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.

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.

28.7 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.

28.7.1 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.

28.7.1.1 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.

28.7.1.2 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
Titel	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: `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.

Feld	Beschreibung
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*.

28.7.2 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*.

28.8 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.

28.8.1 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.

28.8.1.1 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.

Option	Beschreibung
	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.
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

Option	Beschreibung
	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*.

28.8.2 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.

28.8.3 Ändern von Replikationsaufträgen

Nach der Erstellung eines Replikationsauftrags in der Föderation können Sie dessen Eigenschaften ändern.

28.8.3.1 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.
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.

Sektionen	Beschreibung
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.

28.8.4 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`

28.9 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.

28.9.1 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.

28.10 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.

28.10.1 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 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:

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.

28.10.2 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

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.

> ⓘ 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 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.

Um die Änderungen der ursprünglichen Website beizubehalten, können Sie das Objekt auf der Zielwebsite löschen.

28.11 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.

28.11.1 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*.

28.11.2 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.

> **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*.

28.11.3 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:

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*.

28.12 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.

28.12.1 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.

> **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 394]

28.12.2 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.

28.12.3 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.

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 394]

28.13 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.

28.13.1 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.

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.

28.13.2 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 System Y repliziert, und es ist nicht erforderlich, den LifeCycle Manager für den Import von System X auf System Y auszuführen.

28.13.3 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.

28.13.4 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 replizierten Informationen.

28.14 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. Wählen Sie *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.

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:MaxMetaspaceSize=256m"
fi
export JAVA_OPTS
# fi
```

> **Hinweis**
>
> In BI 4.2 SP 5 können Sie mit dem Parameter "MaxMetaspaceSize" – anders als über "MaxPermSize" – den Metaspace-Speicherplatz definieren.
>
> - Wenn Sie ein Upgrade von einer älteren Version auf BI 4.2 SP 5 vornehmen, müssen Sie diesen Parameter für alle vorhandenen Server manuell bearbeiten.
> - Wenn Sie eine Neuinstallation von BI 4.2 SP 5 durchführen, wird der Parameter standardmäßig ersetzt.

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.

> **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, wählen Sie *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:
   - **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 430]
Verwenden von Web Services in Föderation [Seite 417]
Einschränkungen der aktuellen Version [Seite 429]

28.14.1 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.
  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 410]

28.14.2 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 eine Werteliste verwendet, das bzw. die ursprünglich auf der Zielwebsite erstellt und dann auf die ursprüngliche Website repliziert wurde.

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.

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:MaxMetaspaceSize=256m"`.

> **Hinweis**
>
> In BI 4.2 SP 5 können Sie mit dem Parameter "MaxMetaspaceSize" – anders als über "MaxPermSize" – den Metaspace-Speicherplatz definieren.
>
> - Wenn Sie ein Upgrade von einer älteren Version auf BI 4.2 SP 5 vornehmen, müssen Sie diesen Parameter für alle vorhandenen Server manuell bearbeiten.

> - Wenn Sie eine Neuinstallation von BI 4.2 SP 5 durchführen, wird der Parameter standardmäßig ersetzt.

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) Adaptive Processing Server anpassen

Das neue Java-Argument `-XX:MetaspaceSize` wird in Kombination mit der vorhandenen `-XX:MaxMetaspaceSize` der APS-Befehlszeile hinzugefügt, um die Initialisierungserfahrung zu verbessern und die unerwünschte und vollständige Speicherbereinigung innerhalb des Java-Prozesses im Zusammenhang mit Adaptive Processing Server(n) zu vermeiden.

Beim Testen auf einer VM mit minimalem RAM-Verbrauch, einem Standard-APS, und "Alle Services" eingeschlossen ist durch diese Werte für MetaSpace und MaxMetaSpace möglicherweise ein schnellerer Start und eine schnellere Initialisierung des APS möglich als mit den vorkonfigurierten Einstellungen. Es werden keine "vollständigen Speicherbereinigungen" gemeldet.

Mehr Informationen zum *Anpassen der JAVA-Optionen von Adaptive Processing Servern, um eine vollständige Speicherbereinigung mit MetaSpace zu vermeiden* finden Sie in SAP-Hinweis 3001317.

12) 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=<TempDir>`.

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=<TempDir>“`.

In den vorangehenden Beispielen entspricht `<TempVerz>` dem Speicherort des gewünschten temporären Verzeichnisses.

13) 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 425]
Einschränkungen der aktuellen Version [Seite 429]

29 Verwalten von Replikationslisten

29.1 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. **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, Word, Textdateien, RTF-Dateien, Shockwave-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

29.1.1 Erstellen von Replikationslisten

Die Replikationslisten sind im Bereich "Replikationslisten" der CMC abgelegt. Sie können Replikationslisten in dafür erstellten Ordnern und Unterordnern organisieren.

29.1.1.1 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.

29.1.1.2 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.
Von ausgewählten Universen benötigte 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.

Optionen für Objektabhängigkeit	Definition
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.
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*.

29.1.2 Ändern von Replikationslisten

Nachdem Sie eine Replikationsliste erstellt haben, können Sie deren Eigenschaften oder Objekte ändern.

29.1.2.1 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.
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 436]

29.1.2.2 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 436]

30 Veröffentlichungen

30.1 Entwurfsaufgaben

30.1.1 Veröffentlichung in der CMC erstellen

1. Navigieren Sie unter *Ordner* in der Central Management Console (CMC) zu dem Ordner, in dem Sie eine Veröffentlichung erstellen möchten.
2. Klicken Sie mit der rechten Maustaste auf den ausgewählten Ordner, und wählen Sie *Neu* > *Veröffentlichung*.
   Das Dialogfeld *Neue Veröffentlichung* wird mit allgemeinen Eigenschaftenoptionen angezeigt.

   > **Hinweis**
   >
   > Beim Erstellen einer Veröffentlichung oder beim Anzeigen von Eigenschaften einer Veröffentlichung werden auf der Registerkarte *Übersicht* kurz gefasste Informationen zu einer Veröffentlichung angezeigt.

3. (Erforderlich) Geben Sie im Feld *Titel* einen Titel für die Veröffentlichung ein.
4. (Optional) Geben Sie im Feld *Beschreibung* eine Beschreibung für die Veröffentlichung ein.
5. (Optional) Geben Sie im Feld *Schlüsselwörter* die Schlüsselwörter ein, die mit dem Inhalt der Veröffentlichung verbunden sind.
6. Klicken Sie unter *Quelldokumente* auf die Schaltfläche *Hinzufügen*.
7. Wählen Sie im Dialogfeld *Quelldokumente auswählen* ein oder mehrere Quelldokumente aus, die zur Veröffentlichung hinzugefügt werden sollen.
8. Klicken Sie auf *OK*.

   > **Hinweis**
   >
   > Das Kontrollkästchen *Zur Laufzeit regenerieren* ist standardmäßig für alle Quelldokumente aktiviert. Auf diese Weise wird das Dokument bei Ausführung der Veröffentlichung mit der Datenquelle abgeglichen und regeneriert.
   >
   > Wenn das Quelldokument bei Ausführung der Veröffentlichung nicht regeneriert werden soll, heben Sie die Auswahl des Kontrollkästchens *Zur Laufzeit regenerieren* für das Dokument auf.

9. Klicken Sie auf *Speichern und schließen*.

30.1.2 Veröffentlichung zum Bearbeiten öffnen

1. Suchen Sie die Veröffentlichung im BI-Launchpad:

a. Klicken Sie in der Gruppe *Meine Startseite* auf die Kachel *Ordner*, und navigieren Sie zu dem Ordner, in dem Sie die Veröffentlichung erstellt haben.

b. Klicken Sie auf das Symbol *** neben der Veröffentlichung, und wählen Sie *Eigenschaften*.

   Die Seite *Eigenschaften* der Veröffentlichung wird angezeigt. Hier können Sie verschiedene Eigenschaften der Veröffentlichung ändern und die Änderungen speichern.

2. Suchen Sie die Veröffentlichung in der Central Management Console (CMC) in der BI-Plattform:

   - Doppelklicken Sie auf die Veröffentlichung.
   - Klicken Sie mit der rechten Maustaste auf die Veröffentlichung, und wählen Sie *Eigenschaften*.

   Die Seite *Eigenschaften* der Veröffentlichung wird angezeigt. Hier können Sie verschiedene Eigenschaften der Veröffentlichung ändern und die Änderungen speichern.

Die Veröffentlichung wird in einem neuen Fenster geöffnet.

30.1.3 Allgemeine Eigenschaften für eine Veröffentlichung definieren

Sie definieren die Eigenschaften für eine Veröffentlichung auf der Seite *Eigenschaften*.

In der CMC oder im BI-Launchpad:

1. Öffnen Sie die Veröffentlichung, für die Sie die allgemeinen Eigenschaften definieren möchten.
   Die Seite *Eigenschaften* wird mit den allgemeinen Eigenschaften und dem Titel der Veröffentlichung angezeigt.
2. (Optional) Geben Sie im Feld *Beschreibung* eine Beschreibung für die Veröffentlichung ein.
3. (Optional) Geben Sie im Feld *Schlüsselwörter* die Schlüsselwörter ein, die mit dem Inhalt der Veröffentlichung verbunden sind.
4. Klicken Sie auf *Speichern und schließen*.

30.1.4 Quelldokumente hinzufügen

Beim Erstellen einer Veröffentlichung können Sie auf der Seite *Neue Veröffentlichung* jederzeit Dokumente hinzufügen, ändern und entfernen.

Beim Auswählen der Quelldokumente bestimmt der Dokumenttyp der dynamischen Inhalte, welche Optionen verfügbar sind.

1. Klappen Sie auf der Seite *Neue Veröffentlichung* die Option *Allgemein* auf, und wählen Sie *Quelldokumente*.
2. Klicken Sie auf das Symbol + *(Hinzufügen)*.
3. Wählen Sie im Dialogfeld *Quelldokumente auswählen* die Dokumente mit dynamischem Inhalt des gleichen Dokumenttyps aus, die in die Veröffentlichung aufgenommen werden sollen.
4. Klicken Sie auf *OK*.

   Die ausgewählten Quelldokumente werden auf der Seite *Neue Veröffentlichung* in der Liste *Elemente* angezeigt. Das Kontrollkästchen in der Spalte *Zur Laufzeit regenerieren* ist für alle Quelldokumente

standardmäßig ausgewählt. Wenn dieses Kontrollkästchen ausgewählt ist, wird das Dokument beim Ausführen der Veröffentlichung anhand seiner Datenquelle regeneriert. Wenn Sie dies nicht wünschen, deaktivieren Sie das Kontrollkästchen für dieses Dokument in der Spalte *Zur Laufzeit regenerieren*.

> **Hinweis**
>
> Zur Verbesserung der Systemleistung deaktivieren Sie das Kontrollkästchen in der Spalte *Zur Laufzeit regenerieren* für jedes Dokument.

5. Sie können die Reihenfolge festlegen, in der Dokumente angezeigt werden, wenn Sie Quelldokumente als Anlage oder zusammengeführte PDF-Datei senden. Wählen Sie auf der Seite *Neue Veröffentlichung* im Bereich *Quelldokumente* ein Dokument in der Liste *Elemente* aus, und klicken Sie auf das Symbol *Nach oben* oder *Nach unten*, um die Dokumente neu zu ordnen.
6. Klicken Sie auf *Speichern und schließen*.

30.1.4.1 Ersetzen von Quelldokumenten von Drittherstellern

Ein Quelldokument eines Drittherstellers (auch "agnostisches Dokument" genannt) stammt nicht aus dem BI-Launchpad. Es kann beispielsweise eine Microsoft-Word-, Adobe-PDF- oder Microsoft-Excel-Datei sein.

Damit Sie ein Quelldokument eines Drittherstellers ersetzen können, müssen Sie über die Zugriffsberechtigung "Bearbeiten" für das Dokument verfügen.

Obwohl Sie den Inhalt von Dokumenten von Drittherstellern nicht aktualisieren können, lassen sich diese durch neuere Dokumentversionen ersetzen. Dadurch haben Sie die Möglichkeit, die letzten Quellinformationen in Dokumenten anzuzeigen, die ursprünglich nicht aus dem BI-Launchpad stammen.

1. Klicken Sie mit der rechten Maustaste auf ein Quelldokument eines Drittherstellers, und wählen Sie *Organisieren* > *Datei ersetzen* aus.

   Die Menüoption *Datei ersetzen* steht für ein Dokument eines Drittherstellers nicht zur Verfügung, wenn Sie nicht über das Recht "Bearbeiten" für das Dokument verfügen.
2. Klicken Sie im Dialogfeld *Datei ersetzen* auf *Durchsuchen*, und wählen Sie eine neuere Version der Quelldokumentdatei auf dem Computer aus.

   Wenn eine Meldung mit der Information angezeigt wird, dass die Datei dem Dateiformat des Quelldokuments nicht entspricht, haben Sie eine Datei mit einem anderen Format als das ursprüngliche Quelldokument ausgewählt. Klicken Sie auf *OK*, um die Meldung zu schließen, und klicken Sie dann auf *Durchsuchen*, um das korrekte Quelldokument auszuwählen.
3. Klicken Sie auf *Ersetzen*.
4. Klicken Sie in der Bestätigungsmeldung auf *OK*, um das Dokument des Drittherstellers zu aktualisieren.

30.1.5 Auswählen von Enterprise-Empfängern

Sie wählen Enterprise-Empfänger für eine Veröffentlichung im Dialogfeld *Zeitgesteuerte Verarbeitung* aus.

1. Klicken Sie im Dialogfeld *Zeitgesteuert verarbeiten* auf *Ziele* in der Navigationsliste, und klicken Sie auf *Enterprise-Empfänger*.

2. Wählen Sie Empfänger für die Veröffentlichung:
   a. Klicken Sie unter *Verfügbar* auf *Benutzerliste*, um eine Liste aller Benutzer in der BI-Plattform anzuzeigen oder auf *Gruppenliste*, um eine Liste aller Benutzergruppen in der BI-Plattform anzuzeigen.
   b. Wählen Sie die Benutzer oder Benutzergruppen, und verschieben Sie die Benutzer oder Gruppen in die Liste *Ausgewählt*.

   Geben Sie den Benutzernamen, den vollständigen Namen oder die E-Mail-Adresse eines Empfängers in das Feld *Titel suchen* ein, um den Benutzer in der Liste *Verfügbare Empfänger* schnell zu finden. Zur Auswahl mehrerer Benutzer oder Benutzergruppen gleichzeitig, halten Sie die `Strg`- oder `Umschalt`-Taste gedrückt und klicken auf die einzelnen Benutzer oder Gruppen. Um Empfänger auszuschließen, wählen Sie einen Benutzer oder eine Benutzergruppe in der Liste *Ausgewählt* aus, und verschieben Sie den Benutzer oder die Gruppe in die Liste *Ausgeschlossen*.
3. Klicken Sie auf *OK*.

30.1.6 Auswählen dynamischer Empfänger

Dynamische Empfänger sind Empfänger, die keine BI-Plattform-Benutzer sind. Sie wählen dynamische Empfänger für eine Veröffentlichung im Dialogfeld *Neue Veröffentlichung* aus.

Zum Festlegen von dynamischen Empfängern müssen Sie über eine Quelle dynamischer Empfänger verfügen, die bereits eingerichtet ist und verwendet werden kann. Die Quelle dynamischer Empfänger enthält Empfängerdaten und kann ein Crystal-Reports-Bericht, ein Web-Intelligence-Dokument oder ein individuell codierter Datenprovider sein. Informationen zum Erstellen einer individuell codierten Quelle dynamischer Empfänger finden Sie im *Business Intelligence Platform Java SDK Developer Guide*.

Daten für dynamische Empfänger werden über die Abfrage abgerufen und stimmen u.U. nicht mit den Daten überein, die angezeigt werden, wenn Sie das Dokument einsehen. Abhängig davon, wie die Abfrage aufgebaut ist, können die in der Web-Intelligence-Komponente erstellten Quellen dynamischer Empfänger Werte enthalten, die den Daten in den Quelldokumenten der Veröffentlichung nicht entsprechen. Beispielsweise können wichtige Werte durch einen Filter im Bericht ausgeschlossen werden, oder es sind doppelte Datensätze vorhanden, da die Abfrage für den Abruf von Duplikaten ausgelegt wurde. Schauen Sie sich während des Veröffentlichungsentwurfsprozesses die gesamte Liste der dynamischen Empfänger an.

Zur effizienteren Verarbeitung von Veröffentlichungen verwenden Sie die Liste *Empfänger-ID*, um Empfängerdaten nach Empfänger-ID zu sortieren.

1. Öffnen Sie die Veröffentlichung, für die Sie dynamische Empfänger auswählen möchten.
2. Klicken Sie im Dialogfeld *Eigenschaften* in der Navigationsliste auf *Dynamische Empfänger*.

   Quellen für dynamische Empfänger von Crystal-Reports-Berichten dürfen nicht im `.rptr`-Format vorliegen.
3. Wählen Sie unter *Quelle für die dynamischen Empfänger auswählen* entweder *Provider für dynamischen Empfänger in Web-Intelligence-Bericht* oder *Provider für dynamischen Empfänger in Crystal Reports*.
4. Suchen und wählen Sie das als Quelle für dynamischen Empfänger zu verwendende Objekt, und klicken Sie auf *OK*.
5. Wenn Sie ein Web-Intelligence-Dokument als Quelle für dynamischen Empfänger ausgewählt haben, wählen Sie aus der Liste *Wählen Sie den Datenquellennamen für das Dokument aus* eine Abfrage aus, die in dem Dokument angezeigt wird.
6. Wählen Sie in der Liste *Empfänger-ID (erforderlich)* das Feld aus, das die ID-Werte des Empfängers enthält.

7. (Optional) Wählen Sie in der Liste *Vollständiger Name* das Feld aus, das die vollständigen Namen der Empfänger enthält.
8. Wenn Sie die Veröffentlichung an E-Mail-Adressen senden möchten, wählen Sie in der Liste *E-Mail* das Feld mit den E-Mail-Adressen der Empfänger aus.
9. Legen Sie fest, an welche Empfänger in der Quelle für dynamische Empfänger die Veröffentlichung verteilt werden soll:
   - Um die Veröffentlichung an alle dynamischen Empfänger zu senden, aktivieren Sie das Kontrollkästchen *Gesamte Liste verwenden*.
   - Um die Veröffentlichung an bestimmte dynamische Empfänger zu senden, deaktivieren Sie das Kontrollkästchen *Gesamte Liste verwenden* und aktivieren dann unter *Verfügbar* das Kontrollkästchen für einen Empfänger, und verschieben ihn in die Liste *Ausgewählt*.

   Geben Sie den Benutzernamen, den vollständigen Namen oder die E-Mail-Adresse eines Empfängers in das Feld *Titel suchen* ein, um den Benutzer in der Liste *Verfügbare Empfänger* schnell zu finden. Um einen Empfänger auszuschließen, aktivieren Sie das Kontrollkästchen für den Empfänger und verschieben ihn in die Liste *Ausgeschlossen*.
10. Klicken Sie auf *OK*.

Nachdem Sie die dynamischen Empfänger für die Veröffentlichung angegeben haben, können Sie die Veröffentlichung für dynamische Empfänger personalisieren. Ordnen Sie dazu ein Feld im Quelldokument einer Spalte in der Quelle für dynamische Empfänger zu.

30.1.7 Ziel für eine Veröffentlichung auswählen

Das Ziel für eine Veröffentlichung wählen Sie während der Erstellung oder der zeitgesteuerten Verarbeitung der Veröffentlichung aus.

1. Klappen Sie auf der Seite *Neue Veröffentlichung* oder *Veröffentlichungszeitplan* die Option *Allgemein* auf, und wählen Sie *Ziele*.
2. (Optional) Um zu verhindern, dass Veröffentlichungsinstanzen auf Ihrem System gespeichert werden, löschen Sie den *Enterprise-Standardspeicherort* aus der Liste *Ausgewählte Lieferziele*.
3. Legen Sie einen niedrigen Wert für die Anzahl der Instanzen für das Veröffentlichungsobjekt fest.

   Informationen hierzu finden Sie im *Benutzerhandbuch für SAP BusinessObjects Business Intelligence*.
4. Klicken Sie unter *Lieferziele auswählen* auf *Hinzufügen*, aktivieren Sie das Kontrollkästchen neben jedem Ziel, an das die Veröffentlichung gesendet werden soll.

   Um eine Verknüpfung für eine Veröffentlichung zu erstellen, wählen Sie sowohl *BI-Posteingang* als auch *Enterprise-Standardspeicherort* als Ziel.

   Falls die Veröffentlichung an E-Mail-Empfänger gesendet wird, und Sie eine Verknüpfung zu einem Enterprise-Speicherort in den E-Mail-Haupttext einbetten möchten, wählen Sie sowohl*E-Mail* als auch *Enterprise-Standardspeicherort* als Ziel aus.

   Das von Ihnen ausgewählte Ziel wird im linken Navigationsbereich des Dialogfeldes *Ziele auswählen* angezeigt.
5. Wählen Sie bei Bedarf im linken Navigationsbereich das zu konfigurierende Ziel aus.
   Es werden Optionen für das Ziel angezeigt

6. (Optional) Um einen Namen für die Veröffentlichung anzuzeigen, wählen Sie *Spezifischen Namen verwenden*, und geben Sie einen Namen ein, oder wählen Sie in der Liste *Platzhalter hinzufügen* einen Platzhalter aus.

   Wenn Sie keinen Namen auswählen, wird der Veröffentlichung ein vom System generierter Name zugewiesen. Beim Ausführen der Veröffentlichung wird in jeden Platzhalter ein Wert eingefügt.
7. (Optional) Wenn Sie *Spezifischen Namen verwenden* ausgewählt haben, und die Veröffentlichung mehrere Dokumente enthält, denen Sie individuelle Namen zuordnen möchten, aktivieren Sie das Kontrollkästchen *Spezifischer Name pro Dokument*, und geben Sie einen Namen ein, oder wählen Sie in der Liste *Platzhalter hinzufügen* für jedes Dokument einen Platzhalter aus.

   Wenn Sie keinen Namen auswählen, wird jedem Dokument derselbe vom System generierte Name zugewiesen.
8. (Nur *E-Mail*) Um eine Verknüpfung zum Enterprise-Speicherort in den E-Mail-Haupttext einzubetten, positionieren Sie den Cursor im Feld *Nachricht* und wählen *Viewer* in der Liste *Platzhalter* unter dem Feld aus.

   Der Platzhalter *%SI_VIEWER_URL%* wird in den E-Mail-Haupttext eingefügt. Er wird bei der Ausführung der Veröffentlichung durch eine Verknüpfung ersetzt. Falls Sie keine Verknüpfung einbetten können, stellen Sie sicher, dass Sie sowohl *E-Mail* als auch *Enterprise-Standardspeicherort* als Ziel ausgewählt haben.
9. (Nur *BI-Posteingang*) Klicken Sie unter *Senden als* auf *Verknüpfung*, um eine Verknüpfung zu der Veröffentlichung zu erstellen, oder auf *Kopieren*, um eine Kopie der Veröffentlichung zu erstellen.

   Falls Sie keine Verknüpfung erstellen können, stellen Sie sicher, dass Sie sowohl *BI-Posteingang* als auch *Enterprise-Standardspeicherort* als Ziel ausgewählt haben.
10. Falls Sie mehrere Ziele ausgewählt haben, wiederholen Sie Schritt 5 bis 10 für jedes Ziel, um das Ziel auszuwählen und zu konfigurieren.
11. Klicken Sie auf *Bestätigen*.

30.1.7.1 Zieloptionen für die zeitgesteuerte Verarbeitung

Option	Beschreibung
Enterprise-Standardspeicherort	Sendet das Objekt an einen Enterprise-Standardspeicherort.
BI-Posteingang	Sendet das Objekt an den BI-Launchpad-Posteingang eines Benutzers.
E-Mail	Sendet das Objekt an die E-Mail-Adresse eines Benutzers.
FTP-Server	Sendet das Objekt an einen Speicherort auf einem FTP-Server.
SFTP-Server	Sendet das Objekt an einen Speicherort auf einem SFTP-Server.

Das Kontrollkästchen *Objekte an alle Benutzer senden* ist standardmäßig für alle Ziele ausgewählt. Es gibt jedoch Fälle, in denen die Objekte nicht an jeden Benutzer gesendet werden sollen. Es kann beispielsweise vorkommen, dass drei Empfänger über identische Personalisierungswerte verfügen und damit in ihren Veröffentlichungsinstanzen dieselben Daten erhalten. Wenn Sie das Kontrollkästchen *Objekte an alle Benutzer senden* deaktivieren, wird eine Veröffentlichungsinstanz generiert und an alle drei Empfänger gesendet. Wenn Sie *Objekte an alle Benutzer senden* aktivieren, wird dieselbe Veröffentlichungsinstanz dreimal gesendet (einmal an jeden Empfänger).

Wenn Sie darüber hinaus die Veröffentlichung an einen *FTP-Server*, einen *SFTP-Server* oder ein *Dateisystemziel* senden, während einige Empfänger über identische Personalisierungswerte verfügen, können Sie das

Kontrollkästchen *Objekte an alle Benutzer senden* deaktivieren, um die Gesamtverarbeitungszeit zu verringern. Wenn Sie *Objekte an alle Benutzer senden* deaktivieren, enthalten bei der Konfiguration von Zielen verwendete Platzhalter die Informationen des Publishers (nicht die des Empfängers).

30.1.8 Wiederholungsmuster auswählen

Das Wiederholungsmuster legt fest, wie oft die Veröffentlichung ausgeführt wird. Sie wählen das Wiederholungsmuster für eine Veröffentlichung im Dialogfeld *Zeitgesteuerte Verarbeitung* aus.

1. Klicken Sie mit der rechten Maustaste auf die Veröffentlichung, für die Sie ein Wiederholungsmuster festlegen möchten, und wählen Sie *Zeitgesteuerte Verarbeitung*.
2. Klicken Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* auf *Wiederholung*.
3. Wählen Sie in der Liste *Objekt ausführen* ein Wiederholungsmuster aus.
4. Geben Sie im Feld *Anzahl der zulässigen erneuten Versuche* ein, wie oft der Server versuchen soll, einen fehlgeschlagenen Auftrag erneut auszuführen.
5. Geben Sie im Feld *Wiederholungsintervall in Sekunden* ein, wie lange der Server vor einem erneuten Ausführungsversuch eines Auftrags abwarten soll.
6. Klicken Sie auf *Zeitgesteuert verarbeiten*.

Die Veröffentlichung wird zu geplanten Zeiten ausgeführt.

30.1.8.1 Wiederholungsmuster-Optionen

Option	Beschreibung
Jetzt	Führt das Objekt sofort einmal aus.
Einmal	Führt das Objekt zu einem angegebenen Zeitpunkt einmal aus. Wenn Sie ein Objekt mit Ereignissen zeitgesteuert verarbeiten, wird das Objekt einmal ausgeführt, falls das Ereignis zwischen Start- und Endzeit ausgelöst wird. Wählen Sie den Start- und Endzeitpunkt für die Ausführung des Objekts in der Liste *Startdatum/-zeit* und *Enddatum/-zeit* aus, und geben Sie das Datum für die Start- und Endzeit ein.

Option	Beschreibung
Stündlich	Erstellt eine Instanz pro Stunde zur angegebenen Uhrzeit. Die erste Instanz wird zu einem festgelegten Startzeitpunkt erstellt, und die Instanzen werden stündlich zu dieser Uhrzeit erstellt, bis die Ausführung des Objekts zu einem festgelegten Endzeitpunkt gestoppt wird. Wählen Sie in der Liste *Stunde (n)* und *Minute (x)* aus, wie oft das Objekt ausgeführt werden soll, wählen Sie in der Liste *Startdatum/-zeit* und *Enddatum/-zeit* aus, wann die Ausführung des Objekts gestartet und gestoppt werden soll, und geben Sie das Datum für die Start- und Endzeit ein.
Täglich	Führt das Objekt zu dem angegebenen Zeitpunkt einmal täglich aus. Die erste Instanz wird zu dem festgelegten Startzeitpunkt erstellt, und die Instanzen werden täglich zu dieser Uhrzeit erstellt, bis die Ausführung des Objekts zu einem festgelegten Endzeitpunkt gestoppt wird. Geben Sie im Feld *Tage (n)* das Intervall zur Ausführung des Objekts ein, wählen Sie in der Liste*Startdatum/-zeit* und *Enddatum/-zeit* aus, wann die Ausführung des Objekts gestartet und gestoppt werden soll, und geben Sie das Datum für die Start- und Endzeit ein.
Wöchentlich	Führt das Objekt jede Woche an den ausgewählten Tagen zur angegebenen Startzeit aus. Die erste Instanz wird zu dem festgelegten Startzeitpunkt erstellt, und die Instanzen werden wöchentlich an diesen Tagen zu dieser Uhrzeit erstellt, bis die Ausführung des Objekts zu einem festgelegten Endzeitpunkt gestoppt wird. Aktivieren Sie ein Kontrollkästchen für jeden Tag, an dem das Objekt ausgeführt werden soll, wählen Sie in der Liste *Startdatum/-zeit* und *Enddatum/-zeit* aus, wann die Ausführung des Objekts gestartet und gestoppt werden soll, und geben Sie das Datum für die Start- und Endzeit ein.
Monatlich	Führt das Objekt am angegebenen Datum zur angegebenen Startzeit und in den angegebenen monatlichen Intervallen aus. Die erste Instanz wird zu dem festgelegten Startzeitpunkt erstellt, und die Instanzen werden monatlich zu dieser Uhrzeit erstellt, bis die Ausführung des Objekts zu einem festgelegten Endzeitpunkt gestoppt wird. Wählen Sie im Feld *Monat (n)* das Intervall zur Ausführung des Objekts aus, wählen Sie in der Liste*Startdatum/-zeit* und *Enddatum/-zeit* aus, wann die Ausführung des Objekts gestartet und gestoppt werden soll, und geben Sie das Datum für die Start- und Endzeit ein.

Option	Beschreibung
Am n-ten Tag des Monats	Erstellt eine Instanz jeden Monat an dem angegebenen Tag zur angegebenen Startzeit. Die erste Instanz wird zu dem festgelegten Startzeitpunkt erstellt, und die Instanzen werden monatlich an dem angegebenen Tag zu dieser Uhrzeit erstellt, bis die Ausführung des Objekts zu einem festgelegten Endzeitpunkt gestoppt wird. Geben Sie die Uhrzeit, zu der die Ausführung des Objekts gestartet und gestoppt sowie den Tag des Monats ein, an dem das Objekt ausgeführt werden soll.
Am ersten Montag des Monats	Erstellt eine Instanz am ersten Montag jedes Monats zur angegebenen Startzeit. Geben Sie den Zeitpunkt ein, an dem die Ausführung des Objekts gestartet und gestoppt werden soll.
Am letzten Tag des Monats	Erstellt eine Instanz am letzten Tag jedes Monats zur angegebenen Startzeit. Geben Sie den Zeitpunkt ein, an dem die Ausführung des Objekts gestartet und gestoppt werden soll.
Tag x der n-ten Woche des Monats	Erstellt eine Instanz jeden Monat am angegebenen Tag und in der angegebenen Woche zur angegebenen Startzeit. Geben Sie die Uhrzeit, zu der die Ausführung des Objekts gestartet und gestoppt sowie den Wochentag und die Woche des Monats ein, an dem das Objekt ausgeführt werden soll.
Kalender	Erstellt eine Instanz an jedem angegebenen Kalenderdatum zur angegebenen Startzeit. Geben Sie die Uhrzeit ein, zu der die Ausführung des Objekts gestartet und gestoppt werden soll, und wählen Sie die Kalenderdaten aus, an denen das Objekt ausgeführt werden soll.

30.1.9 Personalisierte Platzhalter für Veröffentlichungsquelldokumente auswählen

Sie wählen personalisierte Platzhalter für eine Veröffentlichung im Dialogfeld *Zeitgesteuerte Verarbeitung* aus.

Bevor Sie personalisierte Platzhalter in Veröffentlichungsinstanznamen verwenden können, müssen die Quelldokumente der Veröffentlichung auf die Verwendung der Personalisierung zum Filtern von Daten eingestellt sein.

Wenn Sie eine Veröffentlichungsinstanz zeitgesteuert verarbeiten, können Sie Platzhalter im Feld *Spezifischen Namen verwenden* für Quelldokumente verwenden, und Sie können Text und Platzhalter in einem Veröffentlichungsnamen kombinieren sowie mehrere Platzhalter verwenden.

1. Klicken Sie mit der rechten Maustaste auf die Veröffentlichung, für die Sie Platzhalter auswählen möchten, und wählen Sie *Zeitgesteuerte Verarbeitung*.
2. Klicken Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* in der Navigationsliste auf *Ziele*.
3. Wählen Sie unter *Optionen für ausgewählte Ziele anzeigen* die Option *Spezifischen Namen verwenden*, und wählen Sie einen Platzhalter für den Veröffentlichungsnamen aus der Liste *Platzhalter hinzufügen*.
   Die von Ihnen ausgewählten Platzhalter werden im Feld *Spezifischer Name* für den Dokumenttitel angezeigt.
4. So fügen Sie einzelne Dokumente hinzu:
   a. Wählen Sie unter *Zielname* die Option *Spezifischer Name pro Dokument*.
   b. Wählen Sie für jeden Dokumenttitel einen Platzhalter aus der Liste *Platzhalter hinzufügen* aus.

   Die von Ihnen ausgewählten Platzhalter werden im Feld *Spezifischer Name* für alle Dokumenttitel angezeigt.
5. Klicken Sie auf *OK*.

Nachdem die Personalisierung für eine Veröffentlichung eingerichtet ist, werden personalisierte Platzhalter in der Liste *Platzhalter hinzufügen* im Dialogfeld *Ziele* angezeigt.

30.1.10 Personalisierte Platzhalter für E-Mail-Felder auswählen

Sie wählen personalisierte Platzhalter für eine Veröffentlichung im Dialogfeld *Zeitgesteuerte Verarbeitung* aus.

Sie können in jedem beliebigen E-Mail-Feld Text und Platzhalter kombinieren – und mehrere Platzhalter verwenden. Bei der zeitgesteuerten Verarbeitung einer Veröffentlichung an ein E-Mail-Ziel können Sie in den Feldern *Von*, *An*, *Cc*, *Bcc*, *Betreff*, *Nachricht* und *Spezifischen Namen verwenden* Platzhalter verwenden.

1. Klicken Sie mit der rechten Maustaste auf die Veröffentlichung, für die Sie Platzhalter auswählen möchten, und wählen Sie *Zeitgesteuerte Verarbeitung*.
2. Klicken Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* in der Navigationsliste auf *Ziele*.
3. Wählen Sie in der Liste *Ziel* die Option *E-Mail* aus.
4. Legen Sie die Zieloptionen, einschließlich Platzhaltern, wie gewünscht fest.
5. Klicken Sie auf *OK*.

30.1.11 Inhalte aus dynamischen Quelldokumenten in eine E-Mail einbetten

Sie betten Inhalte aus einem Quelldokument für eine Veröffentlichung im Dialogfeld *Zeitgesteuerte Verarbeitung* ein.

Sie können Inhalt aus Dokumenten mit dynamischen Inhalten in den Textkörper einer E-Mail einfügen. In Crystal-Reports-Berichte können Sie Inhalt aus einem Bericht einbetten. Für Web-Intelligence-Dokumente lassen sich vollständige Dokumente oder einzelne Berichtsregisterkarten einbetten.

1. Klicken Sie mit der rechten Maustaste auf die Veröffentlichung, der Sie die Inhalte entnehmen möchten, und wählen Sie *Zeitgesteuerte Verarbeitung*.
2. Klicken Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* in der Navigationsliste auf *Formate*.
3. (Nur Crystal-Reports-Berichte) Aktivieren Sie unter *Formatoptionen für ausgewähltes Dokument* das Kontrollkästchen *mHTML*.
4. (Nur Web-Intelligence-Dokumente) Wählen Sie aus, ob Sie das gesamte Dokument oder eine Berichtsregisterkarte veröffentlichen möchten:
   a. Aktivieren Sie unter *Ausgabeformat* das Kontrollkästchen *mHTML*.
   b. Wählen Sie unter *Details zum Ausgabeformat* die Option *Alle Berichte*, um das gesamte Dokument zu veröffentlichen, oder *Einen Bericht auswählen*, und wählen Sie eine Berichtsregisterkarte in der Liste.
5. Klicken Sie in der Navigationsliste auf *Ziele*.
6. Aktivieren Sie im Dialogfeld *Ziele* unter *Ziele auswählen* das Kontrollkästchen *E-Mail*.

   Die Konfigurationsoptionen für E-Mails werden angezeigt.
7. Geben Sie in das Feld *Von* einen Namen oder eine E-Mail-Adresse ein, oder wählen Sie in der Liste *Platzhalter hinzufügen* die Option *E-Mail-Adresse* aus.

   Sie können beispielsweise **`Robert`**, **`Publisher`** oder **`publisher@sap.com`** eingeben. Wenn Sie einen Namen eingeben, wird dieser an Ihren E-Mail-Server angehängt (z. B. **`Publisher@<EmailServer>`**).
8. Geben Sie im Feld *Betreff* einen Betreff ein, oder wählen Sie einen Platzhalter.

   Falls Sie den Bericht personalisiert haben, stehen personalisierte Platzhalter in der Liste *Platzhalter hinzufügen* zur Verfügung.
9. Geben Sie im Feld *Nachricht* die Nachricht ein, die im Textkörper der E-Mail angezeigt werden soll.
10. Um dynamische Inhalte in das Feld *Nachricht* einzubetten, positionieren Sie den Cursor im Feld *Nachricht* an der Stelle, an der die Inhalte eingebettet werden sollen, und wählen *HTML-Berichtsinhalt* in der Liste *Platzhalter hinzufügen*.
    %SI_DOCUMENT_HTML_CONTENT% wird im Feld *Nachricht* angezeigt. Wenn die Veröffentlichung ausgeführt wird, wird der Platzhalter durch personalisierte Inhalte aus dem Dokument mit dynamischen Inhalten ersetzt.
11. Enthält die Veröffentlichung weitere Quelldokumente, so aktivieren Sie das Kontrollkästchen *Anlage hinzufügen*.

    Andere Quelldokumente in der Veröffentlichung werden während der Veröffentlichung als Anlage zur E-Mail hinzugefügt.
12. Klicken Sie auf *OK*.

30.1.12 Veröffentlichungserweiterung in der CMC hinzufügen

Bei einer Veröffentlichungserweiterung handelt es sich um eine Codebibliothek, die Geschäftslogik auf Veröffentlichungen anwendet. Sie müssen eine Veröffentlichungserweiterung hinzufügen, bevor Sie sie in einer Veröffentlichung verwenden können.

Bevor Sie eine Veröffentlichungserweiterung verwenden können, müssen Sie sie auf allen Rechnern implementieren, auf denen der Adaptive Processing Server läuft, und dann den Adaptive Processing Server

sowie weitere Server, die einen Publishing-Dienst hosten, neu starten. Der Speicherort des Servers variiert je nach Betriebssystem:

- Unter Windows befindet sich der Server unter `<Installverz>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib\`
- In Unix befindet sich der Server unter `<Installverz>/sap_bobj/enterprise_xi40/java/lib/`

Sie können Veröffentlichungserweiterungen nur in der Central Management Console (CMC) hinzufügen. (Sie können sie nicht beim Entwurf einer Veröffentlichung im BI-Launchpad hinzufügen.)

Um die Reihenfolge, in der die Veröffentlichungserweiterungen ausgeführt werden, festzulegen, klicken Sie auf *Nach oben* oder *Nach unten* unterhalb der Liste *Vor dem Versand der Veröffentlichung* oder der Liste *Nach dem Versand der Veröffentlichung*. Weitere Informationen zu Veröffentlichungserweiterungen finden Sie im *Business Intelligence Platform Java SDK Developer Guide*.

1. Rufen Sie in der CMC den Verwaltungsbereich *Ordner* auf, und suchen Sie die Veröffentlichung, der Sie eine Erweiterung hinzufügen möchten.
2. Klicken Sie mit der rechten Maustaste auf die Veröffentlichung, und wählen Sie *Eigenschaften*.
3. Erweitern Sie im Dialogfeld *Eigenschaften* den Bereich *Zusätzliche Optionen* in der Navigationsliste, und klicken Sie auf *Veröffentlichungserweiterung*.
4. Geben Sie im Feld *Name der Veröffentlichungserweiterung* den Namen der Erweiterung ein.
5. Geben Sie im Feld *Klassenname* den vollständig qualifizierten Klassennamen für die Erweiterung ein.
6. (Optional) Geben Sie im Feld *Parameter* einen Parameternamen ein.
7. Um die Erweiterung nach der Verarbeitung, jedoch vor dem Versand zu verwenden, klicken Sie über der Liste *Vor dem Versand der Veröffentlichung* auf die Schaltfläche *Hinzufügen*.
   Die Erweiterung wird zur Liste *Vor dem Versand der Veröffentlichung* hinzugefügt.
8. Um die Erweiterung nach dem Versand zu verwenden, klicken Sie über der Liste *Nach dem Versand der Veröffentlichung* auf die Schaltfläche *Hinzufügen*.
   Die Erweiterung wird zur Liste *Nach dem Versand der Veröffentlichung* hinzugefügt.
9. Klicken Sie auf *Speichern*.

30.1.13 E-Mail-Benachrichtigung für einen Veröffentlichungsauftrag in der CMC aktivieren

Wenn Sie nach der Ausführung eines Veröffentlichungsauftrags per E-Mail benachrichtigt werden möchten, aktivieren Sie die E-Mail-Benachrichtigung.

Vergewissern Sie sich vor dem Aktivieren der E-Mail-Benachrichtigung, dass der Adaptive Job Server ordnungsgemäß konfiguriert ist.

Sie können die E-Mail-Benachrichtigung nur in der Central Management Console (CMC) aktivieren. (Sie können sie nicht beim Entwurf einer Veröffentlichung im BI-Launchpad aktivieren.)

1. Rufen Sie in der CMC den Verwaltungsbereich *Ordner* auf, und suchen Sie den Veröffentlichungsauftrag, der Sie die E-Mail-Benachrichtigung aktivieren möchten.
2. Klicken Sie mit der rechten Maustaste auf den Veröffentlichungsauftrag, und wählen Sie *Zeitgesteuert verarbeiten*.
3. Klicken Sie im Dialogfeld *Zeitgesteuert verarbeiten* in der Navigationsliste auf *Benachrichtigung*, und klappen Sie *E-Mail-Benachrichtigung*: *Nicht verwendet* auf.

4. Wenn Sie möchten, dass für erfolgreiche Veröffentlichungsaufträge E-Mail-Benachrichtigungen an die Standardempfänger-E-Mail-Adressen versendet werden, aktivieren Sie das Kontrollkästchen *Ein Auftrag wurde erfolgreich ausgeführt* und wählen dann *Standardwerte des Job Servers verwenden* aus, um die Standardadressen auf dem Adaptive Job Server zu verwenden.
5. Wenn Sie möchten, dass für erfolgreiche Veröffentlichungsaufträge E-Mail-Benachrichtigungen an E-Mail-Adressen ausgewählter Empfänger versendet werden, aktivieren Sie das Kontrollkästchen *Ein Auftrag wurde erfolgreich ausgeführt*, wählen dann *Zu verwendende Werte hier festlegen* und führen folgende Aktionen durch:
   a. Geben Sie im Feld *Von* die E-Mail-Adresse oder den Namen des Absenders der Benachrichtigung ein.
   b. Geben Sie im Feld *An* die E-Mail-Adressen der einzelnen Empfänger ein, die die Benachrichtigung erhalten sollen.
   c. Geben Sie im Feld *Cc* die E-Mail-Adressen weiterer einzelner Empfänger ein, die eine Kopie der Benachrichtigung erhalten sollen.
   d. Geben Sie im Feld *Betreff* den Betreff der Benachrichtigung ein.
   e. Geben Sie im Feld *Nachricht* eine Nachricht ein, die mit der Benachrichtigungs-E-Mail verschickt werden soll.
6. Wenn Sie möchten, dass für fehlgeschlagene Veröffentlichungsaufträge E-Mail-Benachrichtigungen an die Standardempfänger-E-Mail-Adressen versendet werden, aktivieren Sie das Kontrollkästchen *Ein Auftrag konnte nicht ausgeführt werden* und wählen dann *Standardwerte des Job Servers verwenden* aus, um die Standardadressen auf dem Adaptive Job Server zu verwenden.
7. Wenn Sie möchten, dass für fehlgeschlagene Veröffentlichungsaufträge E-Mail-Benachrichtigungen an E-Mail-Adressen ausgewählter Empfänger versendet werden, aktivieren Sie das Kontrollkästchen *Ein Auftrag konnte nicht ausgeführt werden*, wählen dann *Zu verwendende Werte hier festlegen* und führen folgende Aktionen durch:
   a. Geben Sie im Feld *Von* die E-Mail-Adresse oder den Namen des Absenders der Benachrichtigung ein.
   b. Geben Sie im Feld *An* die E-Mail-Adressen der einzelnen Empfänger ein, die die Benachrichtigung erhalten sollen.
   c. Geben Sie im Feld *Cc* die E-Mail-Adressen weiterer einzelner Empfänger ein, die eine Kopie der Benachrichtigung erhalten sollen.
   d. Geben Sie im Feld *Betreff* den Betreff der Benachrichtigung ein.
   e. Geben Sie im Feld *Nachricht* eine Nachricht ein, die mit der Benachrichtigungs-E-Mail verschickt werden soll.
8. Klicken Sie auf *Zeitgesteuert verarbeiten*.

30.1.14 Audit-Benachrichtigung für einen Veröffentlichungsauftrag in der CMC aktivieren

Aktivieren Sie die Audit-Benachrichtigung, wenn Sie erfolgreich ausgeführte oder fehlgeschlagene Veröffentlichungsaufträge prüfen möchten.

Sie können die Audit-Benachrichtigung nur in der Central Management Console (CMC) aktivieren. (Sie können sie nicht beim Entwurf einer Veröffentlichung im BI-Launchpad aktivieren.) Weitere Informationen über Audits finden Sie im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.

1. Rufen Sie in der CMC den Verwaltungsbereich *Ordner* auf, und suchen Sie den Veröffentlichungsauftrag, der Sie die Audit-Benachrichtigung aktivieren möchten.

2. Klicken Sie mit der rechten Maustaste auf den Veröffentlichungsauftrag, und wählen Sie *Zeitgesteuert verarbeiten*.
3. Klappen Sie im Dialogfeld *Zeitgesteuert verarbeiten* den Bereich *Zusätzliche Optionen* auf, klicken Sie auf *Benachrichtigung*, und klappen Sie *Audit-Benachrichtigung: Nicht verwendet* auf.
4. Um erfolgreich ausgeführte Veröffentlichungsaufträge zu prüfen, wählen Sie *Ein Auftrag wurde erfolgreich ausgeführt* aus.
5. Um fehlgeschlagene Veröffentlichungsaufträge zu prüfen, wählen Sie *Ein Auftrag konnte nicht ausgeführt werden* aus.
6. Klicken Sie auf *Zeitgesteuert verarbeiten*.

30.1.15 Ereignisse zum Auslösen einer Veröffentlichung auswählen

Mit der ereignisbasierten zeitgesteuerten Verarbeitung erhalten Sie zusätzliche Kontrolle darüber, wann eine Veröffentlichung ausgeführt wird. Sie können durch Ereignisse die Ausführung einer Veröffentlichung anstoßen oder ein Ereignis durch einen Veröffentlichungsauftrag anstoßen.

Weitere Informationen zu Ereignissen finden Sie im *Benutzerhandbuch für SAP BusinessObjects Business Intelligence*.

1. Klicken Sie auf das Symbol *** neben der Veröffentlichung, für die Sie Ereignisse auswählen, und wählen Sie *Zeitgesteuert verarbeiten*.
2. Erweitern Sie auf der Seite *Zeitgesteuert verarbeiten* die Option *Allgemein*, und wählen Sie in der Navigationsliste *Ereignisse*.
3. Um dateibasierte und benutzerdefinierte Ereignisse für eine Veröffentlichung anzugeben, klicken Sie auf das Feld *Abzuwartende Ereignisse*.
4. Aktivieren Sie im Dialogfeld *Ereignisse auswählen* das Kontrollkästchen neben den Ereignissen, um sie in die Liste *Ausgewählte Elemente* zu verschieben, und klicken Sie auf *Hinzufügen*.

   Die Ereignisse lösen die Ausführung des Veröffentlichungsauftrags aus.

   > **Hinweis**
   >
   > Aktivieren Sie das Kontrollkästchen *Beliebiges Ereignis*, wenn Sie eine zeitgesteuerte Veröffentlichung auslösen möchten, nachdem eines der Ereignisse eintritt.

5. Um Zeitsteuerungsereignisse für eine Veröffentlichung festzulegen, wählen Sie *Bei Beendigung auszulösende Ereignisse*.
6. Aktivieren Sie im Dialogfeld *Ereignisse auswählen* das Kontrollkästchen neben den Ereignissen, um sie in die Liste *Ausgewählte Elemente* zu verschieben, und klicken Sie auf *Hinzufügen*.

   Die Ereignisse treten nach der Ausführung des Veröffentlichungsauftrags ein.
7. Klicken Sie auf *Zeitgesteuert verarbeiten*.

30.1.16 Servergruppe für eine Veröffentlichung auswählen

Sie können Veröffentlichungen über Speicherorte in Föderationen zeitgesteuert verarbeiten. Weitere Informationen über Servergruppen finden Sie im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.

1. Klicken Sie auf das Symbol *** neben der Veröffentlichung, für die Sie eine Servergruppe auswählen, und wählen Sie *Zeitgesteuert verarbeiten*.
2. Erweitern Sie auf der Registerkarte *Zeitgesteuert verarbeiten* die Option *Allgemein*, und wählen Sie in der Navigationsliste die Option *Zeitsteuerungsserver-Gruppe*.
3. Wenn der Veröffentlichungsauftrag auf der ursprünglichen Website ausgeführt werden soll, aktivieren Sie die Umschaltfläche *Auf ursprünglicher Website ausführen*.
4. Wählen Sie eine Servergruppenoption aus, und klicken auf *Zeitgesteuert verarbeiten*.

30.1.17 Profilauflösungsmethode in der CMC auswählen

1. Rufen Sie in der CMC den Verwaltungsbereich *Ordner* auf, und suchen Sie die Veröffentlichung, für die Sie eine Profilauflösungsmethode auswählen möchten.
2. Klicken Sie mit der rechten Maustaste auf den Veröffentlichungsauftrag, und wählen Sie *Eigenschaften*.
3. Erweitern Sie im Dialogfeld *Eigenschaften* die Option *Eigenschaften* in der Navigationsliste, und klicken Sie auf *Erweitert*.
4. Führen Sie unter *Profilauflösungsmethode* eine der folgenden Aktionen durch:
   - Wählen Sie *Nicht zusammenführen*, wenn Profile aus mehreren Benutzergruppen zu separaten Dokumenten führen sollen.
   - Wählen Sie *Zusammenführen*, wenn Profile aus mehreren Benutzergruppen für dasselbe Dokument gelten sollen.
5. Klicken Sie auf *Speichern und schließen*.

30.1.18 Berichtsbursting-Methode in der CMC auswählen

1. Rufen Sie in der CMC den Verwaltungsbereich *Ordner* auf, und suchen Sie die Veröffentlichung, für die Sie eine Profilauflösungsmethode auswählen möchten.
2. Klicken Sie mit der rechten Maustaste auf den Veröffentlichungsauftrag, und wählen Sie *Eigenschaften*.
3. Erweitern Sie im Dialogfeld *Eigenschaften* die Option *Eigenschaften* in der Navigationsliste, und klicken Sie auf *Erweitert*.
4. Wählen Sie unter *Berichtsbursting-Methode* eine Berichtsbursting-Methode aus.
5. Klicken Sie auf *Speichern und schließen*.

30.2 Crystal-Reports-Berichte – Entwurfsaufgaben

30.2.1 Crystal-Reports-Berichte mithilfe von Parameterwerten personalisieren

Sie personalisieren Crystal-Reports-Berichte im Dialogfeld *Zeitgesteuerte Verarbeitung*.

- Bevor Sie Profile für die Personalisierung von Daten für Enterprise-Empfänger verwenden können, müssen diese in der BI-Plattform konfiguriert werden.
- Zum Ausführen dieser Aufgabe muss der Crystal-Reports-Bericht Parameter enthalten.

1. Führen Sie einen Rechtsklick auf den Crystal-Reports-Bericht aus, den Sie personalisieren möchten, und wählen Sie *Zeitgesteuerte Verarbeitung*.
2. Klicken Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* in der Navigationsliste auf *Personalisierung*.
3. Überprüfen Sie die Parameterwerte unter *Parameter*, und notieren Sie sich die Werte, die geändert werden müssen.
4. Um einen Standardwert zu ändern, klicken Sie auf *Werte bearbeiten* neben dem Standardparameterwert, wählen Sie den Parameterwert aus, oder geben Sie ihn ein und klicken auf *OK*.
5. Führen Sie eine der folgenden Aktionen aus:
   - Um die Standardparameterpersonalisierung mit Werten des Enterprise-Empfängerprofils zu überschreiben, wählen Sie in der Spalte *Zuordnung von Enterprise-Empfängern* ein Profil aus der Liste. Wenn dieses Profil in der BI-Plattform nicht konfiguriert ist, schlägt die Personalisierung fehl. Wenden Sie sich an die Systemverwaltung, wenn der BI-Plattform Profile hinzugefügt werden müssen.
   - Wenn Sie zur Personalisierung eines Berichts nur Standardparameterwerte verwenden, wählen Sie *Standardwert für alle Empfänger* in der Spalte *Zuordnung von Enterprise-Empfängern*.

   Die Spalte *Zuordnung von Enterprise-Empfängern* wird nur angezeigt, wenn die Veröffentlichung für Enterprise-Empfänger vorgesehen ist.
6. Um die Standardparameterpersonalisierung mit Werten der Personalisierung für dynamische Empfänger zu überschreiben, wählen Sie in der Spalte *Zuordnung dynamischer Empfänger* eine dynamische Empfängerquelle in der Liste.

   Die Spalte *Zuordnung dynamischer Empfänger* wird nur angezeigt, wenn die Veröffentlichung für dynamische Empfänger vorgesehen ist.

   Wenn Sie zur Personalisierung eines Berichts Standardparameterwerte verwenden, wählen Sie *Nicht angegeben* in der Spalte *Zuordnung dynamischer Empfänger* aus.
7. Klicken Sie auf *OK*.

30.2.2 Crystal Reports-Berichte durch Filtern von Feldern personalisieren

Sie personalisieren Crystal-Reports-Berichte im Dialogfeld *Zeitgesteuerte Verarbeitung*.

Bevor Sie Profile für die Personalisierung von Daten für Enterprise-Empfänger verwenden können, müssen diese in der BI-Plattform konfiguriert werden.

Wenn Sie Filter verwenden, wird eine ViewTime-Auswahlformel zum Bericht hinzugefügt, um Daten zu filtern. Diese Formel wird bei der Ausführung der Veröffentlichung angewendet und nicht im Bericht gespeichert. Sie können in Crystal-Reports-Berichten mehrere Felder filtern. Profile mit statischen Werten können in Crystal-Reports-Berichten nur Zeichenfolgenfelder filtern. Zum Filtern anderer Feldtypen verwenden Sie Ausdrucksprofilwerte. Wenn Sie einem Profil den falschen Feldtyp zuordnen, ist keine Personalisierung möglich.

Diese Funktion ist für Crystal-Reports-Berichte im Format `.rptr` nicht verfügbar.

1. Führen Sie einen Rechtsklick auf den Crystal-Reports-Bericht aus, den Sie personalisieren möchten, und wählen Sie *Zeitgesteuerte Verarbeitung*.
2. Klicken Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* in der Navigationsliste auf *Personalisierung*.
3. Wählen Sie unter *Lokale Profile* in der Spalte *Berichtfeld* ein Crystal-Reports-Berichtfeld in der Liste aus.

   Die Liste der verfügbaren Felder schließt alle Datenbankfelder und wiederkehrenden Formeln im Hauptbericht und in nicht angeforderten Unterberichten ein.
4. Wählen Sie in der Spalte *Zuordnung von Enterprise-Empfängern* ein Profil aus der Liste.

   Dieses Profil ordnet den Bericht den für Enterprise-Empfänger definierten Profilwerten zu. Wenn das Profil in der BI-Plattform nicht konfiguriert ist, schlägt die Personalisierung fehl. Wenn Sie zusätzliche Profile benötigen, wenden Sie sich an Ihren Systemadministrator.

   Die Spalte *Zuordnung von Enterprise-Empfängern* wird nur für Veröffentlichungen angezeigt, die für Enterprise-Empfänger vorgesehen sind.
5. Wählen Sie in der Spalte *Zuordnung dynamischer Empfänger* eine dynamische Empfängerquelle in der Liste aus.

   Das Berichtfeld wird einer Spalte in der dynamischen Empfängerquelle zugeordnet, die entsprechende Werte enthält.

   Die Spalte *Zuordnung dynamischer Empfänger* wird nur für Veröffentlichungen angezeigt, die für dynamische Empfänger vorgesehen sind.
6. Wiederholen Sie die Schritte 2 bis 5 für jedes zu filternde Berichtfeld.
7. Klicken Sie auf *OK*.

30.2.3 Veröffentlichungsformat für einen Crystal-Reports-Bericht auswählen

Sie können das Veröffentlichungsformat für einen Crystal-Reports-Bericht über *Veröffentlichungseigenschaften* > *Berichtselemente* > *Formate* auswählen.

Sie können mehrere Veröffentlichungsformate für einen Crystal-Reports-Bericht auswählen und konfigurieren. Wenn Sie ein Format auswählen, werden die verfügbaren Formatierungsoptionen angezeigt. Für einige Optionen, beispielsweise *Crystal Reports* und *Crystal Reports (RPTR)*, werden keine Formatierungsoptionen angezeigt und die standardmäßige Quelldokumentformatierung wird angewendet.

1. Klicken Sie mit der rechten Maustaste auf den Crystal-Reports-Bericht, um ein Veröffentlichungsformat festzulegen, und wählen Sie *Zeitgesteuerte Verarbeitung*.
2. Klicken Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* auf *Formate*.
3. Wählen Sie unter *Formatoptionen für ausgewähltes Dokument:* ein Format für die Veröffentlichung des Crystal-Reports-Berichts.

Die Optionen für das ausgewählte Format werden angezeigt.

4. Konfigurieren Sie die Formatierungsoptionen wie gewünscht.
5. Wenn das Kontrollkästchen *Im Bericht definierte Exportoptionen verwenden* verfügbar ist, führen Sie eine der folgenden Aktionen durch:
   - Aktivieren Sie das Kontrollkästchen, um die im Quelldokument definierten Standardexportoptionen zu verwenden.
   - Deaktivieren Sie das Kontrollkästchen, um Exportoptionen für das ausgewählte Format zu konfigurieren, und konfigurieren Sie dann die angezeigten Optionen.
6. Wiederholen Sie die Schritte 3 bis 5 für jedes Format, in dem Sie diesen Crystal-Reports-Bericht veröffentlichen möchten.
7. Klicken Sie auf *OK*.

Wiederholen Sie diese Aufgabe für jeden Crystal-Reports-Bericht in der Veröffentlichung.

30.2.3.1 Formatierungsoptionen für Crystal-Reports-Berichte

Wenn Sie *Tabulatorgetrennter Text (TTX)* als Formatierungsoption wählen, werden keine weiteren Optionen angezeigt. Die *PDF*-Optionen gelten für als PDF-Dateien veröffentlichte Quelldokumente.

Microsoft Excel (97-2003)

Option	Beschreibung
Seitenbereich	• Um einen gesamten Bericht als Excel-Datei zu veröffentlichen, wählen Sie *Alle*. • Um bestimmte Berichtsseiten zu veröffentlichen, wählen Sie *Seiten*, geben Sie die erste Seitenzahl in das Feld *von* und die letzte Seite in das Feld *bis* ein.
Wenn Sie das Kontrollkästchen *Im Bericht definierte Exportoptionen verwenden* deaktivieren, sind die folgenden Optionen verfügbar:	
Spaltenbreite festlegen	• Um die Spaltenbreite im Verhältnis zu Objekten in einem Bericht zu definieren, wählen Sie *Spaltenbreite basierend auf Objekten in* und wählen eine Option in der Liste aus: *Gesamter Bericht*, *Berichtskopf*, *Seitenkopf*, *Gruppenkopf #*, *Details*, *Gruppenfuß #*, *Seitenfuß* oder *Berichtsfuß*. • Um eine konstante Breite für alle Berichtsspalten zu definieren, wählen Sie *Gleichbleibende Spaltenbreite (in Punkt)* und geben eine Zahl in das Feld ein.

Option	Beschreibung
Seitenkopf und -fuß exportieren	Aktivieren Sie dieses Kontrollkästchen, um festzulegen, wie häufig Kopf- und Fußzeilen in Excel-Dateien angezeigt werden, und wählen Sie eine Option aus der Liste – *<ohne>*, *Einmal pro Bericht* oder *Auf jeder Seite*.
Seitenumbrüche für jede Seite erstellen	Aktivieren Sie dieses Kontrollkästchen, um Seitenumbrüche zu erstellen, die den Seitenumbrüchen im Bericht entsprechen.
Datumswerte zu Zeichenfolgen konvertieren	Aktivieren Sie dieses Kontrollkästchen, um Datumswerte in Textzeichenfolgen zu konvertieren.
Rasterlinien anzeigen	Aktivieren Sie dieses Kontrollkästchen, um Rasterlinien in Excel-Dateien einzuschließen.

Microsoft Excel (97-2003) (Nur Daten)

Wenn Sie das Kontrollkästchen *Im Bericht definierte Exportoptionen verwenden* deaktivieren, sind die folgenden Optionen verfügbar:

Option	Beschreibung
Spaltenbreite festlegen	• Um die Spaltenbreite im Verhältnis zu Objekten in einem Bericht zu definieren, wählen Sie *Spaltenbreite basierend auf Objekten in* und wählen eine Option in der Liste aus: *Gesamter Bericht*, *Berichtskopf*, *Seitenkopf*, *Gruppenkopf #*, *Details*, *Gruppenfuß #*, *Seitenfuß* oder *Berichtsfuß*. • Um eine konstante Breite für alle Berichtsspalten zu definieren, wählen Sie *Gleichbleibende Spaltenbreite (in Punkt)* und geben eine Zahl in das Feld ein.
Objektformatierung exportieren	Aktivieren Sie dieses Kontrollkästchen, um die Objektformatierung eines Berichts beizubehalten.
Bilder exportieren	Aktivieren Sie dieses Kontrollkästchen, um Berichtsbilder in Excel-Dateien zu veröffentlichen.
Arbeitsblattfunktionen für Gruppenergebnisse verwenden	Aktivieren Sie dieses Kontrollkästchen, um unter Verwendung von Berichtszusammenfassungen Arbeitsblattfunktionen für Excel-Dateien zu erstellen.
Relative Objektposition beibehalten	Aktivieren Sie dieses Kontrollkästchen, um die relative Position der Berichtsobjekte beizubehalten.

Option	Beschreibung
Spaltenausrichtung beibehalten	Aktivieren Sie dieses Kontrollkästchen, um die Spaltenausrichtung des Berichts beizubehalten.
Seitenkopf und -fuß exportieren	Aktivieren Sie dieses Kontrollkästchen, um festzulegen, wie häufig Kopf- und Fußzeilen in Excel-Dateien angezeigt werden, und wählen Sie eine Option aus der Liste – *<ohne>*, *Einmal pro Bericht* oder *Auf jeder Seite*.
Seitenköpfe vereinfachen	Aktivieren Sie dieses Kontrollkästchen, um Seitenköpfe in einem Bericht zu vereinfachen.
Gruppengliederungen anzeigen	Aktivieren Sie dieses Kontrollkästchen, um Gruppengliederungen aus einem Bericht anzuzeigen.

Microsoft Excel-Arbeitsmappe (nur Daten)

Wenn Sie das Kontrollkästchen *Im Bericht definierte Exportoptionen verwenden* deaktivieren, sind die folgenden Optionen verfügbar:

Option	Beschreibung
Spaltenbreite festlegen	• Um die Spaltenbreite im Verhältnis zu Objekten in einem Bericht zu definieren, wählen Sie *Spaltenbreite basierend auf Objekten in* und wählen eine Option in der Liste aus: *Gesamter Bericht*, *Berichtskopf*, *Seitenkopf*, *Gruppenkopf #*, *Details*, *Gruppenfuß #*, *Seitenfuß* oder *Berichtsfuß*. • Um eine konstante Breite für alle Berichtsspalten zu definieren, wählen Sie *Gleichbleibende Spaltenbreite (in Punkt)* und geben eine Zahl in das Feld ein.
Objektformatierung exportieren	Aktivieren Sie dieses Kontrollkästchen, um die Objektformatierung eines Berichts beizubehalten.
Bilder exportieren	Aktivieren Sie dieses Kontrollkästchen, um Berichtsbilder in Excel-Dateien zu veröffentlichen.
Arbeitsblattfunktionen für Gruppenergebnisse verwenden	Aktivieren Sie dieses Kontrollkästchen, um unter Verwendung von Berichtszusammenfassungen Arbeitsblattfunktionen für Excel-Dateien zu erstellen.
Relative Objektposition beibehalten	Aktivieren Sie dieses Kontrollkästchen, um die relative Position der Berichtsobjekte beizubehalten.

Option	Beschreibung
Spaltenausrichtung beibehalten	Aktivieren Sie dieses Kontrollkästchen, um die Spaltenausrichtung des Berichts beizubehalten.
Seitenkopf und -fuß exportieren	Aktivieren Sie dieses Kontrollkästchen, um festzulegen, wie häufig Kopf- und Fußzeilen in Excel-Dateien angezeigt werden, und wählen Sie eine Option aus der Liste – *<ohne>*, *Einmal pro Bericht* oder *Auf jeder Seite*.
Seitenköpfe vereinfachen	Aktivieren Sie dieses Kontrollkästchen, um Seitenköpfe in einem Bericht zu vereinfachen.
Gruppengliederungen anzeigen	Aktivieren Sie dieses Kontrollkästchen, um Gruppengliederungen aus einem Bericht anzuzeigen.

Microsoft Word (97-2003)

Option	Beschreibung
Seitenbereich	• Um einen gesamten Bericht als Word-Datei zu veröffentlichen, wählen Sie *Alle*. • Um bestimmte Berichtsseiten zu veröffentlichen, wählen Sie *Seiten*, geben Sie die erste Seitenzahl in das Feld *von* und die letzte Seite in das Feld *bis* ein.

PDF

Option	Beschreibung
Seitenbereich	• Um einen gesamten Bericht als PDF-Datei zu veröffentlichen, wählen Sie *Alle*. • Um bestimmte Berichtsseiten zu veröffentlichen, wählen Sie *Seiten*, geben Sie die erste Seitenzahl in das Feld *von* und die letzte Seite in das Feld *bis* ein.
Wenn Sie das Kontrollkästchen *Im Bericht definierte Exportoptionen verwenden* deaktivieren, ist die folgende Option verfügbar:	
Lesezeichen aus Gruppenstruktur erstellen	Aktivieren Sie dieses Kontrollkästchen, um auf der Grundlage der Gruppenstruktur Lesezeichen in der generierten PDF-Datei zu erstellen.

Rich Text Format (RTF)

Option	Beschreibung
Seitenbereich	• Um einen gesamten Bericht als RTF-Datei zu veröffentlichen, wählen Sie *Alle*. • Um bestimmte Berichtsseiten zu veröffentlichen, wählen Sie *Seiten*, geben Sie die erste Seitenzahl in das Feld *von* und die letzte Seite in das Feld *bis* ein.

Microsoft Word – Editierbar (RTF)

Option	Beschreibung
Seitenbereich	• Um einen gesamten Bericht als Word-Datei zu veröffentlichen, wählen Sie *Alle*. • Um bestimmte Berichtsseiten zu veröffentlichen, wählen Sie *Seiten*, geben Sie die erste Seitenzahl in das Feld *von* und die letzte Seite in das Feld *bis* ein.
Wenn Sie das Kontrollkästchen *Im Bericht definierte Exportoptionen verwenden* deaktivieren, ist die folgende Option verfügbar:	
Seitenwechsel nach jeder Berichtseite einfügen	Aktivieren Sie dieses Kontrollkästchen, um Seitenumbrüche zu erstellen, die den Seitenumbrüchen im Bericht entsprechen.

Nur Text

Wenn Sie das Kontrollkästchen *Im Bericht definierte Exportoptionen verwenden* deaktivieren, ist die folgende Option verfügbar:

Option	Beschreibung
Anzahl der Zeichen pro Zoll	Geben Sie die Anzahl der Zeichen ein, die pro Zoll in einer reinen Textdatei angezeigt werden sollen. Der empfohlene Bereich liegt zwischen 8 und 16.

Text mit Seitenzahlen

Wenn Sie das Kontrollkästchen *Im Bericht definierte Exportoptionen verwenden* deaktivieren, sind die folgenden Optionen verfügbar:

Option	Beschreibung
Zeilen pro Seite	Geben Sie die Anzahl der Zeilen ein, die auf jeder Seite einer paginierten Textdatei angezeigt werden sollen.
Anzahl der Zeichen pro Zoll	Geben Sie die Anzahl der Zeichen ein, die pro Zoll in einer paginierten Textdatei angezeigt werden sollen. Der empfohlene Bereich liegt zwischen 8 und 16.

Zeichengetrennte Werte (CSV)

Wenn Sie das Kontrollkästchen *Im Bericht definierte Exportoptionen verwenden* deaktivieren, sind die folgenden Optionen verfügbar:

Option	Beschreibung
Begrenzungszeichen	Geben Sie das als Begrenzungszeichen zu verwendende Zeichen ein.
Trennzeichen	Geben Sie das zum Trennen von Werten zu verwendende Zeichen ein, oder aktivieren Sie das Kontrollkästchen `Tab`, um Werte durch Tabulatoren zu trennen.
Modus	Wählen Sie *Standardmodus* (standardmäßig) oder *Legacy-Modus*. Im Standardmodus können Sie steuern, wie Berichtsseiten und Gruppenköpfe und -füße in der CSV-Ausgabe angezeigt werden.
Berichts- und Seitensektionen	• Wählen Sie *Exportieren*, um Berichts- und Seitensektionen zu exportieren. • Wählen Sie *Nicht exportieren*, wenn die Berichts- oder Seitensektionen nicht exportiert werden sollen. • Um die Berichts- und Seitensektionen zu trennen, aktivieren Sie das Kontrollkästchen *Berichts-/Seitensektionen isolieren*.

Option	Beschreibung
Gruppensektionen	• Wählen Sie *Exportieren*, um Gruppensektionen zu exportieren. • Wählen Sie *Nicht exportieren*, wenn die Gruppensektionen nicht exportiert werden sollen. • Um die Gruppensektionen zu trennen, aktivieren Sie das Kontrollkästchen *Berichts-/Seitensektionen isolieren*.

XML

Wenn Sie das Kontrollkästchen *Im Bericht definierte Exportoptionen verwenden* deaktivieren, ist die folgende Option verfügbar:

Option	Beschreibung
XML-Exportformate	Um das XML-Format anzugeben, wählen Sie eine Option aus der Liste.

30.2.4 (Optional) Druckoptionen für Crystal-Reports-Berichte in Veröffentlichungen auswählen

Sie können die Druckoptionen für einen Crystal-Reports-Bericht unter *Eigenschaften der Veröffentlichung* > *Berichtselemente* > *Druckeinstellungen* auswählen.

Bevor Sie die Druckoptionen für den Standarddrucker einstellen können, müssen die folgenden Voraussetzungen erfüllt sein:

- Der Drucker muss ordnungsgemäß installiert und konfiguriert sein.
- Der Crystal Reports Job Server muss unter einem Konto mit Berechtigungen ausgeführt werden, die den Zugriff auf den angegebenen Drucker erlauben.
  Weitere Informationen finden Sie im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.

Sie können Instanzen im Crystal-Reports-Format bei jeder Ausführung einer Veröffentlichung drucken, indem Sie den Standarddrucker des Crystal Reports Job Servers oder einen anderen Drucker auswählen. Die BI-Plattform druckt Instanzen nach der Personalisierung, jedoch vor dem Versand der Veröffentlichung.

1. Klicken Sie mit der rechten Maustaste auf den Crystal-Reports-Bericht, um Druckoptionen festzulegen, und wählen Sie *Zeitgesteuerte Verarbeitung*.
2. Klicken Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* auf *Druckeinstellungen*.
3. Wählen Sie unter *Dokumente* den Crystal-Reports-Bericht aus, der bei der Veröffentlichungsausführung gedruckt werden soll.
4. Aktivieren Sie das Kontrollkästchen *Crystal-Reports-Berichte bei zeitgesteuerter Verarbeitung drucken*.

Die Druckoptionen für den Crystal-Reports-Bericht werden angezeigt.

5. Wählen Sie *Standarddrucker*, um auf dem Standarddrucker des Job Servers zu drucken, oder wählen Sie *Drucker angeben* und wählen den Pfad und Namen des Druckers aus:
   - Wenn der Job Server unter Windows ausgeführt wird, geben Sie in das Feld *Drucker angeben* **`\\<Druckserver>\<Druckername>`** ein.
     Ersetzen Sie `<Druckserver>` durch den Namen des Druckerservers und `<Druckername>` durch den Namen des Druckers.
   - Wenn der Job Server unter Unix ausgeführt wird, bestätigen Sie, dass Unix angezeigt (nicht ausgeblendet) wird, und geben Sie den Druckbefehl, den Sie normalerweise verwenden, in das Feld *Drucker angeben* ein.
     Beispiel: Geben Sie **`lp -d <druckername>`** ein.
6. Geben Sie im Feld *Anzahl der Exemplare* die Anzahl der Kopien ein, die gedruckt werden sollen.
7. Wählen Sie unter *Seitenbereich* die Option *Alle* aus, um alle Seiten der Veröffentlichung zu drucken, oder wählen Sie *Seiten* und geben den zu druckenden Seitenbereich ein.
8. (Optional) Wählen Sie in der Liste *Sortieroption setzen auf:* die Option *Sortieren*, *Nicht sortieren* oder *Druckerstandardwerte verwenden*.
9. (Optional) Wählen Sie in der Liste *Seitenskalierung* die Option *Passend skalieren*, *Nur an Größe anpassen* oder *Nicht skalieren*.
10. (Optional) Um den Berichtsinhalt auf der Seite zu zentrieren, aktivieren Sie das Kontrollkästchen *Seite zentrieren*.
11. (Optional) Wenn der Crystal-Reports-Bericht breit ist und Sie ihn auf einer Seite drucken möchten, aktivieren Sie das Kontrollkästchen *Horizontale Seiten an eine Seite anpassen*.
12. Klicken Sie auf *Zeitgesteuert verarbeiten*.

30.2.5 (Optional) Versandregel für Empfänger für einen Crystal-Reports-Bericht in einer Veröffentlichung auswählen

Versandregeln für Empfänger legen fest, ob eine Veröffentlichung nach der Verarbeitung und Personalisierung an einen bestimmten Empfänger geliefert wird. Nach der Erstellung einer Veröffentlichung können Sie diese öffnen und die zugehörigen Versandregeln ändern.

1. Klicken Sie auf das Symbol *** neben der Veröffentlichung, für das die Versandregel festgelegt werden soll, und wählen Sie *Eigenschaften*.
2. Klappen Sie *Berichtsfunktionen* im Fenster *Veröffentlichungseigenschaften* auf, und klicken Sie in der Navigationsliste auf *Versandregeln*.
3. Wählen Sie unter *Versandregel für Empfänger* die Option *Einzelnes Dokument senden, wenn Bedingung erfüllt ist* oder *Alle Dokumente nur übermitteln, wenn sämtliche Bedingungen erfüllt sind*.
4. Wählen Sie in der Spalte *Bedingung* neben jedem Dokument die Bedingung aus, die erfüllt sein muss, bevor die Veröffentlichung versendet wird.
5. Klicken Sie auf *Speichern und schließen*.

30.2.6 (Optional) Globale Versandregel für eine Veröffentlichung auswählen

Durch globale Versandregeln wird festgelegt, ob eine Veröffentlichung verarbeitet und an alle Empfänger versendet werden kann. Eine globale Versandregel können Sie für jede Veröffentlichung in der BI-Plattform festlegen.

1. Klicken Sie auf das Symbol *** neben der Veröffentlichung, für das die Versandregel festgelegt werden soll, und wählen Sie *Eigenschaften*.
2. Erweitern Sie auf der Seite *Veröffentlichungseigenschaften* die Option *Berichtsfunktionen*, und klicken Sie in der Navigationsliste auf *Versandregeln*.
3. Klicken Sie unter *Globale Versandregel* auf *Durchsuchen*.
   Das Dialogfeld *Dokument auswählen* wird angezeigt. Sie können einen Crystal-Reports-Bericht als Quelle für die globale Versandregel auswählen.

   > **Hinweis**
   >
   > Der Crystal-Reports-Bericht muss eine Warnung enthalten.

4. Navigieren Sie zu dem Crystal-Reports-Bericht, wählen Sie ihn aus, und klicken Sie auf *OK*.
5. Wählen Sie in der Liste *Bedingung* die entsprechende Bedingung zur Verarbeitung und zum Versand der Veröffentlichung aus.
6. Klicken Sie auf *Speichern und schließen*.

30.2.7 (Optional) Zusammengeführte PDF-Dateien aus Crystal-Reports-Berichten formatieren

Voraussetzung für das Formatieren von zusammengeführten PDF-Dateien:

- Crystal-Reports-Berichte müssen über Titel verfügen, damit Sie in die zusammengeführte PDF-Datei eingefügt werden können. Um einem Bericht einen Titel zu geben, öffnen Sie den Bericht in SAP Crystal Reports, wählen *Datei* > *Gruppenergebnis-Info* und geben auf der Registerkarte *Gruppenergebnis* im Feld *Titel* einen Titel für den Bericht ein. Sichern Sie den Bericht, und exportieren Sie diesen erneut in das Repository.
- Für eine Veröffentlichung müssen die Crystal-Reports-Berichte und PDF-Dateien, die Sie zusammenführen möchten, im BI-Launchpad auf der Seite *Eigenschaften* unter *Quelldokumente* in der richtigen Reihenfolge aufgeführt sein.
- Klappen Sie für eine Veröffentlichung im BI-Launchpad auf der Registerkarte *Eigenschaften* die Option *Berichtsfunktionen* auf.
- Unter *Formate* muss das Kontrollkästchen *PDF* als Format für alle Crystal-Reports-Berichte aktiviert sein, die Sie in einer PDF-Datei zusammenführen möchten.
- Im BI-Launchpad muss auf der Seite *Zeitgesteuert verarbeiten* unter *Ziele* das Kontrollkästchen *Exportierte PDF zusammenführen* für jedes Ziel aktiviert sein, an das Sie die zusammengeführte PDF-Datei senden möchten.

Stellen Sie sicher, dass die zusammengeführte PDF-Datei detaillierte Lesezeichen enthält, um eine einfachere Navigation zu ermöglichen. Führen Sie diese Schritte für jeden Crystal-Reports-Bericht in der Liste aus.

- Wählen Sie den Bericht im Bereich *Formate* in der Liste *Dokumente* aus.
- Deaktivieren Sie das Kontrollkästchen *Im Bericht definierte Exportoptionen verwenden*.
- Aktivieren Sie das Kontrollkästchen *Lesezeichen aus Gruppenstruktur erstellen*.

Um eine zusammengeführte PDF-Datei zu formatieren, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf das Symbol *** neben der Veröffentlichung, für die Sie eine zusammengeführte PDF-Datei formatieren möchten, und wählen Sie *Eigenschaften*.
2. Erweitern Sie auf der Seite *Eigenschaften* die *Berichtsfunktionen*, und klicken Sie in der Navigationsliste auf *Optionen für zusammengeführte PDFs*.
3. Erstellen Sie ein Inhaltsverzeichnis für die zusammengeführte PDF-Datei:
   a. Aktivieren Sie die Umschaltfläche *Inhaltsverzeichnis erstellen*.
   Daraufhin werden die Formatoptionen für das Inhaltsverzeichnis angezeigt.
   b. Geben Sie im Feld *Titel* einen Titel für das Inhaltsverzeichnis ein.
   c. Wählen Sie in der Liste *Schriftart Titel* die Schriftart, den Schriftgrad (in Punkt) und die Schriftfarbe für den Titel des Inhaltsverzeichnisses aus.
   d. Wählen Sie in der Liste *Schriftart Element* die Schriftart, den Schriftgrad (in Punkt) und die Schriftfarbe für die Elemente des Inhaltsverzeichnisses aus.
4. Legen Sie das Format der Seitenzahlen für die zusammengeführte PDF-Datei fest:
   a. Aktivieren Sie die Umschaltfläche *Laufende Seitenzahlen anwenden*.
   Daraufhin werden die Formatoptionen für die Seitenzahlen angezeigt.
   b. Geben Sie in das Feld *Zahlenformat* ein Format für die Seitenzahlen ein.
   Standardmäßig ist das Format auf `Page &p of &P` festgelegt. Sie können dieses Format ändern, müssen jedoch `&p` als Platzhalter für die aktuelle Seitenzahl und `&P` als Platzhalter für die Gesamtanzahl an Seiten verwenden.
   c. Wählen Sie in der Liste *Position der Seitenzahl* die Ausrichtung der Seitenzahlen für die zusammengeführte PDF-Datei aus.
   d. Wählen Sie in der Liste *Schriftart Seitenzahl* die Schriftart, den Schriftgrad (in Punkt) und die Schriftfarbe der Seitenzahlen aus.
   e. Wenn das Inhaltsverzeichnis Seitenzahlen aufweisen soll, aktivieren Sie das Kontrollkästchen *Seitenzahlen auf Inhaltsverzeichnisseiten anwenden*.
5. Legen Sie die Anmeldedaten für die Empfänger und die Berechtigungen für Aktionen der Empfänger fest:
   a. Aktivieren Sie die Umschaltfläche *Beschränkungen festlegen*.
   b. Geben Sie im Feld *Benutzerkennwort* das Kennwort ein, das Empfänger zum Anzeigen der zusammengeführten PDF-Datei eingeben müssen.
   c. Geben Sie im Feld *Eigentümerkennwort* das Kennwort ein, das Empfänger zum Bearbeiten der zusammengeführten PDF-Datei eingeben müssen.
   d. Aktivieren Sie das Kontrollkästchen *Drucken zulassen*, damit die Empfänger die PDF-Datei drucken können.
   e. Aktivieren Sie das Kontrollkästchen *Ändern des Inhalts zulassen*, damit die Empfänger die PDF-Datei ändern können.
   f. Damit Empfänger PDF-Inhalte kopieren und einfügen können, aktivieren Sie das Kontrollkästchen *Kopieren und Einfügen zulassen*.

g. Aktivieren Sie das Kontrollkästchen *Ändern von Anmerkungen zulassen*, damit die Empfänger Anmerkungen in der PDF-Datei ändern können.

6. Klicken Sie auf *Speichern*.

30.2.8 Datenbank-Anmeldedaten für einen Crystal-Reports-Bericht in einer Veröffentlichung konfigurieren

Sie können die Datenbank-Anmeldedaten konfigurieren, die Empfänger für die Anmeldung an der Datenbank und zum Regenerieren der Daten im Crystal-Reports-Bericht verwenden.

Bestätigen Sie, dass die Datenbankeinstellungen für den Crystal-Reports-Bericht korrekt sind, oder ändern Sie die Standarddatenbankeinstellung eines Berichts. Wählen Sie in der CMC im Bereich *Ordner* den Crystal-Reports-Bericht aus, und wählen Sie *Verwalten* > *Standardeinstellungen* > *Datenbankkonfiguration* aus, um die Datenbankinformationen zu prüfen oder neue Informationen einzugeben.

> **Hinweis**
>
> Um zu vermeiden, dass vorhandene Dokumente oder Veröffentlichungen beschädigt werden, werden Änderungen in der **CMC-Datenbankkonfiguration** erst bei der nächsten zeitgesteuerten Verarbeitung oder Veröffentlichung dieses Crystal-Reports-Berichts angezeigt.

1. Klicken Sie auf das Symbol *** neben der Veröffentlichung, um Datenbankanmeldeinformationen zu konfigurieren, und wählen Sie *Zeitgesteuerte Verarbeitung* oder *Eigenschaften*.
2. Erweitern Sie auf der Seite *Zeitgesteuerte Verarbeitung* oder *Eigenschaften* die *Berichtsfunktionen*, und klicken Sie in der Navigationsliste auf *Databankanmeldung*.
3. Wählen Sie in der Liste *Datenquellen* eine Datenquelle aus.
   Die Datenbankinformationen für die Datenquelle werden im Bereich *Details* angezeigt.
4. Bestätigen Sie, dass die Informationen in den Feldern *Datenbankserver* und *Datenbank* korrekt sind.
5. Geben Sie im Feld *Benutzer* den Benutzernamen ein, den Empfänger für die Anmeldung verwenden müssen.
6. Geben Sie im Feld *Kennwort* das Kennwort ein, das Empfänger für die Anmeldung verwenden müssen.
7. Klicken Sie auf *Zeitgesteuert verarbeiten* (oder auf der Seite *Eigenschaften* auf *Speichern*).

   Sie können auch die Datenquelleninformationen, auf die der Crystal-Reports-Bericht verweist, im Bericht selbst ändern. Öffnen Sie den Bericht in SAP Crystal Reports, und wählen Sie *Datenbank* > *Speicherort der Datenquelle festlegen*. Wählen Sie eine Verbindung aus, oder erstellen Sie eine neue Verbindung im Dialogfeld *Datenquellenpfad festlegen*.

30.3 Web-Intelligence-Dokumente – Entwurfsaufgaben

30.3.1 Veröffentlichungsformat für ein Web-Intelligence-Dokument auswählen

Sie müssen für jedes Web-Intelligence-Dokument in einer Veröffentlichung, das aus einer Quelle mit dynamischem Inhalt stammt, ein Veröffentlichungsformat auswählen.

1. Führen Sie einen Rechtsklick auf das Web-Intelligence-Dokument aus, für das Sie ein Veröffentlichungsformat festlegen möchten, und wählen Sie *Zeitgesteuerte Verarbeitung*.
2. Klicken Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* in der Navigationsliste auf *Formate*.
3. Aktivieren Sie unter *Ausgabeformat* das Kontrollkästchen neben dem Format, in dem das Web-Intelligence-Dokument veröffentlicht werden soll:
   - *Web Intelligence*
   - *Microsoft Excel*
   - *Adobe Acrobat*
   - *mHTML*
4. Falls Sie *Kommagetrennte Werte (CSV)* unter *Formatierungsoptionen und Einstellungen* ausgewählt haben, führen Sie folgende Aktionen aus:
   a. Wählen Sie in der Liste *Textqualifizierer* einen Textqualifizierer aus.
   b. Wählen Sie in der Liste *Spaltenbegrenzungszeichen* ein Spaltenbegrenzungszeichen aus.
   c. Wählen Sie in der Liste *Zeichensatz* einen Zeichensatz aus.
   d. Wenn Sie einen neuen Zeichensatz eingeben möchten, aktivieren Sie das Kontrollkästchen *Neuen Zeichensatz eingeben*, und geben Sie den Zeichensatz in das Feld ein.
   e. Wenn Sie die Einstellungen als Standard verwenden möchten, aktivieren Sie das Kontrollkästchen *Als Standardwerte festlegen*.
   f. Wenn Sie einen kommagetrennten Wert für jede Datenquelle verwenden möchten, aktivieren Sie das Kontrollkästchen *Separate CSV pro Datenprovider generieren*.
5. Wiederholen Sie die Schritte 3 bis 4 für jedes Format, in dem Sie das Dokument veröffentlichen möchten.
6. Klicken Sie auf *OK*.

30.3.2 Web-Intelligence-Dokument mit einem globalen Profilziel personalisieren

Sie können ein Web-Intelligence-Dokument für Enterprise-Empfänger personalisieren, indem Sie anhand eines globalen Profilziels filtern.

- Bevor Sie Profile für die Personalisierung von Daten für Enterprise-Empfänger verwenden können, müssen die Profile in der BI-Plattform konfiguriert werden. Wenn das Profil in der Plattform nicht konfiguriert ist, schlägt die Personalisierung fehl.
- Stellen Sie vor dem Personalisieren eines Web-Intelligence-Dokuments sicher, dass das Profil ein globales Profilziel besitzt.

Wenn Sie unter *Globale Profile* die Personalisierung definieren, müssen Sie unter *Filter* keine Personalisierungsoptionen festlegen. Wenden Sie sich an die Systemverwaltung, wenn der BI-Plattform Profile hinzugefügt werden müssen.

1. Führen Sie einen Rechtsklick auf das Web-Intelligence-Dokument aus, um Ihre Einstellungen vorzunehmen, und wählen Sie *Zeitgesteuerte Verarbeitung*.
2. Klicken Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* in der Navigationsliste auf *Personalisierung*.
3. Wählen Sie unter *Globale Profile* in der Spalte *Zuordnung von Enterprise-Empfängern* ein Profil in der Liste aus.

   Durch dieses Profil wird das Dokument dem Universumsfeld (globales Profilziel) zugeordnet, das für Enterprise-Empfänger gefiltert wird.
4. Klicken Sie auf *OK*.

30.3.3 Web-Intelligence-Dokumente durch Filtern von Feldern personalisieren

Bevor Sie Profile für die Personalisierung von Daten verwenden können, müssen die Profile in der BI-Plattform konfiguriert werden. Wenn das Profil in der Plattform nicht konfiguriert ist, schlägt die Personalisierung fehl.

Profile mit statischen Werten können nur Zeichenfolgenfelder in Quelldokumenten filtern. Zum Filtern anderer Feldtypen verwenden Sie Ausdrucksprofilwerte. Wenn Sie einem Profil den falschen Feldtyp zuordnen, schlägt die Personalisierung fehl. Wenden Sie sich an die Systemverwaltung, wenn der Plattform Profile hinzugefügt werden müssen.

Durch die zeitgesteuerte Verarbeitung und Veröffentlichung eines Web-Intelligence-Dokuments im `.wid`-Format wird eine `.wid`-Datei generiert. Die Filter in `.wid`-Dateien können von jedem Empfänger, der die entsprechenden Zugriffsberechtigungen besitzt, entfernt werden. Sie sollten die Filter mit Überlegung verwenden, wenn die `.wid`-Datei an Empfänger oder Ziele gesendet wird. Wenn Sie z. B. ein Web-Intelligence-Dokument dahingehend filtern, dass die Informationen, die den Empfängern angezeigt werden, eingeschränkt werden, und dann die veröffentlichte `.wid`-Datei an Empfänger senden, kann jeder Empfänger mit den Berechtigungen zur Bearbeitung des Dokuments auch den Filter entfernen oder ändern und so auf Daten zugreifen, die nicht angezeigt werden sollten.

1. Führen Sie einen Rechtsklick auf das Web-Intelligence-Dokument aus, um Ihre Einstellungen vorzunehmen, und wählen Sie *Zeitgesteuerte Verarbeitung*.
2. Klicken Sie im Dialogfeld *Zeitgesteuerte Verarbeitung* in der Navigationsliste auf *Personalisierung*.
3. Wählen Sie unter *Lokale Profile* für jedes in der Spalte *Titel* aufgeführte Profil ein Profil aus der Liste in der Spalte *Berichtfeld* aus.

   Dieses Profil ordnet das Berichtfeld den Profilwerten für Enterprise-Empfänger zu.
4. Wählen Sie unter *Lokale Profile* in der Spalte *Zuordnung von Enterprise-Empfängern* ein Profil in der Liste aus.

   Durch dieses Profil wird das Dokument dem Universumsfeld (globales Profilziel) zugeordnet, das für Enterprise-Empfänger gefiltert wird.
5. Wählen Sie in der Spalte *Zuordnung dynamischer Empfänger* ein Profil aus der Liste.

   Das Feld im Quelldokument wird der Spalte zugeordnet, die die entsprechenden Werte in der dynamischen Empfängerquelle enthält.

6. Wiederholen Sie die Schritte 3 bis 5 für jedes zu filternde Feld.
7. Klicken Sie auf *OK*.

30.3.4 Bearbeiten von Parameter- oder Eingabeaufforderungswerten für ein Objekt

Wenn Sie in einem Inhaltsobjekt nicht die Standard-Parameter- oder -Eingabeaufforderungswerte verwenden möchten, können Sie die Werte bearbeiten.

Parameter und Eingabeaufforderungen fordern zur Eingabe von Informationen auf. In Berichtsobjekten bestimmen die eingegebenen Informationen u. U., welche Daten in einem Bericht angezeigt werden. In einem von Vertriebsmitarbeitern verwendeten Bericht könnten Sie durch einen Parameter beispielsweise zur Auswahl einer Region aufgefordert werden. Wenn eine Region ausgewählt wird, zeigt der Bericht die Ergebnisse nur für die ausgewählte Region an.

1. Klicken Sie im Titel *Dokumente* auf das Symbol *** neben dem Objekt, für das Sie Parameter- oder Eingabeaufforderungswerte zeitgesteuert verarbeiten möchten, und wählen Sie *Zeitgesteuert verarbeiten*.
2. Erweitern Sie auf der Seite *Zeitgesteuert verarbeiten* die *Berichtsfunktionen*, und klicken Sie in der Navigationsliste auf *Eingabeaufforderungen*.

   Die Optionen für Parameter oder Eingabeaufforderungen können sich von Objekt zu Objekt unterscheiden – je nachdem, wie Ihr Systemadministrator den Parameter bzw. die Eingabeaufforderung konfiguriert hat. Beispielsweise können Programmobjekte im Feld *Argument* angezeigt werden.

   Ist die Option *Eingabeaufforderungen* nicht verfügbar, enthält das Inhaltsobjekt, das zeitgesteuert verarbeitet werden soll, keine Parameter oder Eingabeaufforderungen.
3. (Nur Crystal-Reports-Berichte) Klicken Sie im Bereich *Eingabeaufforderungen* auf *Werte bearbeiten ...*, und bearbeiten Sie einen Parameterwert.
4. (Nur Web-Intelligence-Dokumente, die auf einer SAP BEx Query basieren) Klicken Sie im Bereich *Eingabeaufforderungen* auf *Ändern*, um einen Eingabeaufforderungswert zu bearbeiten, oder auf *Löschen*, um den Wert zu entfernen.

   In Web-Intelligence-Dokumenten werden Parameter als Eingabeaufforderungen bezeichnet. Wenn ein zeitgesteuertes Dokument ausgeführt wird, das auf SAP Business Explorer (SAP BEx) Querys basiert, kann der Wert einer Eingabeaufforderung durch eine SAP-BW-Datenquellenvariable festgelegt oder abgerufen werden. Eingabeaufforderungen können obligatorische Variablen in SAP BW-Datenquellen enthalten.

   Die SAP BW-Datenquelle muss in der Lage sein, den für eine Eingabeaufforderung angegebenen Wert zu verarbeiten. Kann die Datenquelle einen Wert nicht verarbeiten, schlägt die Ausführung des Dokuments fehl. So werden SAP-BW-Exit- oder Customer-Exit-Variablen beispielsweise häufig als dynamische Variablen in Eingabeaufforderungen verwendet.

   Ist die Schaltfläche *Löschen* nicht verfügbar, kann Ihr Administrator sie aktivieren, indem er `bex.dynamic_variable.schedule=true` in der Datei `<Installverz>\<WebAppServer>\webapps\boe\web-inf\config\custom\AnalyticalReporting.properties` setzt. Informationen hierzu finden Sie im *Administratorhandbuch für SAP BusinessObjects Business Intelligence*.
5. Klicken Sie auf *Zeitgesteuert verarbeiten*.

30.4 Aufgaben nach dem Entwurf

30.4.1 Veröffentlichung testen

Wenn Sie eine Veröffentlichung zuerst an sich selbst senden möchten, bevor Sie sie an andere Empfänger senden, verwenden Sie den Testmodus im BI-Launchpad.

Wenn Sie eine Veröffentlichung testen und sich selbst als Empfänger hinzugefügt haben, erhalten Sie dieselben Informationen, die auch an die in der Veröffentlichung konfigurierten Empfänger gesendet werden sollen. Sie können ggf. ausgewählte Empfänger von der ursprünglichen Empfängergruppe im Testmodus ausschließen. Auf diese Weise können Sie überprüfen, wie der Veröffentlichungsinhalt Ihren Empfängern angezeigt wird.

1. Wechseln Sie zu dem Ordner, in dem Sie die Veröffntlichung erstellt haben, und wählen Sie ••• (*Hier klicken, um weitere Optionen anzuzeigen*) → *Testmodus*.
2. (Optional) Ändern Sie die Empfänger im *Testmodus* nach Bedarf:
   a. Klicken Sie unter *Enterprise-Empfänger* auf Select.
   b. Unter *Verfügbare Empfänger* können Sie die Benutzer oder Benutzergruppen ein- oder ausschließen.
   c. Wählen Sie *OK*.
3. (Optional) Unter *Dynamische Empfänger* können Sie die Empfängerliste, die aus dem Dokument abgerufen wird, ändern, oder Sie können das Dokument entfernen.
4. Wählen Sie *Test*.

Die Veröffentlichung wird im Testmodus ausgeführt und danach an die vorgesehenen Testempfänger gesendet.

30.4.2 Veröffentlichung zeitgesteuert verarbeiten

Wenn Sie eine Veröffentlichung zeitgesteuert verarbeiten, können Sie das Standardwiederholungsmuster verwenden oder neue Werte eingeben, und Sie können bei jeder zeitgesteuerten Verarbeitung die Empfänger ändern.

Weitere Informationen zum Erstellen einer Veröffentlichung im Business-Intelligence-Launchpad finden Sie unter *Erstellen von Veröffentlichungen im BI-Launchpad* im *Benutzerhandbuch für das Business-Intelligence-Launchpad*.

Eine Veröffentlichung kann anschließend entworfen und gespeichert werden, bevor sie zeitgesteuert verarbeitet werden kann.

1. Klicken Sie auf das Symbol ••• neben der Veröffentlichung, und wählen Sie *Zeitgesteuert verarbeiten*.
2. Erweitern Sie auf der Registerkarte *Zeitgesteuert verarbeiten* die Option *Allgemein*, und wählen Sie in der Navigationsliste *Wiederholung*, und bestätigen Sie, dass die in der Liste *Bericht ausführen* ausgewählte Option korrekt ist.
3. Klicken Sie auf *Zeitgesteuert verarbeiten*.

30.4.2.1 Anzeigen von Veröffentlichungsergebnissen

Die Veröffentlichungsergebnisse können vom Veröffentlicher, von Empfängern sowie in einer Protokolldatei für den Veröffentlichungsauftrag eingesehen werden.

Anzeigen von Ergebnissen als Publisher

Sie können die Ergebnisse einer Veröffentlichung auf verschiedene Arten anzeigen. Nach Ausführung einer Veröffentlichung wird der Veröffentlichungsverlauf mit einer Aufllistung der Veröffentlichungsinstanzen, den Uhrzeiten der Veröffentlichungsausführung und dem Ausführungsstatus der Veröffentlichung (erfolgreich oder fehlgeschlagen) angezeigt. In der Spalte *Instanzenzeit* können Sie auf eine Verknüpfung zu einer Veröffentlichungsinstanz klicken, um die für alle Empfänger zum Ausführungszeitpunkt der Veröffentlichung generierten Instanzen anzuzeigen.

Anzeigen von Protokolldateien für Veröffentlichungsaufträge

Protokolldateien sind zur Fehlerbehebung von Veröffentlichungen sowie zur Ermittlung der Empfänger, die eine Veröffentlichungsinstanz nicht erhalten haben, nützlich. Die BI-Plattform protokolliert Informationen zu den Veröffentlichungsaufträgen, während die einzelnen Stapel personalisierter Veröffentlichungsinstanzen verarbeitet werden, und konsolidiert die Informationen dann in einer oder mehreren Protokolldateien. Die maximale Größe der Protokolldatei beträgt 10 MB und kann nicht geändert werden. Bei Ausführung einer umfangreichen Veröffentlichung mit zahlreichen Einzelinformationen kann die Veröffentlichungsinstanz über mehrere Protokolldateien verfügen.

Protokolldateien für eine Veröffentlichungsinstanz können folgendermaßen im Dialogfeld *Verlauf* angezeigt werden:

- Um die letzte Protokolldatei in einer Serie anzuzeigen, klicken Sie in der Spalte *Status* auf den Status ("Erfolg", "Fehler" oder "Wird ausgeführt"), und klicken Sie dann unten im Dialogfeld *Instanzendetails* auf *Protokolldatei anzeigen*. Sie können die letzte Protokolldatei während der Ausführung der Veröffentlichung anzeigen.
- Um alle Protokolldateien anzuzeigen, klicken Sie in der Spalte *Instanzenzeit* auf die Verknüpfung einer Veröffentlichungsinstanz. Die Protokolldateien sind hinter den personalisierten Instanzen aufgeführt.

Die Aktualisierung der Protokolldateien mit neuen Informationen erfolgt alle zwei Minuten. Wenn Ihr Veröffentlichungsauftrag in weniger als zwei Minuten ausgeführt wurde, hat die Protokolldatei möglicherweise den Status "Ausstehend".

Anzeigen von Ergebnissen als Empfänger

Die folgende Tabelle enthält eine Zusammenfassung der verschiedenen Möglichkeiten zur Anzeige von Veröffentlichungen:

Ziel	So zeigen Sie Veröffentlichungsergebnisse an
Enterprise-Standardspeicherort	Dynamische Empfänger können sich nicht bei der BI-Plattform anmelden, um Veröffentlichungsergebnisse anzuzeigen. Als Empfänger können Sie nur Ihre eigenen personalisierten Veröffentlichungsinstanzen in der Plattform anzeigen. Sie können keine Veröffentlichungsinstanzen anzeigen, die für andere Empfänger personalisiert wurden.
BI-Posteingang	Dynamische Empfänger können sich nicht an der BI-Plattform anmelden, um Veröffentlichungsergebnisse anzuzeigen.
E-Mail	Melden Sie sich bei Ihrer E-Mail-Anwendung an, um den eingebetteten Veröffentlichungsinhalt anzuzeigen oder Anhänge herunterzuladen.
FTP-Server	Melden Sie sich bei Ihrem FTP-Host an.
SFTP-Server	Melden Sie sich bei Ihrem SFTP-Host an.
Lokaler Datenträger	Navigieren Sie zu dem beim Entwurf der Veröffentlichung angegebenen Speicherort.

30.4.3 Abonnieren von Veröffentlichungen bzw. Aufheben eines Abonnements

Zum Abonnieren einer Veröffentlichung nach der zeitgesteuerten Verarbeitung dieser Veröffentlichung abonnieren Sie deren wiederkehrende Instanz oder verarbeiten die Veröffentlichung erneut zeitgesteuert.

Nur wenn Sie entsprechende Zugriffsrechte für Veröffentlichungen besitzen, können Sie diese abonnieren.

Nur Enterprise-Empfänger können eine Veröffentlichung abonnieren oder das Abonnement aufheben. Dynamische Empfänger können Veröffentlichungen weder abonnieren noch das Abonnement aufheben.

1. Wählen Sie auf der Startseite die Kachel *Ordner*.
2. Navigieren Sie zu dem Ordner, in dem sich eine Veröffentlichung befindet, die Sie abonnieren möchten oder für die Sie das Abonnement aufheben möchten.
3. Klicken Sie auf das Symbol *** neben der Veröffentlichung, und wählen Sie *Abonnieren* oder *Abonnement aufheben*.

   Abhängig von Ihrer Auswahl haben Sie nun eine Veröffentlichung abonniert oder das Abonnement aufgehoben.

30.4.4 Abonnieren einer Veröffentlichungsinstanz oder Aufheben eines Abonnements

Nachdem eine wiederkehrende Veröffentlichung zeitgesteuert verarbeitet wurde, können Enterprise-Empfänger die erste wiederkehrende Instanz abonnieren. Wenn eine Veröffentlichung beispielsweise zweimal pro Woche ausgeführt wird, können Sie die erste Veröffentlichungsinstanz abonnieren, die zweite jedoch nicht.

Nur wenn Sie entsprechende Zugriffsrechte für Veröffentlichungen besitzen, können Sie deren Instanzen abonnieren.

Enterprise-Empfänger können eine Veröffentlichungsinstanz abonnieren oder das Abonnement aufheben. Dynamische Empfänger können Veröffentlichungsinstanzen nicht abonnieren oder das Abonnement aufheben.

1. Wählen Sie in der Gruppe *Meine Startseite* die Kachel *Ordner*.
2. Navigieren Sie zu dem Ordner, in dem sich eine Veröffentlichung mit der zugehörigen Instanz befindet, die Sie abonnieren möchten bzw. deren Abonnement Sie aufheben möchten.
3. Klicken Sie auf das Symbol *** neben der Veröffentlichung, und wählen Sie *Verlauf*.
4. Klicken Sie auf der Seite *Verlauf* auf das Symbol *** neben der Instanz, und wählen Sie *Abonnieren* oder *Abonnement aufheben*.

   Abhängig von Ihrer Auswahl haben Sie nun eine Veröffentlichungsinstanz abonniert oder das Abonnement aufgehoben.

30.4.5 Veröffentlichungsinstanz neu verteilen

Wenn Sie eine Instanz an einen Empfänger zurücksenden möchten, jedoch nicht die gesamte Veröffentlichung erneut ausführen möchten, können Sie erfolgreiche Veröffentlichungsinstanzen erneut an alle oder bestimmte ursprüngliche Empfänger verteilen.

Nur Empfänger, die bei der ursprünglichen Ausführung der Veröffentlichung angegeben waren, können neu verteilte Instanzen erhalten.

1. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie im BI-Launchpad mit der rechten Maustaste auf eine Veröffentlichung, und wählen Sie *Verlauf*.
   - Klicken Sie in der Central Management Console (CMC) mit der rechten Maustaste auf eine Publikation, und wählen Sie *Aktionen* > *Verlauf* aus.
2. Wählen Sie im Dialogfeld *Verlauf* eine erfolgreiche Veröffentlichungsinstanz aus.
3. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie im BI-Launchpad *Weitere Aktionen* > *Neu planen* aus.
   - Wählen Sie in der CMC *Aktionen* > *Neu planen* aus.
4. Wählen Sie die Empfänger aus, die neu verteilte Instanzen erhalten sollen:
   - Um eine Instanz neu an Enterprise-Empfänger zu verteilen, klicken Sie auf die Schaltfläche *Enterprise-Empfänger*, und klicken Sie auf die Schaltfläche>, um Empfänger von der Liste *Verfügbar* in die Liste *Ausgewählt* zu verschieben.

- So verteilen Sie eine Instanz an dynamische Empfänger neu:

a. Klicken sie auf *Dynamische Empfänger*, und bestätigen Sie, dass Empfänger-IDs, vollständigen Namen und E-Mail-Adressen zugeordnete Empfänger-IDs korrekt sind.
b. Um die Veröffentlichung an alle dynamischen Empfänger neu zu verteilen, wählen Sie *Gesamte Liste verwenden*.
c. Um die Veröffentlichung neu an ausgewählte dynamische Empfänger zu verteilen, klicken Sie auf die Schaltfläche >, um Empfänger von der Liste *Verfügbar* in die Liste *Ausgewählt* zu verschieben.

5. Klicken Sie auf *Neu verteilen*.
   Der Veröffentlichungsverlauf wird angezeigt, und die neu verteilte Instanz hat den Status "Wird ausgeführt". Das Datum, in der Spalte *Instanzenzeit* wird auf die Uhrzeit der Neuverteilung aktualisiert.

30.4.6 Fehlgeschlagene Veröffentlichung wiederholen

Bevor Sie eine fehlgeschlagene Veröffentlichung wiederholen, zeigen Sie für die Veröffentlichungsinstanz die Protokolldatei an, beseitigen gegebenenfalls Fehler und planen die Veröffentlichung erneut zeitgesteuert ein.

Mithilfe der Option zum "Wiederholen" fehlgeschlagener Instanzen einer Veröffentlichung können Sie:

- Die "fehlgeschlagene" Instanz überschreiben (*Sofort ausführen* und *Erneut zeitgesteuert verarbeiten* erstellen neue Instanzen, wohingegen *Wiederholen* die fehlgeschlagene Instanz selbst verwendet).
- Nur die fehlgeschlagenen Empfänger verarbeiten (bei einer teilweise fehlgeschlagenen Veröffentlichung).
- Den vollständigen Auftrag ausführen, ohne eine neue Instanz zu erstellen (bei einer vollständig fehlgeschlagenen Veröffentlichung).

> **Hinweis**
>
> Sie können die automatische Wiederholung veranlassen, indem Sie unter der Eigenschaft *Wiederholung* der Veröffentlichung die *Zulässige Anzahl der Wiederholungen* sowie das *Wiederholungsintervall in Sekunden* angeben. Bei Fehlschlagen der Veröffentlichung wird ein wiederholter Versuch ausgeführt.

1. Wählen Sie die fehlgeschlagene Veröffentlichungsinstanz aus.
2. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie im BI-Launchpad *Weitere Aktionen* > *Verlauf* aus.
   - Wählen Sie in der Central Management Console (CMC) *Aktionen* > *Verlauf* aus.
3. Klicken Sie mit der rechten Maustaste auf die fehlgeschlagene Instanz, und klicken Sie auf *Wiederholen*.
   Der Status der Instanz ändert sich in *Wird ausgeführt*. Warten Sie, bis sich der Status in *Erfolgreich* geändert hat.

Wenn die Veröffentlichung erneut fehlschlägt, lesen Sie die neue Protokolldatei, und beheben Sie alle aufgetretenen Fehler.

31 Rechte (Anhang)

31.1 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*.

31.2 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.
Objekte dem Ordner 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.

Recht	Beschreibung
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.
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 zur 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.

Recht	Beschreibung
	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 zeitsteuern	*Auf Ziele zeitsteuern* ist das übergeordnete Recht von *An FTP, SMP, BI-Posteingang, SFTP zeitgesteuert verarbeiten* und *Dateisystem*. Wählen Sie das Recht *Auf Ziele zeitsteuern* in Kombination mit dem spezifischen untergeordneten Recht aus, um ein Objekt für das spezifische Ziel zeitgesteuert zu verarbeiten. Wählen Sie beispielsweise die Rechte *Auf Ziele zeitsteuern* und *An FTP zeitgesteuert verarbeiten*, um ein Objekt für ein FTP-Ziel zeitgesteuert zu verarbeiten. Wenn Sie BI-Landschaften ab BI 4.2 SP 4 auf BI 4.2 SP 5 oder höher aktualisieren, finden Sie weitere Informationen zur Fehlerbehebung in 2675734, 2642221, 2626550. Um ein 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). **Hinweis** Wenn das Recht *Auf Ziele zeitsteuern* über die *Zugriffsberechtigung* zugeordnet wird, wie z.B. die Rollen *Voller Zugriff* oder *Zeitgesteuert verarbeiten* in BI 4.2 SP 4 oder früher, werden nach der Aktualisierung auf BI 4.2 SP 5 Patch 03 oder höher auch die untergeordneten Zielrechte, wie z.B. *An FTP, SMP, BI-Posteingang, SFTP zeitgesteuert verarbeiten* und *Dateisystem* ebenso erteilt. Für *Zugriffsberechtigungen* wie *Ansicht auf Abruf* und vorhandene *Benutzerdefinierte Rollen* in BI 4.2 SP 4 oder früher werden nach der Aktualisierung auf BI 4.2 SP 5 Patch 03 oder höher die untergeordneten Zielrechte nicht standardmäßig erteilt. Erteilen Sie die Rechte manuell. Daher kann der Wiederholungsjob für die zeitgesteuerte Verarbeitung, der in BI 4.2 SP 4 oder

Recht	Beschreibung
	früher angelegt wurde, Objekte in BI 4.2 SP 5 Patch 03 oder höher erfolgreich zeitgesteuert verarbeiten.
An FTP zeitgesteuert verarbeiten	Ermöglicht die zeitgesteuerte Verarbeitung von Objekten für ein FTP-Ziel.
An SFTP zeitgesteuert verarbeiten	Ermöglicht die zeitgesteuerte Verarbeitung von Objekten für ein SFTP-Ziel.
An SMTP zeitgesteuert verarbeiten	Ermöglicht die zeitgesteuerte Verarbeitung von Objekten für ein SMTP-Ziel.
An Dateisystem zeitgesteuert verarbeiten	Ermöglicht die zeitgesteuerte Verarbeitung von Objekten für ein Dateisystem-Ziel.
An BI-Posteingang zeitgesteuert verarbeiten	Ermöglicht die zeitgesteuerte Verarbeitung von Objekten für ein BI-Posteingangsziel.
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.
Kommentare hinzufügen – BI-Kommentar	Ermöglicht das Hinzufügen von Kommentaren zu einem Dokument mittels BI-Kommentar.
Kommentare löschen – BI-Kommentar	Ermöglicht das Löschen von Kommentaren aus einem Dokument mittels BI-Kommentar.
Löschen von durch Benutzer erstellten Kommentaren – BI-Kommentar	Ermöglicht das Löschen von durch Benutzer erstellten Kommentaren aus einem Dokument mittels BI-Kommentar.
Ändern von Kommentaren – BI-Kommentar	Ermöglicht das Ändern von Kommentaren in einem Dokument mittels BI-Kommentar.

Recht	Beschreibung
Ändern von durch Benutzer erstellten Kommentaren – BI-Kommentar	Ermöglicht das Ändern von durch Benutzer erstellten Kommentaren in einem Dokument mittels BI-Kommentar.
Anzeigen von Kommentaren – BI-Kommentar	Ermöglicht das Anzeigen von Kommentaren zu einem Dokument mittels BI-Kommentar.
Anzeigen von durch Benutzer erstellten Kommentaren – BI-Kommentar	Ermöglicht das Anzeigen von Kommentaren, die Benutzer zu einem Dokument erstellt haben, mittels BI-Kommentar.
Ausblenden von Kommentaren – BI-Kommentar	Ermöglicht das Ausblenden von Kommentaren zu einem Dokument mittels BI-Kommentar.
Ausblenden von durch Benutzer erstellten Kommentaren – BI-Kommentar	Ermöglicht das Ausblenden von Kommentaren, die Benutzer zu einem Dokument erstellt haben, mittels BI-Kommentar.
Kommentare massenhinzufügen – BI-Kommentar	Ermöglicht Benutzern, die Kommentare zusammen mit dem Dokument zu migrieren.

31.2.1 Zielrechte

Jedes Ziel ist mit einem bestimmten Zielrecht verknüpft. Der BOE-Administrator sollte sicherstellen, dass die Benutzer die gewünschten Zielrechte haben.

Mit dem Recht *Auf Ziele zeitsteuern* konnten Benutzer früher auf alle verfügbaren Ziele zeitgesteuert verarbeiten. Ab dem Release SP05 wurden individuelle Zielrechte für Benutzer vergeben, wobei *Auf Ziele zeitsteuern* ausschließlich dem *Enterprise-Standardspeicherort* entspricht.

Für jedes Ziel werden unter Allgemeine Rechte neue Rechte eingeführt:

- An Dateisystem zeitgesteuert verarbeiten
- An FTP zeitgesteuert verarbeiten
- An Posteingang zeitgesteuert verarbeiten
- An SFTP zeitgesteuert verarbeiten
- An SMTP zeitgesteuert verarbeiten
- An Google Drive zeitgesteuert verarbeiten

Weitere Informationen zu *allgemeinen Rechten* finden Sie unter Allgemeine Rechte [Seite 475].

Damit diese Zieloptionen bei der zeitgesteuerten Verarbeitung zur Verfügung stehen, muss der Administrator die entsprechenden individuellen Zielrechte vergeben. Siehe dazu 2621878. Wenn der Benutzer nur das Recht *Auf Ziele zeitsteuern* hat, kann er nicht auf die Ziele FTP, Posteingang, SFTP, SMTP und Dateisystem zeitgesteuert verarbeiten.

Wenn *Auf Ziele zeitsteuern* in einer früheren Version über die Zugriffsberechtigung zugeordnet wurde, z. B. über die Rollen "Voller Zugriff" oder "Zeitgesteuert verarbeiten", dann werden nach einem Upgrade auf 4.2 SP05 zusätzliche (neu eingeführte) Rechte gewährt. Auf diese Weise ist die zeitgesteuerte Verarbeitung für beliebige Ziele erfolgreich.

Wenn das Recht über die Zugriffsberechtigung *Auf Abruf*, über eine benutzerdefinierte Rolle oder direkt zugeordnet wurde (einzelnes Recht, nicht über eine Rolle), dann wird nur die zeitgesteuerte Verarbeitung auf das Ziel *Enterprise-Standardspeicherort* funktionieren, und andere Ziele schlagen fehl.

Weitere Informationen finden Sie unter Zieloptionen und Eigenschaften für E-Mail-Ziele [Seite 172].

31.3 Rechte für bestimmte Objekttypen

31.3.1 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.
- Typspezifische Rechte für die Ordnerinhalte (wie das Recht *Berichtsdaten drucken* für Crystal-Reports-Berichte).

31.3.2 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

Recht	Beschreibung
	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.

31.3.3 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.

31.3.4 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	Erlaubt einem Benutzer, Berichtsdaten im Text-, CSV-, Excel-, PDF- oder HTML-Format zu exportieren. Mit diesem Befehl können Sie auch den Druckbefehl verwenden, der eine druckbare PDF-Datei generiert.
Abfrageskript: Anzeige aktivieren (SQL , MDX...)	Ermöglicht das Anzeigen von Abfrageskripten (SQL und MDX).
Abfrageskript: Bearbeitung aktivieren (SQL, MDX...)	Ermöglicht das Bearbeiten von Abfrageskripten (SQL und MDX). Sie können auch Freehand-SQL-Datenquellen bearbeiten (FHSQL).
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.
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.

31.3.5 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, gilt als Eigentümer des Kontos. Allerdings ist nach dem Erstellen des Benutzerkontos der Benutzer, für den das Konto erstellt wurde, ebenfalls Eigentümer.

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.

Recht	Beschreibung
Benutzerattribute hinzufügen oder bearbeiten (Eigentümerrecht)	Ermöglicht dem Eigentümer eines Benutzerobjekts die Änderung des Werts der E-Mail-Adresse eines Benutzers oder benutzerdefinierter Benutzerattribute. Dieses Recht gilt für Benutzer.
Einstellungen für Objekte des Benutzers ändern	Zeigt das Menü *Einstellungen* in einem Anwendungsobjekt an Ohne dieses Zugriffsrecht kann der Benutzer keine persönlichen Einstellungen in einer Anwendung vornehmen, und das Menü "Einstellungen" wird in den Anwendungen nicht angezeigt. Beispielsweise kann der Benutzer ohne dieses Recht nicht die Maßeinheit (Zoll oder Millimeter) für Berichte in der Web-Intelligence- oder BI-Launchpad-Anwendung auswählen.

31.3.6 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.

31.3.7 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*.
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:

Recht	Beschreibung
	• 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* .
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.

31.3.8 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.

Recht	Beschreibung
Sicherheitsprofile bearbeiten	Ermöglicht das Einfügen, Bearbeiten und Löschen von Sicherheitsprofilen für das Universum im Information-Design-Tool-Sicherheitseditor. **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.

31.3.9 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.

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 488]

31.3.9.1 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.

31.3.10 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.

Relationale Verbindungsrechte

Recht	Beschreibung
Objekte anzeigen	Ermöglicht es, die Verbindung anzuzeigen.
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.
Verbindung für Free-Hand-SQL-Skripts verwenden	Ermöglicht für Verbindungen die Ausführung von SQL-Skripts.

OLAP-Verbindungsrechte

Recht	Beschreibung
Objekte anzeigen	Ermöglicht es, die Verbindung anzuzeigen.
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.
Verbindung lokal herunterladen	Ermöglicht die Verwendung von auf der Verbindung im Web-Intelligence-Rich-Client erstellten Universen im Offline-Modus.

31.3.11 Anwendungen

31.3.11.1 CMC

Recht	Beschreibung
An der CMC anmelden und dieses Objekt in der CMC anzeigen	Ermöglicht dem Benutzer, sich an der CMC anzumelden
Zugriff auf Instanzen-Manager zulassen	Ermöglicht dem Benutzer, auf den Instanzen-Manager zuzugreifen
Zugriff auf Beziehungsabfrage zulassen	Ermöglicht dem Benutzer, Beziehungsabfragen in der CMC auszuführen
Zugriff auf Sicherheitsabfrage zulassen	Ermöglicht dem Benutzer, Sicherheitsabfragen in der CMC auszuführen

31.3.11.2 Fiorisiertes BI-Launchpad

Berechtigung	Beschreibung
Anmelden am neuen fiorisierten BI-Launchpad	Ermöglicht dem Benutzer die Anmeldung am fiorisierten BI-Launchpad

Berechtigung	Beschreibung
Organisieren	Ermöglicht dem Benutzer, Objekte in den Ordner `Favoriten` zu verschieben und zu kopieren sowie Verknüpfungen zu Objekten zu erstellen
An Business Objects-Posteingang senden	Ermöglicht dem Benutzer, Objekte an den BI-Posteingang von Empfängern zu senden
An E-Mail-Ziel senden	Ermöglicht dem Benutzer, Objekte per E-Mail an Empfänger zu senden
An Dateispeicherort senden	Ermöglicht dem Benutzer, Objekte an einen Dateispeicherort zu senden
An FTP-Adresse senden	Ermöglicht dem Benutzer, Objekte an eine FTP-Adresse zu senden
An SFTP-Adresse senden	Ermöglicht dem Benutzer, Objekte an eine SFTP-Adresse zu senden Das SFTP-Ziel hat die gleichen Eigenschaften wie die FTP-Zielseite, darüber hinaus aber eine Fingerabdruckoption, die vom Benutzer bereitzustellen ist. Jeder SFTP-Server verfügt in seinen Eigenschaften über die Fingerabdruck-Option. Die Prüfung des Fingerabdrucks erfolgt im Backend durch den CMS.

31.3.11.2.1 Rechte für Anwendungen für die Zusammenarbeit

Diese Zugriffsrechte gelten für SAP Jam, wenn die Anwendung in der BI-Plattform konfiguriert ist.

Recht	Beschreibung
Dem Benutzer gehörende Dokumente kommentieren	Ermöglicht dem Benutzer, seine eigenen Dokumente und Instanzen zu kommentieren
Kommentare zu dem Benutzer gehörenden Dokumenten anzeigen	Ermöglicht dem Benutzer, Kommentare zu seinen eigenen Dokumenten und Instanzen anzuzeigen
Einstellungen für Objekte des Benutzers ändern	Zeigt das Menü *Einstellungen* in einem Anwendungsobjekt an Ohne dieses Zugriffsrecht kann der Benutzer keine persönlichen Einstellungen in einer Anwendung vornehmen, und das Menü *Einstellungen* wird in den Anwendungen nicht angezeigt. Beispielsweise kann der Benutzer ohne dieses Recht nicht die Maßeinheit (Zoll oder Millimeter) für Berichte in der Anwendung auswählen.

31.3.11.3 BI-Arbeitsbereiche

Recht	Beschreibung
BI-Arbeitsbereiche erstellen und bearbeiten	Ermöglicht dem Benutzer, neue BI-Arbeitsbereiche erstellen und vorhandene BI-Arbeitsbereiche zu bearbeiten.
Module erstellen und bearbeiten	Ermöglicht dem Benutzer, neue Module zu erstellen und vorhandene Module zu bearbeiten
BI-Arbeitsbereiche bearbeiten	Ermöglicht dem Benutzer, vorhandene BI-Arbeitsbereiche zu bearbeiten (er kann jedoch keine neuen Arbeitsbereiche erstellen)
Einstellungen für Objekte des Benutzers ändern	Zeigt das Menü *Einstellungen* in einem Anwendungsobjekt an Ohne dieses Zugriffsrecht kann der Benutzer keine persönlichen Einstellungen in einer Anwendung vornehmen, und das Menü *Einstellungen* wird in den Anwendungen nicht angezeigt. Beispielsweise kann der Benutzer ohne dieses Recht nicht die Maßeinheit (Zoll oder Millimeter) für Berichte in der Web-Intelligence- oder BI-Launchpad-Anwendung auswählen.

31.3.11.4 Web Intelligence

Die Zugriffsrechte in diesem Abschnitt beziehen sich auf die Web-Intelligence-Anwendung, einschließlich der Rich-Client-Schnittstelle, und können sich auf Viewer und Abfrageeditoren in dieser Anwendung auswirken.

Recht	Beschreibung
Daten: Datentracking aktivieren	Ermöglicht dem Benutzer, geänderte Daten zu verfolgen
Daten: Formatierung geänderter Daten aktivieren	Ermöglicht dem Benutzer, die Formatierung für geänderte Daten auszuwählen
Allgemein: Desktop-Client-Zugriff aktivieren	Ermöglicht die Verwendung des Web Intelligence Desktop (Rich-Client)
Desktop: Dokumente exportieren	Ermöglicht dem Benutzer, im Web-Intelligence-Rich-Client Dokumente in das BI-Plattform-Repository zu exportieren
Desktop: Dokumente für alle Benutzer speichern	Ermöglicht dem Benutzer, im Web-Intelligence-Rich-Client Dokumente lokal ohne Sicherheit zu speichern
Dokumente: Automatische Regenerierung beim Öffnen deaktivieren	Verhindert, dass Dokumente beim Öffnen automatisch regeneriert werden

Recht	Beschreibung
Dokumente: Automatische Speicherung aktivieren	Ermöglicht das automatische Speichern von Dokumenten, wenn diese Funktion vom Administrator in der CMC aktiviert wurde
Dokumente: Erstellung aktivieren	Ermöglicht dem Benutzer, neue Dokumente zu erstellen
Allgemein: Web-Intelligence-Einstellungen bearbeiten	Ermöglicht dem Benutzer das Ändern der Web-Intelligence-Einstellungen im BI-Launchpad
Allgemein: Web-Client-Zugriff aktivieren	Ermöglicht dem Benutzer die Verwendung des Web-Intelligence-Web-Clients
Abfrage: Aus Universum generiertes Skript bearbeiten	Ermöglicht dem Benutzer, die aus Universen generierten SQL- oder MDX-Abfrageskripte zu bearbeiten
Abfrage: Freehand-SQL bearbeiten	Ermöglicht dem Benutzer das Bearbeiten von Freehand-SQL-Abfrageskripten
Abfrage: Aus Universum generiertes Skript anzeigen	Ermöglicht dem Benutzer, die aus Universen generierten SQL- oder MDX-Abfrageskripte im Abfrageeditor anzuzeigen
Abfrage: Freehand-SQL anzeigen	Ermöglicht dem Benutzer das Anzeigen von Freehand-SQL-Abfrageskripten
Berichterstellung: Gruppenwechsel erstellen und bearbeiten	Ermöglicht dem Benutzer das Erstellen und Bearbeiten von Gruppenwechseln
Berichterstellung: Regeln zur bedingten Formatierung erstellen und bearbeiten	Ermöglicht dem Benutzer, Regeln zur bedingten Formatierung zu erstellen und zu bearbeiten
Berichterstellung: Vordefinierte Berechnungen erstellen und bearbeiten	Ermöglicht dem Benutzer das Erstellen und Bearbeiten vordefinierter Berechnungen
Berichterstellung: Eingabesteuerelemente und Gruppen erstellen und bearbeiten	Ermöglicht dem Benutzer das Erstellen und Bearbeiten von Eingabesteuerelementen
Berichterstellung: Filter erstellen und bearbeiten und Eingabesteuerelemente nutzen	Ermöglicht es Benutzern, Berichtsfilter zu erstellen und zu bearbeiten und die Eingabesteuerelemente zu nutzen.
Berichterstellung: Sortierungen und Rangfolgen erstellen und bearbeiten	Ermöglicht dem Benutzer das Erstellen und Bearbeiten von Sortierungen und Rangfolgen
Berichterstellung: Formeln, Variablen, Gruppen und Referenzen erstellen	Ermöglicht dem Benutzer das Erstellen von Formeln, Variablen, Gruppen und Referenzen
Berichterstellung: Dokumentänderung aktivieren	Ermöglicht dem Benutzer, die Berichtsformatierung zu bearbeiten. Ohne dieses Zugriffsrecht ist der Entwurfsmodus nicht verfügbar.
Berichterstellung: Objekte zusammenführen	Ermöglicht dem Benutzer die Datensynchronisierung mithilfe von zusammengeführten Dimensionen in Berichten und im Datenmanager
Berichterstellung: Berichte, Tabellen, Diagramme und Zellen einfügen und entfernen	• Ermöglicht dem Benutzer, Berichte, Tabellen, Diagramme und Zellen einzufügen und zu entfernen • Aktiviert den Duplikate-Workflow (Kopieren/Einfügen)

31.3.11.5 Universe-Design-Tool

Recht	Beschreibung
Universumintegrität überprüfen	Ermöglicht dem Benutzer, die Integrität des Universums zu überprüfen
Strukturfenster regenerieren	Ermöglicht dem Benutzer, das Strukturfenster zu regenerieren
Tabellenliste verwenden	Ermöglicht dem Benutzer, mithilfe der Tabellenliste Datenbankdaten anzuzeigen
Universumseinschränkungen anwenden	Ermöglicht dem Benutzer, vordefinierte Universumseinschränkungen auf Benutzer eines importierten Universums anzuwenden
Universum verknüpfen	Ermöglicht dem Benutzer die Verknüpfung zweier Universen und die gemeinsame Verwendung von Komponenten
Verbindungen erstellen, ändern oder löschen	Ermöglicht dem Benutzer das Erstellen, Ändern und Löschen von Universumsverbindungen, die im Repository der BI-Plattform oder als persönliche bzw. freigegebene Verbindungen gespeichert sind
Einstellungen für Objekte des Benutzers ändern	Zeigt das Menü *Einstellungen* in einem Anwendungsobjekt an Ohne dieses Zugriffsrecht kann der Benutzer keine persönlichen Einstellungen in einer Anwendung vornehmen, und das Menü *Einstellungen* wird in den Anwendungen nicht angezeigt. Beispielsweise kann der Benutzer ohne dieses Recht nicht die Maßeinheit (Zoll oder Millimeter) für Berichte in der Web-Intelligence- oder BI-Launchpad-Anwendung auswählen.

31.3.11.6 Information-Design-Tool

Recht	Beschreibung
Sicherheitsprofile verwalten	Ermöglicht dem Benutzer, den Sicherheitseditor zu öffnen Zum Arbeiten mit Sicherheitsprofilen müssen Sie auch über Rechte für das Universum verfügen.

Recht	Beschreibung
Projekte freigeben	Ermöglicht dem Benutzer, ein lokales Projekt freizugeben und ein freigegebenes Projekt mit dem lokalen Projekt zu synchronisieren
Verbindungen erstellen, ändern oder löschen	• Ermöglicht dem Benutzer, gesicherte Verbindungen in der Ansicht "Veröffentlichte Ressourcen" zu erstellen oder zu löschen • Ermöglicht dem Benutzer, Verbindungen im Verbindungseditor zu bearbeiten • Ermöglicht dem Benutzer, Verbindungen in einem Repository zu veröffentlichen
Universum veröffentlichen	Ermöglicht dem Benutzer, Universen in einem Repository zu veröffentlichen
Universum abrufen	Ermöglicht dem Benutzer, veröffentlichte Universen in einem zu bearbeitenden lokalen Projekt abzurufen
Für alle Benutzer speichern	Ermöglicht dem Benutzer, beim Abrufen von Universen einen Speichervorgang für alle Benutzer auszuführen
Statistik berechnen	Ermöglicht dem Benutzer die Auswahl von Tabellen und Spalten für die Berechnung und Veröffentlichung von Statistiken
Einstellungen für Objekte des Benutzers ändern	Zeigt das Menü *Einstellungen* in einem Anwendungsobjekt an Ohne dieses Zugriffsrecht kann der Benutzer keine persönlichen Einstellungen in einer Anwendung vornehmen, und das Menü *Einstellungen* wird in den Anwendungen nicht angezeigt. Beispielsweise kann der Benutzer ohne dieses Recht nicht die Maßeinheit (Zoll oder Millimeter) für Berichte in der Web-Intelligence- oder BI-Launchpad-Anwendung auswählen.

31.3.11.7 Warnmeldungen

Recht	Beschreibung
Warnmeldungen auslösen	Ermöglicht dem Benutzer, Warnungsereignisse auszulösen Zum Auslösen einer Warnung für ein Dokument sind die folgenden zusätzlichen Rechte erforderlich: • Die Rechte "Anzeigen" und "Zeitgesteuert verarbeiten" für das Dokument • Die Rechte "Anzeigen" und "Auslösen" für das betreffende Ereignis

Recht	Beschreibung
Objekte abonnieren	Ermöglicht dem Benutzer, ein Warnungsereignis zu abonnieren. Zum Abonnieren eines Ereignisses sind die folgenden zusätzlichen Rechte erforderlich: • Das Recht "Anzeigen" für das betreffende Ereignis • Das Recht "Abonnieren" für das eigene Konto des Benutzers Zum Abonnieren einer Warnung in einem Dokument sind die folgenden zusätzlichen Rechte erforderlich: • 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
Einstellungen für Objekte des Benutzers ändern	Zeigt das Menü *Einstellungen* in einem Anwendungsobjekt an Ohne dieses Zugriffsrecht kann der Benutzer keine persönlichen Einstellungen in einer Anwendung vornehmen, und das Menü *Einstellungen* wird in den Anwendungen nicht angezeigt. Beispielsweise kann der Benutzer ohne dieses Recht nicht die Maßeinheit (Zoll oder Millimeter) für Berichte in der Web-Intelligence- oder BI-Launchpad-Anwendung auswählen.

31.3.11.8 SAP BusinessObjects Mobile

Recht	Beschreibung
Anmelden bei SAP BusinessObjects Mobile	Ermöglicht dem Benutzer, sich von der Mobile-Anwendung aus an der BI-Plattform anzumelden und Dokumente anzuzeigen
Dokumentwarnmeldungen abonnieren	Ermöglicht dem Benutzer, Warnmeldungen zu Dokumenten und wiederkehrenden Instanzen zu abonnieren Wenn einem Benutzer dieses Recht in der Vergangenheit gewährt wurde, kann er auch weiterhin abonnierte Warnmeldungen erhalten, selbst wenn er nicht mehr über das Recht verfügt. Der Benutzer muss das Abonnement ausdrücklich kündigen, wenn er die Warnmeldungen nicht mehr erhalten möchte.

Recht	Beschreibung
	Um Warnmeldungen zu Dokumenten und wiederkehrenden Instanzen für die zeitgesteuerte Verarbeitung abonnieren zu können, muss der Benutzer über den "vollen Zugriff" auf den Ordner `Systemereignisse`, der unter *Ereignisse* in der CMC zu finden ist, verfügen.
Dokumente im lokalen Gerätespeicher speichern	Ermöglicht dem Benutzer, Dokumente auf einem Mobilgerät zu speichern Wenn einem Benutzer das Recht "Dokumente im lokalen Gerätespeicher speichern" in der Vergangenheit gewährt wurde und er Dokumente auf dem Mobilgerät gespeichert hat, bleiben die Dokumente auf dem Mobilgerät erhalten (auch wenn das Recht nicht mehr besteht), aber werden bei der Synchronisation nicht mehr synchronisiert.
Dokumente vom Gerät per E-Mail senden	Ermöglicht dem Benutzer, Berichte mit einer E-Mail-Nachricht zu senden
Einstellungen für Objekte des Benutzers ändern	Zeigt das Menü *Einstellungen* in einem Anwendungsobjekt an Ohne dieses Zugriffsrecht kann der Benutzer keine persönlichen Einstellungen in einer Anwendung vornehmen, und das Menü *Einstellungen* wird in den Anwendungen nicht angezeigt. Beispielsweise kann der Benutzer ohne dieses Recht nicht die Maßeinheit (Zoll oder Millimeter) für Berichte in der Web-Intelligence- oder BI-Launchpad-Anwendung auswählen.

Weitere Informationen finden Sie im *Installations- und Implementierungshandbuch für SAP BusinessObjects Mobile*.

31.3.11.9 BI Admin Cockpit

Recht	Beschreibung
Zugang zu BI Admin Cockpit gewähren	Ermöglicht den Zugang zum BI Admin Cockpit in der CMC
Zugang zur Überwachung gewähren	Ermöglicht den Zugang zur Überwachung im BI Admin Cockpit
Zugang zu grafischem Vergleich gewähren	Ermöglicht den Zugang zum grafischen Vergleich im BI Admin Cockpit
Grafischer Vergleich - Vergleich erstellen	Ermöglicht das Erstellen neuer Vergleiche zwischen InfoObjects im Grafischen Vergleich

Recht	Beschreibung
Grafischer Vergleich - Vergleich löschen	Ermöglicht das Löschen vorheriger Vergleiche im Grafischen Vergleich
Grafischer Vergleich - Vergleich erneut ausführen	Ermöglicht es, vorherige Vergleiche im Grafischen Vergleich erneut auszuführen
Grafischer Vergleich - Vergleich anzeigen	Ermöglicht das Anzeigen eines Vergleichs im Grafischen Vergleich

32 Servereigenschaften (Anhang)

32.1 Über Servereigenschaften (Anhang)

In diesem Anhang zu Servereigenschaften werden Eigenschaften beschrieben, die für die einzelnen Server der BI-Plattform festgelegt werden können.

32.1.1 Allgemeine Servereigenschaften

Die in diesem Abschnitt beschriebenen Servereigenschaften gelten für alle Servertypen.

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. **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* ist standardmäßig auf **TRUE** festgelegt, und *Anforderungs-Port* hat keinen Eintrag.

Eigenschaft	Beschreibung	Standardwert
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**.

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**.

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.

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**.

Eigenschaft	Beschreibung	Standardwert
Klicken Sie auf \ {71}Konfigurationsvorlage festlegen\ {72}.	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**.

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`**.

32.1.2 Kerndienste-Eigenschaften

Die Kategorie "Kerndienste" umfasst die folgenden Server:

- Adaptive Job Server
- Adaptive Processing Server
- Central Management Server
- Event Server
- Input File Repository Server
- Output File Repository Server
- Web Application Container Server

Eigenschaften des Adaptive Job Servers

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

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

Eigenschaften des Adaptive Processing Servers

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

Eigenschaften des Proxydiensts für das Client-Auditing

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Eigenschaften des Sicherheitstokendiensts

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

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

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

Eigenschaften des Übersetzungsdiensts

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Eigenschaften des Überwachungsdiensts

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Eigenschaften des Plattformsuchdiensts

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

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.

Eigenschaften des Central Management Service

Eigenschaft	Beschreibung	Standardwert
Name Server-Port	Gibt den Port an, den der CMS auf anfängliche Namensdienstanforderungen überwacht.	6400

Eigenschaft	Beschreibung	Standardwert
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 versucht, weitere Verbindungen einzurichten, bis die angeforderte Anzahl von Verbindungen schließlich eingerichtet ist. Die Metrik *Eingerichtete Systemdatenbankverbindungen* des CMS zeigt die aktuelle Anzahl eingerichteter Verbindungen.	14
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** (wahr)

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

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

Eigenschaften des Input-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.	%DefaultInputFRSDir/%
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.	%DefaultInputFRS-Dir/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
Dateispeicherort des Virenprüfungsadapters	Gibt den absoluten Pfad für den Dateispeicherort des Virenprüfungsadapters an.	

Eigenschaften des Output File Repository Servers

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.	%DefaultOutputFRSDir/%

Eigenschaft	Beschreibung	Standardwert
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.	%DefaultOutputFRS-Dir/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 Web Application Container Servers

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

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). Die verfügbaren Menüoptionen sind: • *Nicht angegeben* • *Keine* • *Niedrig* • *Mittel* • *Hoch*	Nicht angegeben

Eigenschaften des Business-Process-BI-Dienstes

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Eigenschaften des Query-Builder-Dienstes

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

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

Eigenschaft	Beschreibung	Standardwert
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. 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.	Nicht ausgewählt
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.

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

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. • *COOKIE* wird verwendet, wenn der Anmeldenamen von einem Webbrowser-Cookie abgerufen wird. Domäne, Name, Wert und Pfad müssen in dem Cookie gespeichert sein.	**HTTP_HEADER**
Benutzernamensparameter	Mit dieser Beschriftung wird der vertrauenswürdige Benutzer zum Abrufen eines Anmeldetokens identifiziert.	**X-SAP-TRUSTED-USER**

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 Standarddomäne des Active Directorys wird verwendet, damit die Benutzer keine Domäne bei der Anmeldung angeben müssen. Zum Beispiel: falls die Standarddomäne auf „mydomain“ gesetzt ist und ein Benutzer sich mit dem Benutzernamen „user“ anmeldet, versucht die Anmeldungsstelle des Active Directorys, „user@mydomain.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 Keytab-Datei. Über eine Keytab-Datei können Kerberos-Filter so konfiguriert werden, dass das Kennwort des Benutzerkontos auf dem Webanwendungscomputer nicht offengelegt wird.	Leer

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-Authentifizierungsdienst verwendet einen Dienstprinzipalnamen, um einen Dienst zu authentifizieren.	Leer
Keytab-Datei	Der vollständige Pfad zu einer Keytab-Datei. Über eine Keytab-Datei können Kerberos-Filter so konfiguriert werden, dass das Kennwort des Benutzerkontos auf dem Webanwendungscomputer nicht offengelegt wird.	Leer

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** (wahr)
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

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** (wahr)
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`

Eigenschaft	Beschreibung	Standardwert
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 angegeben werden, wenn Sie *HTTP über Proxy aktivieren* auswählen.	Leer
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

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

Eigenschaft	Beschreibung	Standardwert
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 Zertifikatspeichers angegeben haben, sodass der WACS auf private Schlüssel aus dem Zertifikatspeicher zugreifen kann. Ein Wert kann nur angegeben werden, wenn Sie *HTTPS aktivieren* auswählen.	Leer
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

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.

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

32.1.3 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.

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.

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. ⓘ 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*.	**60**

Eigenschaft	Beschreibung	Standardwert
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**

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. **Hinweis** Hierfür muss die Eigenschaft *Protokollierungsebene* auf *Hoch* gesetzt werden.	Deaktiviert
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

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 Netzwerkschichten und Datenbanken werden unter *Konnektivitätsdienst-Metriken* angezeigt.	Nicht markiert
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

Eigenschaft	Beschreibung	Standardwert
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.

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.

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.

Hochstufverwaltungsdienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Hochstufverwaltung-ClearCase-Dienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Eigenschaften des grafischen Vergleichsdienstes

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Weitere Informationen

Allgemeine Servereigenschaften [Seite 499]

32.1.4 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 2020 Report Application Server
- Crystal Reports 2020 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.

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**.

Eigenschaft	Beschreibung	Standardwert
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**.
Zeitüberschreitung für Verbindungen 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 ist 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 ist 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. 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 beträgt 0 Sekunden.
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.

Eigenschaft	Beschreibung	Standardwert
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.

Crystal-Reports-Verarbeitungsdienst-Eigenschaften

Eigenschaft	Beschreibung	Standardwert
Zeitlimit für Auftrag im Leerlauf (Minuten)	Gibt an, wie viele Minuten der Crystal Reports Processing Server zwischen Anforderungen für einen bestimmten Auftrag wartet.	Der Standardwert ist 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 1000.
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**.

Eigenschaft	Beschreibung	Standardwert
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**.
Zeitüberschreitung für Verbindungen 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 ist 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 beträgt 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 beträgt 0.

Eigenschaft	Beschreibung	Standardwert
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 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
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

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.

Eigenschaften von Crystal Reports 2020 Report Application Server

Hinweis

Wenn Sie eine beliebige dieser Eigenschaften bearbeiten, muss der Server neu gestartet werden, damit die Änderungen wirksam werden.

Eigenschaften des Diensts zum Anzeigen und Ändern von Crystal-Reports-2020-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**.

Eigenschaft	Beschreibung	Standardwert
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.
Zeitüberschreitung für Verbindungen 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 Server unnötigerweise darauf, dass ein Auftrag im Leerlauf geschlossen wird).	Der Standardwert ist 30 Minuten.
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 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 20000 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 ist 20 Minuten.

Eigenschaft	Beschreibung	Standardwert
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`

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.

Eigenschaften des Crystal Reports 2020 Processing Servers

Hinweis

Wenn Sie eine beliebige dieser Eigenschaften bearbeiten, muss der Server neu gestartet werden, damit die Änderungen wirksam werden.

Eigenschaften des Crystal-Reports-2020-Verarbeitungsdienests

Eigenschaft	Beschreibung	Standardwert
Zeitlimit für Auftrag im Leerlauf (Minuten)	Gibt an, wie viele Minuten der Crystal Reports Processing Server zwischen Anforderungen für einen bestimmten Auftrag wartet.	Der Standardwert ist 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 1000.
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**.

Eigenschaft	Beschreibung	Standardwert
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**.
Zeitüberschreitung für Verbindungen 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 ist 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 beträgt 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 beträgt 0.

Eigenschaft	Beschreibung	Standardwert
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 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%/CrystalReports2020ProcessingServer/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 20000.

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.

32.1.5 Analysis Services-Eigenschaften

Die Analysis Services-Kategorie umfasst den Adaptive Processing Server:

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.

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.
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.

32.1.6 Eigenschaften des Datenföderations-Diensts

Die Datenföderations-Dienstekategorie umfasst den Adaptive Processing Server:

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.

32.1.7 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

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 Intelligence alle Hierarchiedaten ab, was sich auf die Leistung und Stabilität des Systems auswirken kann.	`-Dsap.sl.bics.expandToLevel=n` n kann jede Ganzzahl zwischen 0 und 99 sein. Falls n=0 oder falls dieser Parameter nicht angegeben wird, verwenden die Hierarchien nicht den Parameter "Bis Ebene aufklappen".

Eigenschaft	Beschreibung	Standardwert
Auswahloption zur Variablen-auswahl	Legt die Auswahloption für die Variablenauswahl fest. Wenn die Eigenschaft auf "Intervall" festgelegt wird, ist das Textfeld nicht verfügbar, und Benutzer können ausschließlich Start- und Endwerte in das Dialogfeld "Eingabeaufforderungen" eingeben. Wenn die Eigenschaft auf "Mehrfachwerte" gesetzt wird, ist das Textfeld "Geben Sie einen Wert ein" verfügbar, und Benutzer können Werte für BW-Auswahloptionsvariablen eingeben. **Hinweis** Diese Eigenschaft aktualisiert nicht lokale Installationen des Web-Intelligence-Rich-Client. Informationen zum Aktualisieren der lokalen Registrierung solcher Installationen finden Sie im Installationshandbuch für Web-Intelligence-Rich-Client.	`-Dsap.sl.bics.variableComplexSelectionMapping=n` , wobei n entweder ein Intervall oder ein Mehrfachwert sein kann. **Hinweis** Bei älteren Versionen als BI 4.1 SP05 ist der Standardwert für diese Option "Intervall". Wenn Sie diese Eigenschaft den Einstellungen des Adaptive Processing Server hinzufügen und sie auf "Mehrfachwert" setzen, müssen vorhandene Dokumente folgenden Aktionen unterzogen werden: • Ein Dokument muss bereinigt werden. • Die Standardwerte für Abfrage-eingabeaufforderungen müssen dahingehend geändert werden, dass sie mit der Mehrfachwert-Auswahl kompatibel sind.

Eigenschaften des Web-Intelligence-Überwachungsdienstes

Eigenschaft	Beschreibung	Standardwert
Überwachung aktivieren	Gibt an, ob die Überwachung für den Dienst aktiviert ist.	**TRUE** (wahr)
Verzögerung der Überwachungsthread-Schleife (Sekunden)	Gibt die Zeitspanne in Sekunden zwischen den Ping-Versuchen an, die der Dienst für Clients durchführt.	300
Standardzeitüberschreitung bei Bereinigung der 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
Standardzeitüberschreitung bei Austausch der 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** (wahr)

Eigenschaft	Beschreibung	Standardwert
Dienst-Aktivitätsüberwachung aktivieren		**TRUE** (wahr)

Eigenschaften des Visualisierungsdiensts

Eigenschaft	Beschreibung	Standardwert
Zeitüberschreitung 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
Zeitüberschreitung 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

Eigenschaften des Rebean-Diensts

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

Eigenschaften des Dokument-Wiederherstellungsdiensts

Eigenschaft	Beschreibung	Standardwert
Keine Konfigurationseigenschaften		

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.

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** (wahr)
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

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 *Maximale Anzahl der Dokumente vor dem Recycling* festgelegten Wert überschreitet.	1200
Zeitlimit 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 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 liegt zwischen 1 und 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

Eigenschaft	Beschreibung	Standardwert
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** (wahr)
Zeitüberschreitung für Verbindungen 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 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.	200 Der gültige Bereich liegt zwischen 5 und 65.535.
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** (wahr)
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** (wahr)

Eigenschaft	Beschreibung	Standardwert
Wiederholungsanzahl nach Ping-Fehler des APS-Service	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. **Hinweis** Diese Eigenschaft sollte nur zu Debugging-Zwecke bei der Behebung von Fehlern aktiviert werden. Ist während des normalen Betriebs auf **FALSE** eingestellt.	**FALSE** (falsch)

Eigenschaften des Web-Intelligence-Verarbeitungsdiensts

Eigenschaft	Beschreibung	Standardwert
Verwendung von HTTP-URL aktivieren	Legt fest, ob der Server auf remote gespeicherte Dateien zugreifen kann.	**TRUE** (wahr)
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

Eigenschaften des gemeinsamen Web-Intelligence-Diensts

Eigenschaft	Beschreibung	Standardwert
Cache-Zeitüberschreitung (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** (falsch)
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** (wahr)

Eigenschaft	Beschreibung	Standardwert
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** (wahr)
Maximale Größe des 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 4095 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 4095 MB.
Verzeichnis für Bilder	Gibt den Speicherort des Bildverzeichnisses an.	Leer
Ausgabe-Cache-Verzeichnis	Gibt den Speicherort des Caches an.	Leer

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 535]

32.1.7.1 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.

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. Jedem Benutzer ist maximal ein aktives Dokument gestattet anstatt `<Maximale Anzahl der Dokumente pro Benutzer>`.

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 lehnt neue Verbindungen und neue Client-Aufrufe ab. Für Web-Intelligence-Dokumente ist nur die Option *Speichern* zulässig. Benutzer, die eine Aktion anfordern, 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 schließen.
- Wenn während der Systembereinigung nicht genügend Arbeitsspeicher freigegeben werden konnte, beginnt der Server, Dokumente im *Bearbeitungsmodus* 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
  ```

  Der Server kann Dokumente nicht schließen, wenn ein Client-Aufruf ausgeführt wird. Jedes Dokument, das regeneriert oder in ein anderes Format exportiert oder für das irgendein zeitaufwändiger Vorgang ausgeführt wird, wird nicht geschlossen, wenn der Server diesen Grenzwert erreicht. Wenn der Server nicht genügend Speicher freigeben kann und immer noch der Wert `<Oberer Grenzwert für Arbeitsspeicher>` überschritten wird, startet der Server neu.

Maximaler Grenzwert für Arbeitsspeicher

Wenn <Maximaler Grenzwert für Arbeitsspeicher> erreicht wird, werden alle aktuellen Vorgänge abgebrochen. Alle Client-Aufrufe werden beendet. Sobald der Aufruf beendet ist, wird das entsprechende Dokument geschlossen.

33 Servermetrik (Anhang)

33.1 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

33.1.1 Allgemeine Servermetriken

Anhand der folgenden Metriken wird der Rechner beschrieben, auf dem der angegebene Server ausgeführt wird.

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.
Anzahl der Kerne	Zeigt die Anzahl der Prozessorkerne des Rechners an, auf dem der BI-Plattform-Server gehostet wird.
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.

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.
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.

Metrik	Beschreibung
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.

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.

Protokollierungsdienst-Metriken

Metrik	Beschreibung
Protokollierungsverzeichnis	Dieses Verzeichnis enthält die Protokolldateien für den Server .

33.1.2 Central Management Server-Metriken

In der folgenden Tabelle werden die Servermetriken beschrieben, die im Fenster *Metriken* für die Central Management Server angezeigt werden.

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.

Metrik	Beschreibung
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. 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.

Metrik	Beschreibung
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.
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.

Metrik	Beschreibung
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* (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.

33.1.3 Connection Server-Metriken

Die folgenden Metriken gelten speziell für den Connection Server.

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: • *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*.

33.1.4 Event Server-Metriken

In der folgenden Tabelle werden die Servermetriken beschrieben, die im Fenster *Metriken* für Event Server angezeigt werden.

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.

33.1.5 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.

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.
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.

33.1.6 Adaptive Processing Server-Metriken

In der folgenden Tabelle werden die Servermetriken beschrieben, die im Fenster *Metriken* für Adaptive Processing Server angezeigt werden.

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 der JVM zugeordneten Prozesse werden berücksichtigt. Ein Wert, der größer als 80 % ist, kann einen CPU-Engpass anzeigen.

Metrik	Beschreibung
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.
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.

Metrik	Beschreibung
Dienste	Eine kommagetrennte Liste der vom Server gehosteten Dienste.

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.activeOLAPConnection Count	Die Anzahl der derzeit offenen Verbindungen zwischen OLAP-Clients und dem Dienst.

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.

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.

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.

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).
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*.

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*.

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.
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.

BEx-Web-Applications-Dienstmetriken

Metrik	Beschreibung
Anzahl an Sitzungen	Die Gesamtzahl der Sitzungen, die in einem BEx-Web-Applications-Dienst aktiv sind.

33.1.7 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.

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.

Weitere Informationen

Adaptive Processing Server-Metriken [Seite 544]

33.1.8 Adaptive Job Server-Metriken

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.

Metrik	Beschreibung
Standardeinstellungen für 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 SFTP-Ziel gültig	*WAHR*, wenn der Server Dokumente an das im Fenster *Ziel* für den Server angegebene SFTP-Serverziel senden kann. Ansonsten *FALSCH*. Wenn der Fingerabdruck nicht genau mit dem SFTP-Server übereinstimmt, können Probleme auftreten.
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.

In der folgenden Tabelle werden die Metriken der einzelnen Dienste zur zeitgesteuerten Verarbeitung beschrieben, die auf dem Server ausgeführt werden.

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.

Metrik für untergeordnete Prozesse

Metrik	Beschreibung
Dienst zur zeitgesteuerten Verarbeitung	Der Name des untergeordneten Prozesses.
PID	Die ID des untergeordneten Prozesses.

Metrik	Beschreibung
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.
Komm.-Fehler	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*.

33.1.9 Crystal-Reports-Server-Metriken

Die folgende Tabelle enthält Beschreibungen der Servermetriken, die auf dem Bildschirm *Metriken* für den Crystal Reports Processing Server und den Crystal Reports 2020 Processing Server angezeigt werden.

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.

Metrik	Beschreibung
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.
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.

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.

Metrik	Beschreibung
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.
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 2020 Report Application Server angezeigt werden.

Crystal-Reports-2020-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.

Metrik	Beschreibung
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.

33.1.10 Web Intelligence Server-Metriken

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.

Metrik	Beschreibung
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.
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).

34 Server-Platzhalter

34.1 Server- und Knotenplatzhalter

Mit Ausnahme von *%SERVER_FRIENDLY_NAME%* und *%SERVER_NAME%* gelten diese Platzhalter für alle Server auf demselben Knoten.

> **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%*
> - *%IntroscopeAgentEnterpriseManagerPort%*
> - *%IntroscopeAgentEnterpriseManagerTransport%*
> - *%NCSInstrumentLevelThreshold%*
> - *%SMDAgentHost%*
> - *%SMDAgentPort%*

> **Achtung**
>
> Platzhalter, die nicht zur Bearbeitung vorgesehen sind, sollten in keiner Weise geändert werden. Der Systemadministrator muss sicherstellen, dass nur die richtige Person aus der Administratorgruppe (die für die Knotenverwaltung vorgesehen ist) über die Bearbeitungsrechte für den Knoten verfügt. Für alle anderen Benutzer, einschließlich anderer Mitglieder der Administratorgruppe, sollte die Anzeige/Verwaltung der Knotenobjekte durch Anwendung der entsprechenden Sicherheitsrechte eingeschränkt werden. Wenn einer der Platzhalterwerte versehentlich beschädigt wurde und der CMS nicht angezeigt wird, lesen Sie den folgenden SAP-Hinweis 3269127.

> **Hinweis**
>
> Im SAP-Knowledge-Base-Artikel 3278916 erfahren Sie, wie Sie einschränken können, dass Platzhalter verändert werden, um so mögliche schädliche Beeinträchtigungen der BI-Landschaft zu verhindern.

Platzhalter

Platzhalter	Beschreibung	Standardwerte
%AuditingDatabaseConnection%	Die vom CMS verwendete Audit-Datenbankverbindung.	Dieser Wert wird während der Installation festgelegt.

Platzhalter	Beschreibung	Standardwerte
%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`
%CONNECTIONSERVER_EXE%	Der Name der ausführbaren Datei für den 64-Bit-Connection Server.	Unter Windows: `ConnectionServer.exe`. Unter UNIX: `ConnectionServer`.
%CRCPP_BINDIR%	Das Verzeichnis, in dem sich die Server-Binärdateien von Crystal Reports C++ 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`.

Platzhalter	Beschreibung	Standardwerte
%CRCPP_DefaultWorkingDir%	Das Standard-Arbeitsverzeichnis für Crystal-Reports-C++-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 der Interpreter nach ausführbaren Dateien durchsucht.	Unter Windows: „Path“. Unter UNIX: „LD_LIBRARY_PATH“.
%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.

Platzhalter	Beschreibung	Standardwerte
%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/`.
%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`.

Platzhalter	Beschreibung	Standardwerte
%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“.
%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/`.

Platzhalter	Beschreibung	Standardwerte
%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 Instrumentationsdaten gesendet werden.	Dieser Wert wird während der Installation festgelegt.
%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.postoffice-hub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportHTTPS%	Die Klasse, der zum Senden der Instrumentationsdaten an den Introscope Agent Enterprise Manager über HTTPS verwendet wird.	com.wily.isengard.postoffice-hub.link.net.HttpTunnelingSocketFactory

Platzhalter	Beschreibung	Standardwerte
%IntroscopeAgentEnterpriseManagerTransportSSL%	Die Klasse, der zum Senden der Instrumentationsdaten an den Introscope Agent Enterprise Manager über SSL verwendet wird.	com.wily.isengard.postoffice-hub.link.net.SSLSocketFactory
%IntroscopeAgentEnterpriseManagerTransportTCP%	Die Klasse, der zum Senden der Instrumentationsdaten an den Introscope Agent Enterprise Manager über TCP verwendet wird.	com.wily.isengard.postoffice-hub.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`.
%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.

Platzhalter	Beschreibung	Standardwerte
%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 Enterprise 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 2020 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`.

Platzhalter	Beschreibung	Standardwerte
%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.
%SMDAgentHost%	Der Hostname des SMD Agent, 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.	$LD_PRELOAD$

Platzhalter	Beschreibung	Standardwerte
%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.	$LD_PRELOAD_ONCE$

Weitere Informationen

Anzeigen und Bearbeiten der Platzhalter eines Knotens [Seite 170]

35 Verwalten kryptografischer Schlüssel

35.1 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 566]
Erstellen eines neuen Kryptografieschlüssels [Seite 568]
Löschen eines Kryptografieschlüssels aus dem System [Seite 568]
Sperren eines Kryptografieschlüssels [Seite 569]
Anzeigen der einem Kryptografieschlüssel zugeordneten Objekte [Seite 568]
Kryptografieschlüssel als gefährdet markieren [Seite 569]

35.1.1 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

Status	Beschreibung
	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.
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.

35.1.2 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.

35.2 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.
   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.

35.3 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 569]
Status von Kryptografieschlüsseln [Seite 566]

35.4 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.

35.5 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 *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

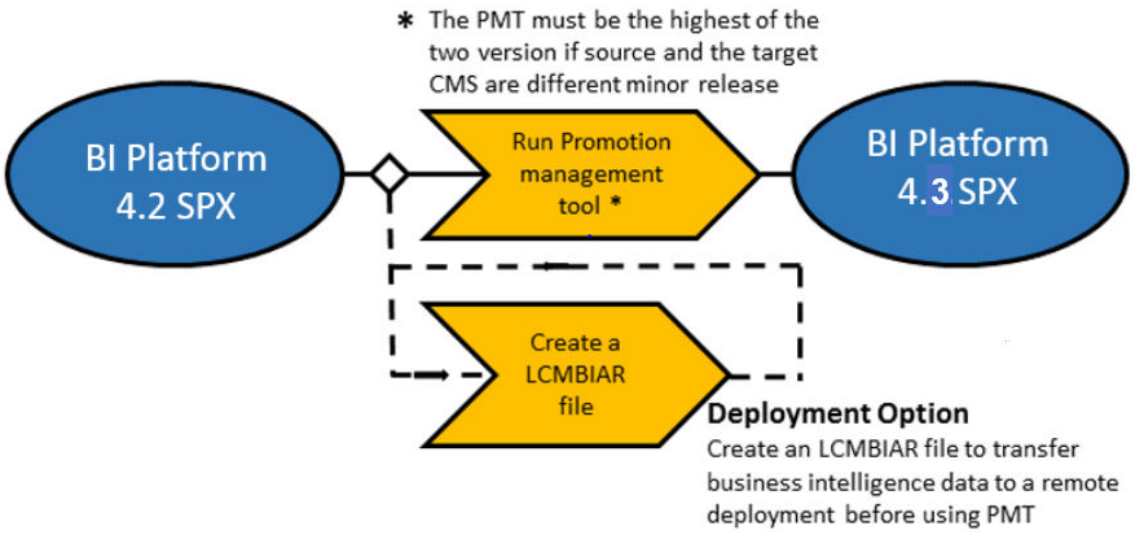
Sperren eines Kryptografieschlüssels [Seite 569]
Status von Kryptografieschlüsseln [Seite 566]
Anzeigen der einem Kryptografieschlüssel zugeordneten Objekte [Seite 568]

36 Hochstufverwaltung

36.1 Hochstufverwaltung

36.1.1 Herzlich willkommen bei der Hochstufverwaltung

36.1.1.1 Übersicht



Mit der Hochstufverwaltung können Sie Folgendes tun:

- BI-Ressourcen (Business Intelligence) aus einem Repository in ein anderes verschieben oder transportieren.
- Abhängigkeiten der Ressourcen verwalten.
- Den letzten Stand der hochgestuften Ressourcen im Zielsystem bei Bedarf wieder herstellen.

Außerdem unterstützt die Hochstufverwaltung 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.

36.1.1.2 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.
- *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.

36.1.1.3 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
   - 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.

36.1.1.4 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=<p
ath>\krb5.ini
```

> → Nicht vergessen
>
> Geben Sie den korrekten Pfad zu `bsclogin.conf` und `krb5.ini` in Ihrer Implementierung an.

36.1.2 Erste Schritte mit der Hochstufverwaltung

36.1.2.1 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.

36.1.2.2 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 die Erstellung 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 oder Ordners.
	Ermöglicht das Regenerieren der Startseite, um eine aktualisierte Liste der Aufträge und Ordner abzurufen.
Eigenschaften	Ermöglicht das Ändern der Eigenschaften für einen ausgewählten Auftrag. Sie können Titel, Beschreibung und Schlüsselwörter des ausgewählten Auftrags ändern.

Option	Beschreibung
Änderungsverlauf	Ermöglicht die Anzeige des Verlaufs des ausgewählten Auftrags.
Neuer Auftrag	Ermöglicht die Erstellung eines neuen Auftrags.
Importieren	Ermöglicht den Import von BIAR-, LCMBIAR- oder Überschreibungsdateien.
Bearbeiten	Ermöglicht die Bearbeitung 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.
1	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 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.

36.1.2.3 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:

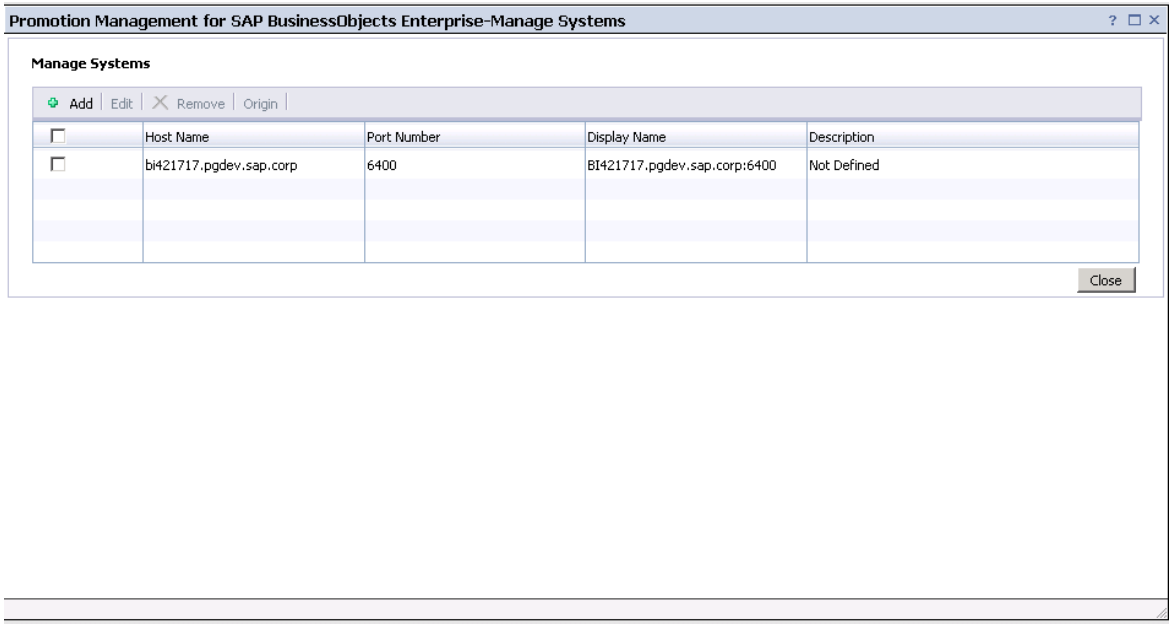
- *Systeme verwalten* – Diese Option ermöglicht das Hinzufügen aller für Hochstufverwaltungsaktivitäten erforderlichen Systeme.
- *Rollback-Einstellungen* – Diese Option ermöglicht die Auswahl eines Systems, für das Rollbacks aktiviert sind.
- *Auftragseinstellungen* – Diese Option ermöglicht das Anzeigen 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.

36.1.2.3.1 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.

   > **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 577]
Verwenden der Option "Auftragseinstellungen" [Seite 578]

36.1.2.3.2 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 578]

36.1.2.3.3 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:

- *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

Apache Subversion als Versionsverwaltungssystem verwenden [Seite 666]

36.1.2.3.4 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 Quellsystem jeglicher Verbindungsinformationen.
- *Zentrale Hochstufverwaltung*: Das System, über das die Hochstufverwaltung ausgeführt wird.
- *Ziel*: Das Endsystem, in das die BI-Ressourcen hochgestuft werden.

36.1.2.3.4.1 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 576].

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. Wählen Sie im Bereich *Ursprung* das gewünschte Quellsystem aus dem Dropdown-Menü aus.

   > ⓘ Hinweis
   >
   > Über die Option *Neues System* können Sie sich auch an einem neuen System anmelden. Um ein neues System als Quellsystem zu wählen, führen Sie Folgendes aus:
   > 1. Wählen Sie im Dropdown-Menü die Option *Neues System* aus.
   > Das Dialogfeld Origin Login (Ursprungsanmeldung) wird angezeigt.
   > 2. Geben Sie die gültigen Anmeldedaten in die Felder *System*, *Benutzername*, *Kennwort* und *Authentifizierung* ein.
   > 3. Wählen Sie *Log On* (Anmelden) aus.
3. Wählen Sie *Login* (Anmeldung).
4. Wählen Sie *Scan Now* (Jetzt scannen).

   Der Scan-Vorgang wird gestartet. Die *Liste der eindeutigen Verbindungen* wird angezeigt.

   > ⓘ Hinweis
   >
   > Um einen wiederholten Scan-Vorgang einzuplanen, wählen Sie *Wiederholungseinstellungen*.

5. Wählen Sie aus der Liste der Überschreibungen diejenigen Überschreibungen aus, die Sie hochstufen möchten, indem Sie die entsprechenden Kontrollkästchen aktivieren.

> **ⓘ Hinweis**
>
> Sie können in der Liste anhand von Schlüsselwörtern (Name der Überschreibung, Datum der letzten Aktualisierung usw.) nach bestimmten Überschreibungen suchen.
>
> Sie können Überschreibungen auch nach den folgenden Parametern filtern: Alle, Verbindung, Qwaas, Crystal Report.
>
> Darüber hinaus können Sie die Überschreibungen alphabetisch sortieren.

6. Wählen Sie im Bereich *Ziel* das gewünschte Zielsystem aus dem Dropdown-Menü aus. Sie können mehrere Zielsysteme angeben.

> **ⓘ Hinweis**
>
> Über die Option *Neues System* können Sie sich auch an einem neuen System anmelden. Um ein neues System als Zielsystem zu wählen, führen Sie Folgendes aus:
>
> 1. Wählen Sie im Dropdown-Menü die Option *Neues System* aus.
> Das Dialogfeld Destination Login (Zielanmeldung) wird angezeigt.
> 2. Geben Sie die gültigen Anmeldedaten in die Felder *System*, *Benutzername*, *Kennwort* und *Authentifizierung* ein.
> 3. Wählen Sie *Log On* (Anmelden) aus.

Um die Überschreibungen als LCMBIAR-Datei zu exportieren, führen Sie Folgendes aus:

1. Wählen Sie im Dropdown-Menü Export to LCMBIAR File (In LCMBIAR-Datei exportieren).
2. Wählen Sie *Exportieren*.
 Das Dialogfeld *Exporteinstellungen* wird angezeigt.
3. Geben Sie in den entsprechenden Feldern die gültigen Anmeldedaten ein.
4. Wählen Sie *Fertig*.

7. Wählen Sie *Hochstufen*.

Das Dialogfeld Multiple Destination Overrides (Mehrere Zielüberschreibungen) wird angezeigt.

> **ⓘ Hinweis**
>
> Standardmäßig werden alle Zielsysteme ausgewählt, an denen Sie zurzeit angemeldet sind. Sie können Überschreibungen selektiv für ein bestimmtes Zielsystem hochstufen, indem Sie das zu diesem gehörige Kontrollkästchen aktivieren.

8. Wählen Sie *Fertig*.

Die Hochstufung der Überschreibungen ist abgeschlossen.

9. 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".

10. Wählen Sie *Aktualisieren* für die Objekte, die Sie bearbeiten möchten.

Das Dialogfeld *Allgemeine Verbindungseigenschaften bearbeiten* wird angezeigt.

11. Überschreiben Sie die entsprechenden Werte, und klicken Sie dann auf *Fertig*.

Die bearbeiteten Objekte erhalten den Status „Aktiv“.

> **Hinweis**
>
> Sie können eine Verbindung auch aktivieren, indem Sie *Inaktiv* wählen, ohne die Verbindung im Zielsystem bearbeiten zu müssen.

12. Wählen Sie *Speichern*.

36.1.2.3.4.2 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 576].

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.

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*.

36.1.2.3.4.3 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 576].

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*.
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*.

36.1.2.3.5 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 642] finden Sie weitere

Informationen zum Verwenden der Option "CTS-Einstellungen" und zum Einrichten des CTS für den Einsatz mit der Hochstufverwaltung.

36.1.3 Verwenden der Hochstufverwaltung

Wenn Sie sich bei der Hochstufverwaltung anmelden, wird standardmäßig die Seite *Hochstufungsaufträge* angezeigt.

> **Hinweis**
>
> Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

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.

36.1.3.1 Erstellen und Löschen von Ordnern

In diesem Abschnitt wird beschrieben, wie Ordner auf der Hochstufungsaufträge-Startseite erstellt und gelöscht werden.

> ⓘ Hinweis
>
> Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

36.1.3.1.1 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 586]
Löschen eines Ordners [Seite 585]

36.1.3.1.2 Löschen eines Ordners

In diesem Abschnitt wird das Löschen von Ordnern beschrieben.

> ⓘ Hinweis
>
> Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

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 586]

36.1.3.2 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:

> **Hinweis**
>
> Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

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.

Feld	Beschreibung
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.

   > **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 579]

36.1.3.2.1 Anmelden an einem neuen CMS

In diesem Abschnitt wird die Anmeldung bei einem neuen CMS beschrieben.

> **Hinweis**
>
> Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

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 586].
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*.

Weitere Informationen

Bearbeiten von Aufträgen [Seite 590]
Hinzufügen eines InfoObjects zu einem Auftrag [Seite 591]
Aufträge mit verbundenen Repositorys hochstufen [Seite 594]
Zeitsteuern von Auftragshochstufungen [Seite 600]

36.1.3.3 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.

> ⓘ Hinweis
>
> Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

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 591]
Bearbeiten von Aufträgen [Seite 590]
Aufträge mit verbundenen Repositorys hochstufen [Seite 594]

36.1.3.4 Suchen nach Aufträgen

Mit der Suchfunktion der Hochstufverwaltung können Sie einen Auftrag im Repository suchen.

> ⓘ Hinweis
>
> Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

Zum Suchen eines Auftrags führen Sie die folgenden Schritte aus:

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 591]
Bearbeiten von Aufträgen [Seite 590]

36.1.3.5 Bearbeiten von Aufträgen

In diesem Abschnitt wird das Bearbeiten von Aufträgen beschrieben.

> ⓘ Hinweis
>
> - Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.
> - 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 591]
Aufträge mit verbundenen Repositorys hochstufen [Seite 594]
Zeitsteuern von Auftragshochstufungen [Seite 600]

36.1.3.6 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.
> - Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

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 586] und Bearbeiten von Aufträgen [Seite 590].
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 und 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.

Weitere Informationen

Verwalten der Abhängigkeiten eines Auftrags [Seite 592]
Aufträge mit verbundenen Repositorys hochstufen [Seite 594]
Zeitsteuern von Auftragshochstufungen [Seite 600]

36.1.3.7 Verwalten der Abhängigkeiten eines Auftrags

In diesem Abschnitt wird die Verwaltung von abhängigen Objekten eines InfoObjects beschrieben.

> **Hinweis**
>
> Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

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 586] und Bearbeiten von Aufträgen [Seite 590].
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 593].

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.

> ⓘ Hinweis
>
> Wenn Sie einen Ordner zum Hochstufen auswählen, wird der Inhalt des ausgewählten Ordners als Primärressource betrachtet.

Weitere Informationen

Aufträge mit verbundenen Repositorys hochstufen [Seite 594]

36.1.3.8 Suchen nach abhängigen Objekten

Mit der erweiterten Suchfunktion in der Hochstufverwaltung können Sie die von InfoObjects abhängigen Objekte im Repository suchen.

> ⓘ Hinweis
>
> Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

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 592]

36.1.3.9 Aufträge mit verbundenen Repositorys hochstufen

In diesem Abschnitt wird die Hochstufung von Aufträgen vom Quellsystem in das Zielsystem beschrieben, wenn beide Systeme live sind.

> **Hinweis**
>
> Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

Die folgende Tabelle enthält die InfoObject-Typen, die mithilfe der Hochstufverwaltung hochgestuft werden können:

Kategorie	Objekttypen, die hochgestuft werden können
Berichte	Crystal-Reports-Berichte, Web Intelligence, QaaWS, Lumira
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, Sätze	Universen (UNV), Verbindungen, Sätze
EPM-Dashboard	Universen, Verbindungen, Berichte und Analysen
BusinessView	DataFoundation
Föderation • Replikationsliste • Replikationsaufträge	Die Replikationsliste stuft folgende Objekte hoch: Flash, .txt, Diskussionen, .pdf, Hyperlink, .xls, Objektpaket, Crystal-Reports-Berichte, Web-Intelligence-Dokumente, Universen, Programm, Verbindungen, Datagrundlage, 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, DSL Universe (UNX), Business Layer (BLX), Connection (CNX), Datengrundlage (DFX), WEBI, Data Federator, Data Steward, BI-Arbeitsbereich usw.
Tenants	Das Promotion Management unterstützt das Hochstufen von Tenants zusammen mit dessen Abhängigkeiten vom Quell- in das Zielsystem, indem Optionen zum Auswählen und Hinzufügen von Tenants und der zugehörigen Tenant-Objekte zu einem Auftrag bereitgestellt werden. Darüber hinaus stellt es Beziehungen zwischen den Tenants und den zugehörigen Tenant-Objekten in Form von Abhängigkeiten her. Die Funktion lässt sich sowohl im GUI- als auch im CLI-Modus der Hochstufverwaltung ausführen.

BI-Kommentar wird von der Hochstufverwaltung unterstützt. Wenn Sie ein Dokument mit Kommentaren hochstufen, werden jegliche Kommentare zu dem Dokument ebenfalls vom Quell- in das Zielsystem migriert

(Live-zu-Live, Live-zu-BIAR, BIAR-zu-Live). Um ein Dokument mit Kommentaren hochzustufen, wählen Sie *Hochstufen* > *Kommentareinstellungen* und aktivieren dann das Kontrollkästchen *Kommentare einschließen*.

> **Hinweis**
>
> Standardmäßig ist das Kontrollkästchen *Kommentare einschließen* nicht aktiviert.

Beim Hochstufen von replizierten Objekte werden die replikationsspezifischen Informationen der zugehörigen Objekte ebenfalls vom Quell- in das Zielsystem hochgestuft (Live-in-Live, Live-in-BIAR, BIAR-in-Live).
Um Dokumente ohne replikationsspezifische Informationen hochzustufen, wählen Sie *Hochstufen* > *Förderationsjob-Einstellungen*, und deaktivieren Sie das Kontrollkästchen *Beziehung von Förderationsjobs einschließen*.

> **Hinweis**
>
> Das Kontrollkästchen *Kommentare einschließen* ist standardmäßig aktiviert.

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 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.
   - *Sicherheit auf oberster Ebene hochstufen* – Verwenden Sie diese Option, um die Sicherheitsberechtigungen der obersten Ebene hochzustufen.

> **⚠ Achtung**
>
> Mit der Option *Sicherheit auf oberster Ebene hochstufen* werden die Sicherheitsberechtigungen der obersten Ebene im Zielsystem überschrieben.

Sie können auch auf *Sicherheit anzeigen* klicken, um die Sicherheitsabhängigkeiten der InfoObjects im Auftrag anzuzeigen.

> **ⓘ Hinweis**
>
> Die Schaltfläche *Rechte anzeigen* ist deaktiviert, bis Sie den neuen Auftrag gespeichert haben.

6. Wählen Sie *Speichern*.

   Die Schaltfläche *Rechte anzeigen* ist aktiviert. Sie können nun die Sicherheitsabhängigkeiten anzeigen.
7. 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.
8. Klicken Sie auf *Zeitgesteuerte Verarbeitung*, wenn die Hochstufung zu einem bestimmten Zeitpunkt oder regelmäßig ausgeführt werden soll.
9. 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.

36.1.3.10 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 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
>
> - Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.
> - Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

Weitere Informationen

Exportieren eines Auftrags in eine LCMBIAR-Datei [Seite 597]
Importieren eines Auftrags aus einer LCMBIAR-Datei [Seite 598]

36.1.3.10.1 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 586]
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* oder *SFTP*, um die LCMBIAR-Datei auf einen FTP- bzw. SFTP-Server zu exportieren. Geben Sie Hostnamen, Port, Benutzernamen, Kennwort, Verzeichnis und Dateinamen ein, und wählen Sie dann *Exportieren*.

> **Hinweis**
>
> Wenn Sie *SFTP* als *LCMBIAR-Dateiziel* wählen, müssen Sie zusätzlich den SFTP-Fingerabdruck eingeben.

10. Wählen Sie in der Dropdownliste *Ziel* die Option *Ausgabe in LCMBIAR-Datei*, und klicken Sie auf *LCMBIAR-Dateiziel*.

Sie können den Export eines Auftrags in eine LCMBIAR-Datei zeitsteuern. Weitere Informationen hierzu finden Sie im Abschnitt Zeitsteuern von Auftragshochstufungen [Seite 600].

Weitere Informationen

Hinzufügen eines InfoObjects zu einem Auftrag [Seite 591]
Verwalten der Abhängigkeiten eines Auftrags [Seite 592]

36.1.3.10.2 Importieren eines Auftrags aus einer LCMBIAR-Datei

Sie können Aufträge aus einer LCMBIAR-Datei importieren. Die LCMBIAR-Datei wird vom Speichermedium in das Zielsystem kopiert.

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- oder SFTP-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*
  2. Geben Sie die entsprechenden Informationen in die Felder "Host", "Port", "Benutzername", "Kennwort", "Verzeichnis" und "Dateiname" ein und klicken auf *OK*.
- Zum Importieren einer LCMBIAR-Datei von einem SFTP-Server führen Sie die folgenden Schritte aus:
  1. Wählen Sie *SFTP*.
  2. Geben Sie die entsprechenden Informationen in die Felder "Host", "Port", "Benutzername", "Kennwort", "Verzeichnis", "Fingerabdruck" und "Dateiname" ein, und klicken Sie auf *OK*.

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.

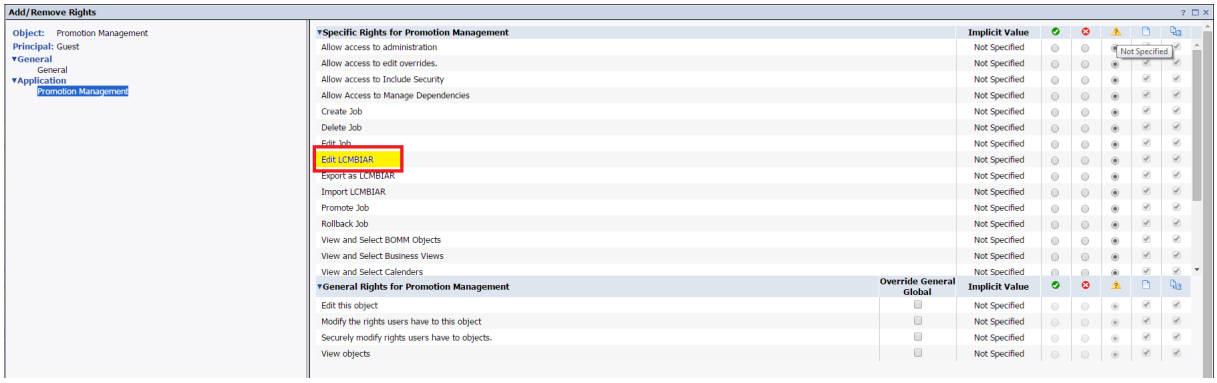
   Sie können auch auf die Option *Probeweise hochstufen* klicken, um die hochzustufenden Objekte und den Hochstufungsstatus anzuzeigen.
7. **Optional:** Wenn Sie ein Web-Intelligence-Dokument mit Anpassungen importieren, aktivieren Sie auf der Registerkarte *Benutzergruppen-BI-Einstellungen* die Option *Benutzergruppen-BI-Einstellungen überschreiben*, um die Anpassungen zu importieren.

Weitere Informationen

Verwalten der Abhängigkeiten eines Auftrags [Seite 592]

36.1.3.10.2.1 Selektives Abrufen von Objekten aus einer LCMBIAR-Datei

Um Objekte aus einer LCMBIAR-Datei selektiv abzurufen, muss der Benutzer über die Berechtigung *LCMBIAR bearbeiten* verfügen.



Um Objekte aus einer LCMBIAR-Datei selektiv abzurufen, führen Sie Folgendes aus:

1. Wählen Sie die hochzustufenden Objekte aus.
2. Klicken Sie auf *Hochstufen*.

> ⓘ Hinweis
>
> - Es wird ein neuer Auftrag mit den ausgewählten Objekten erstellt.
> - Der gleiche Vorgang kann mit dem Befehlszeilentool ausgeführt werden. Weitere Informationen finden Sie unter Befehlszeilentool-Parameter [Seite 613]
> - Eine selektive Hochstufung wird für Live-zu-Live-Szenarios nicht unterstützt.

36.1.3.11 Zeitsteuern von Auftragshochstufungen

In diesem Abschnitt wird die zeitgesteuerte Verarbeitung der Hochstufung eines Auftrags beschrieben. Außerdem wird die Eingabe von Wiederholungsoptionen und Parametern erläutert.

> ⓘ Hinweis
>
> Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

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. Dies gilt jedoch nicht, wenn Sie versuchen, eine Auftragshochstufung mit einer LCMBIAR-Datei einzuplanen, da LCMBIAR nicht als 'echtes' Ziel betrachtet wird.

> → 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".

Weitere Informationen

Exportieren eines Auftrags in eine LCMBIAR-Datei [Seite 597]

36.1.3.11.1 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 602]

36.1.3.12 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

> **Hinweis**
>
> Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

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.

36.1.3.13 Rollback für Aufträge ausführen

Mit der Option "Rollback" können Sie das Zielsystem nach der Hochstufung eines Auftrags wieder in seinen vorherigen Status zurückversetzen.

> **Hinweis**
>
> Sicherheitserweiterungen werden im Hochstufverwaltungstool implementiert, was zu Änderungen an bestimmten Verhaltensweisen beim Ausführen von Aktionen führt. Weitere Informationen finden Sie unter 3350454.

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.

36.1.3.13.1 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

Mehrere Versionen von BI-Ressourcen verwalten [Seite 664]

36.1.3.13.2 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*.
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 604]
Verwenden der Option "Teilrollback" [Seite 603]

36.1.3.13.2.1 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.

Weitere Informationen

Rollback für Aufträge ausführen [Seite 602]
Verwenden der Option "Teilrollback" [Seite 603]
Rollback von Aufträgen nach Ablauf des Kennworts ausführen [Seite 604]

36.1.4 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.

36.1.4.1 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.
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 durch Hinzufügen des Parameters `-javaargs Xmx3g`. Weitere Informationen finden Sie im SAP-Hinweis 2286419.

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.

36.1.4.2 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.

    > ⓘ 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.

36.1.5 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. Weitere Informationen zur Hochstufung mehrerer Objekte finden Sie in SAP-Knowledge-Base-Artikel 1969259.

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 [Seite 612].

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
LCM_password=<AdministratorPassword>
Destination_CMS=<TargetSystem>
Destination_userName=Administrator
Destination_password=<AdministratorPassword>
exportDependencies=false
includeSecurity=true
stacktrace=true
```

```
consolelog=true
```

36.1.5.1 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
   ```

36.1.5.2 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
- 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
```

36.1.5.3 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')")
   ```

   Wenn Sie denselben Job erneut ausführen, schließen Sie den LCM-Job mittels der folgenden Abfrage aus:

   ```
   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)") and SI_KIND not in
   ('LCMJob')
   ```

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“.

36.1.5.4 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.

36.1.6 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

36.1.6.1 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.

Die Datei muss das Format `<Dateiname>.properties` haben

Zum Beispiel: `<MeineEigenschaften.properties>`

36.1.6.2 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.

36.1.6.3 Befehlszeilenparameter

Die Befehlszeilenparameter für die Befehlszeilenoption der Hochstufverwaltung sind in folgende drei Hochstufungsarten unterteilt:

- Hochstufen von Objekten aus einer LCMBIAR-Datei zu einem Live-CMS
- Hochstufen von Objekte von einem Quell-CMS (Live) zu einem Ziel-CMS (Live)
- Exportieren von Objekten von einem Live-CMS in eine LCMBIAR-Datei

Zusätzlich zu den drei speziell für die Hochstufung bestimmten Parametern stehen Ihnen weitere Parameter für allgemeine Befehle zur Verfügung, die in sämtlichen Hochstufungsvorgängen verwendet werden können.

→ Nicht vergessen

Befehlszeilenparameter dürfen nicht in Anführungszeichen gesetzt werden.

ⓘ 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_<USER>_<Timestamp>` 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.

Weitere Informationen

LCMBIAR-Datei auf einen Live-CMS [Seite 618]
Quell-CMS (Live) zu Ziel-CMS (Live) [Seite 624]
Live-CMS in LCMBIAR-Datei [Seite 621]
Befehlszeilenparameter – Übersicht [Seite 628]

36.1.6.3.1 Befehlszeilenparameter nach Hochstufungsszenario

Die Befehlszeilenparameter werden in der vorgeschlagenen Reihenfolge, sortiert nach Hochstufungsszenario, aufgeführt. Die Tabelle enthält alle verfügbaren Parameter und deren Voraussetzung für das jeweilige Hochstufungsszenario (Obligatorisch oder Optional). Jeder obligatorische Parameter wird für das entsprechende Hochstufungsszenario beschrieben. Die optionalen Parameter werden im Bereich "Befehlszeilenparameter – Übersicht" beschrieben. Weitere Informationen zu allen szenariobedingten Parametern sowie eine Übersicht aller verfügbaren Parameter finden Sie unter "Zugehörige Links".

Parametergruppe	Parameter	LCMBIAR zu Live	Live zu LCMBIAR	Live zu Live	Rollback
Eigenschaftendatei	`lcmproperty`	Optional	Empfohlen	Empfohlen	Empfohlen
Vorgangsart	`action`	Obligatorisch action=promote	Obligatorisch action=export	Obligatorisch action=promote	Obligatorisch action=rollback

Parametergruppe	Parameter	LCMBIAR zu Live	Live zu LCMBIAR	Live zu Live	Rollback
LCM-Knoten	`LCM_CMS`	Obligatorisch			
	`LCM_userName`	Obligatorisch			
	`LCM_Password`	Obligatorisch Erforderlich in der Konsole, falls leer.			
	`LCM_authentication`	Optional: Standardmäßig = `secEnterprise`			
	`LCM_SystemID`	Obligatorisch nur für die SAP-Authentifizierung.			
	`LCM_ClientID`	Obligatorisch nur für die SAP-Authentifizierung.			
Quelle (Live oder LCMBIAR)	`importLocation`	Obligatorisch	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
	`lcmbiarpassword`	Obligatorisch (kann leer sein)	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
	`Source_CMS`	Nicht anwendbar	Obligatorisch	Obligatorisch	Nicht anwendbar
	`Source_UserName`	Nicht anwendbar	Obligatorisch	Obligatorisch	Nicht anwendbar
	`Source_password`	Nicht anwendbar	Obligatorisch Erforderlich in der Konsole, falls leer.	Obligatorisch Erforderlich in der Konsole, falls leer.	Nicht anwendbar
	`Source_authentication`	Nicht anwendbar	Optional Standardmäßig = `secEnterprise`	Optional Standardmäßig = `secEnterprise`	Nicht anwendbar
	`Source_systemID`	Nicht anwendbar	Obligatorisch nur für die SAP-Authentifizierung.	Obligatorisch nur für die SAP-Authentifizierung.	Nicht anwendbar
	`Source_clientID`	Nicht anwendbar	Obligatorisch nur für die SAP-Authentifizierung.	Obligatorisch nur für die SAP-Authentifizierung.	Nicht anwendbar
Ziel (Live oder LCMBIAR)	`Destination_CMS`	Obligatorisch	Nicht anwendbar	Obligatorisch	Nicht anwendbar
	`Destination_username`	Obligatorisch	Nicht anwendbar	Obligatorisch	Nicht anwendbar

Parametergruppe	Parameter	LCMBIAR zu Live	Live zu LCMBIAR	Live zu Live	Rollback
	`Destination_password`	Obligatorisch	Nicht anwendbar	Obligatorisch	Nicht anwendbar
	`Destination_authentication`	Optional Standardmäßig = `secEnterprise`	Nicht anwendbar	Optional Standardmäßig = `secEnterprise`	Nicht anwendbar
	`Destination_systemID`	Obligatorisch nur für die SAP-Authentifizierung.	Nicht anwendbar	Obligatorisch nur für die SAP-Authentifizierung.	Nicht anwendbar
	`Destination_clientID`	Obligatorisch nur für die SAP-Authentifizierung.	Nicht anwendbar	Obligatorisch nur für die SAP-Authentifizierung.	Nicht anwendbar
	`ExportLocation`	Nicht anwendbar	Obligatorisch	Nicht anwendbar	Nicht anwendbar
	`lcmbiarpassword`	Nicht anwendbar	Obligatorisch (kann leer sein)	Nicht anwendbar	Nicht anwendbar
Auftrag	`JOB_CUID`	Nicht anwendbar	Optional	Optional	Obligatorisch
	`Override`	Optional	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
	`forceOverride` Verfügbar in SP4	Optional	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
	`Timeout` Verfügbar in SP4	Optional	Nicht anwendbar	Optional	Nicht anwendbar
Export	`ExportDependencies`	Nicht anwendbar	Optional Standardmäßig = `False`	Optional Standardmäßig = `False`	Nicht anwendbar
	`ExportQuery`	Nicht anwendbar	Obligatorisch	Obligatorisch	Nicht anwendbar
	`ExportQueriesTotal`	Nicht anwendbar	Optional: Verwenden Sie diesen Parameter, wenn Sie über mehr als eine Exportabfrage verfügen.	Optional: Verwenden Sie diesen Parameter, wenn Sie über mehr als eine Exportabfrage verfügen.	Nicht anwendbar

Parametergruppe	Parameter	LCMBIAR zu Live	Live zu LCMBIAR	Live zu Live	Rollback
	`BatchJobQuery`	Nicht anwendbar	Optional: In Verbindung mit ExportQuery verwenden.	Optional: In Verbindung mit ExportQuery verwenden.	Nicht anwendbar
	`LimitQueryBatchSize`	Nicht anwendbar	Optional	Optional	Nicht anwendbar
Protokollierung	`Consolelog`	Optional Standardmäßig = `False`	Optional Standardmäßig = `False`	Optional Standardmäßig = `False`	Nicht anwendbar
	`ResultFileName`	Optional	Optional	Optional	Nicht anwendbar
	`LogFileName` Verfügbar in SP4	Optional	Optional	Optional	Nicht anwendbar
Objektauswahl	`Selected_CUIDS`	Optional	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
	`selectUser` Verfügbar in SP4	Nicht anwendbar	Optional Standardmäßig = `All`	Optional Standardmäßig = `All`	Nicht anwendbar
	`selectGroup` Verfügbar in SP4	Nicht anwendbar	Optional Standardmäßig = `All`	Optional Standardmäßig = `All`	Nicht anwendbar
Sicherheit	`IncludeApplicationSecurity`	Optional Standardmäßig = `False`	Optional Standardmäßig = `False`	Optional Standardmäßig = `False`	Nicht anwendbar
	`IncludeSecurity`	Optional Standardmäßig = `False`	Optional Standardmäßig = `False`	Optional Standardmäßig = `False`	Nicht anwendbar
	`IncludeTopLevelSecurity`	Optional Standardmäßig = `False`	Optional Standardmäßig = `False`	Optional Standardmäßig = `False`	Nicht anwendbar
Kommentare	`IncludeComments`	Optional Standardmäßig = `False`	Optional Standardmäßig = `False`	Optional Standardmäßig = `False`	Nicht anwendbar

Parametergruppe	Parameter	LCMBIAR zu Live	Live zu LCMBIAR	Live zu Live	Rollback
Föderationsjobs	`IncludeFederationJobsRelationship`	Optional Standardmäßig = `True`	Nicht anwendbar	Optional Standardmäßig = `True`	Nicht anwendbar

Weitere Informationen

LCMBIAR-Datei auf einen Live-CMS [Seite 618]
Live-CMS in LCMBIAR-Datei [Seite 621]
Quell-CMS (Live) zu Ziel-CMS (Live) [Seite 624]
Befehlszeilenparameter – Übersicht [Seite 628]

36.1.6.3.2 LCMBIAR-Datei auf einen Live-CMS

Beim Hochstufen von Objekten aus einer LCMBIAR-Datei auf einen Live-CMS können Sie in der Befehlszeile auf eine Eigenschaftendatei verweisen, die die Hochstufungsreihenfolge wie folgt definiert:

- der Speicherort für den Import und die Hochstufungs-Vorgangsart
- Anmeldedaten für den CMS, der die Hochstufverwaltung hostet (bisher Lifecycle Management Tool (LCM) genannt)
- Anmeldedaten für den Ziel-CMS
- weitere Parameter, die für eine erfolgreiche Hochstufung zum CMS erforderlich sind, z.B. das LCMBIAR-Kennwort, ggf. die Einstellung zum Überschreiben vorhandener Objekte

Sie können weitere optionale Parameter einbinden, um andere Hochstufungsaufgaben zu erfüllen. Diese optionalen Parameter werden im Abschnitt Befehlszeilenparameter – Übersicht [Seite 628] beschrieben.

Das folgende Beispiel veranschaulicht die Hochstufung einer LCMBIAR-Datei auf einen Live-CMS, ohne in der Befehlszeile auf eine Eigenschaftendatei zu verweisen:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -action promote -LCM_CMS myCMS.mydomain.sap:6400 -LCM_userName
adminLCM -LCM_password my_adminpassword1 -
Destination_CMS myCMS.mydomain.sap:6400 -Destination_userName adminLCM
-Destination_password my_adminpassword1 -
importLocation "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\Samples\webi\WebISamples.lcmbiar" -
lcmbiarpassword
```

Das folgende Beispiel veranschaulicht die Hochstufung einer LCMBIAR-Datei auf einen Live-CMS unter Verwendung einer Eigenschaftendatei in der Befehlszeile:

```
Go to
```

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -lcmproperty C:\LCMTEST\MyPropertyFile.properties
#
LCM command line property file
#
action=promote
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
#
importLocation=C:\Backup\CR.lcmbiar
lcmbiarpassword=validlcmbiarpassword
#
Destination_CMS=myCMS.mydomain.sap:6400
Destination_userName=adminLCM
Destination_password=my_adminpassword1
#
```

Die folgende Tabelle enthält die obligatorischen Parameter, die eine Eigenschaftendatei zur erfolgreichen Hochstufung aus einer LCMBIAR-Datei auf einen Live-CMS benötigt:

Parametergruppe	Parameter	Beschreibung
Vorgangsart	`action`	Durchzuführender Vorgang über das Command Line Interface (CLI) Wert: export Beispiel: `action=export`
LCM-Knoten	`LCM_CMS`	CMS für die Hochstufverwaltung Wert: Freiformtext Beispiel: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Benutzernamen des Kontos, den das Tool zum Herstellen einer Verbindung mit dem CMS der Hochstufverwaltung verwenden muss. Wert: Freiformtext Beispiel: `LCM_userName=adminLCM`
	`LCM_password`	Kennwort für das Benutzerkonto Wert: Freiformtext Beispiel: `LCM_password=my_adminpassword1`

Parametergruppe	Parameter	Beschreibung
Quelle: LCMBIAR-Datei	`importLocation`	Speicherort der LCMBIAR-Datei, die die hochzustufenden Objekte enthält. Wert: Freiformtext. Muss eine `<.lcmbiar>`-Erweiterung aufweisen. Beispiel: `importLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Ermöglicht die Ver- und Entschlüsselung von BIAR-Dateien mithilfe eines Kennworts. Wert: Freiformtext Beispiel: `lcmbiar=validlcmbiarpassword`
Ziel: Live-CMS	`Destination_CMS`	CMS, mit dem sich das Tool verbinden muss. Wert: Gültiger CMS-Name Beispiel: `Destination_CMS=myCMS.mydomain.sap:6400`
	`Destination_username`	Benutzername des Kontos, den das Tool zum Herstellen einer Verbindung mit dem BI-Plattform-CMS verwenden muss. Wert: Gültiger Benutzername Beispiel: `Destination_username=adminLCM`
	`Destination_password`	Kennwort für das Benutzerkonto Wert: Gültiges Kennwort Beispiel: `Destination_password=my_adminpassword1`

Weitere Informationen

Live-CMS in LCMBIAR-Datei [Seite 621]

Quell-CMS (Live) zu Ziel-CMS (Live) [Seite 624]
Befehlszeilenparameter – Übersicht [Seite 628]

36.1.6.3.3 Live-CMS in LCMBIAR-Datei

Beim Hochstufen von Objekten von einem Live-CMS in eine LCMBIAR-Datei können Sie in der Befehlszeile auf eine Eigenschaftendatei verweisen, die die Hochstufungsreihenfolge wie folgt definiert:

- Hochstufungs-Vorgangsart: Export
- Anmeldedaten für den CMS, der die Hochstufverwaltung hostet (bisher Lifecycle Management Tool (LCM) genannt)
- Anmeldedaten für den Quell-CMS
- Zielverzeichnis der LCMBIAR-Datei
- Weitere erforderliche Parameter für die erfolgreiche CMS-Hochstufung, wie z. B. LCMBIAR-Kennwort und Sicherheitseinstellungen

Sie können weitere optionale Parameter einbinden, um andere Hochstufungsaufgaben zu erfüllen. Diese optionalen Parameter werden im Abschnitt Befehlszeilenparameter – Übersicht [Seite 628] beschrieben.

Das folgende Beispiel zeigt eine typische Eigenschaftendatei zur Hochstufung von einem Live-CMS in eine LCMBIAR-Datei:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -lcmproperty C:\LCMTEST\MyPropertyFile.properties
#
#action=export
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
#
Source_CMS=myCMS.mydomain.sap:6400
Source_userName=adminLCM
Source_password=my_adminpassword1
#
exportLocation=E:\LCMTEST\
lcmbiarpassword=
#
#Queries
#
exportQuery1=SELECT TOP 10000 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)")
#
#When applicable...
#
exportDependencies=true
includeSecurity=true
#
#Options
#
consolelog=true
```

Die folgende Tabelle enthält die obligatorischen Parameter, die eine Eigenschaftendatei zur erfolgreichen Hochstufung aus einer LCMBIAR-Datei auf einen Live-CMS benötigt:

Parametergruppe	Parameter	Beschreibung
Vorgangsart	`action`	Durchzuführender Vorgang über das Command Line Interface (CLI) Wert: export Beispiel: `action=export`
LCM-Knoten	`LCM_CMS`	CMS für die Hochstufverwaltung Wert: Freiformtext Beispiel: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Benutzernamen des Kontos, den das Tool zum Herstellen einer Verbindung mit dem CMS der Hochstufverwaltung verwenden muss. Wert: Freiformtext Beispiel: `LCM_userName=adminLCM`
	`LCM_password`	Kennwort für das Benutzerkonto Wert: Freiformtext Beispiel: `LCM_password=my_adminpassword1`
Quelle: Live-CMS	`Source_CMS`	CMS, mit dem sich die Hochstufverwaltung verbinden muss. Wert: Freiformtext Beispiel: `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_userName`	Benutzername des Kontos, den die Hochstufverwaltung zum Herstellen einer Verbindung mit dem BI-Plattform-CMS verwenden muss. Wert: Freiformtext Beispiel: `Source_username=adminLCM`

Parametergruppe	Parameter	Beschreibung
	`Source_password`	Kennwort für das Benutzerkonto Wert: Freiformtext Beispiel: `Source_password=my_adminpassword1`
Ziel: LCMBIAR-Datei	`exportLocation`	Gibt den Speicherort an, an dem die LCMBIAR-Datei abgelegt wird, nachdem die Objekte exportiert und gepackt wurden. Wert: Freiformtext. Muss eine `<.lcmbiar>`-Erweiterung aufweisen. Beispiel: `exportLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Ermöglicht die Ver- und Entschlüsselung von BIAR-Dateien mithilfe eines Kennworts. Wert: Freiformtext Beispiel: `lcmbiarpassword=validlcmbiarpassword`

Parametergruppe	Parameter	Beschreibung
Export	`exportQuery`	Fragt den Quell-CMS ab, um die erforderlichen Objekte für den Export in die LCMBIAR-Datei zu ermitteln. Wert: 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.

Weitere Informationen

LCMBIAR-Datei auf einen Live-CMS [Seite 618]
Quell-CMS (Live) zu Ziel-CMS (Live) [Seite 624]
Befehlszeilenparameter – Übersicht [Seite 628]

36.1.6.3.4 Quell-CMS (Live) zu Ziel-CMS (Live)

Beim Hochstufen von Objekten von einem Quell-CMS (Live) auf einen Ziel-CMS (Live) können Sie in der Befehlszeile auf eine Eigenschaftendatei verweisen, die die Hochstufungsreihenfolge wie folgt definiert:

- Hochstufungs-Vorgangsart: Promote
- Anmeldedaten für den CMS, der die Hochstufverwaltung hostet (bisher Lifecycle Management Tool (LCM) genannt)
- Anmeldedaten für den Quell-CMS
- Anmeldedaten für den Ziel-CMS
- Weitere erforderliche Parameter für die erfolgreiche CMS-Hochstufung, wie z. B. Sicherheits- und Abhängigkeitsparameter

Sie können weitere optionale Parameter einbinden, um andere Hochstufungsaufgaben zu erfüllen. Diese optionalen Parameter werden im Abschnitt Befehlszeilenparameter – Übersicht [Seite 628] beschrieben.

Das folgende Beispiel zeigt eine typische Eigenschaftendatei zur Hochstufung von einem Quell-CMS zu einem Ziel-CMS:

```
#
action=promote
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
LCM_authentication=secEnterprise
#
Source_CMS=myCMS1:myCMS2
Source_userName=adminLCM
Source_password=my_adminpassword1
Source_authentication=secEnterprise
#
Destination_CMS=myCMS1:myCMS2
Destination_userName=adminLCM
Destination_password=my_adminpassword1
Destination_authentication=secEnterprise
#
exportQuery1select*from CI_INFOOBJECTS where SI_NAME='Charting Samples' and
SI_KIND='Webi'
#
includeSecurity=false
#
exportDependencies=false
#
```

Die folgende Tabelle enthält die obligatorischen Parameter, die eine Eigenschaftendatei zur erfolgreichen Hochstufung von einem Quell-CMS zu einem Ziel-CMS benötigt:

Parametergruppe	Parameter	Beschreibung
Vorgangsart	`action`	Durchzuführender Vorgang in der Befehlszeile Wert: promote Beispiel: `action=promote`
LCM-Knoten	`LCM_CMS`	CMS für die Hochstufverwaltung Wert: Freiformtext Beispiel: `LCM_CMS=myCMS.mydomain.sap:6400`

Parametergruppe	Parameter	Beschreibung
	`LCM_userName`	Benutzernamen des Kontos, den das Tool zum Herstellen einer Verbindung mit dem CMS der Hochstufverwaltung verwenden muss. Wert: Freiformtext Beispiel: `LCM_userName=adminLCM`
	`LCM_password`	Kennwort für das Benutzerkonto Wert: Freiformtext Beispiel: `LCM_password=my_adminpassword1`
Quelle: Live-CMS	`source_CMS`	CMS, mit dem sich die Hochstufverwaltung verbinden muss. Wert: Freiformtext Beispiel: `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_username`	Benutzername des Kontos, den die Hochstufverwaltung zum Herstellen einer Verbindung mit dem BI-Plattform-CMS verwenden muss. Wert: Freiformtext Beispiel: `Source_username=adminLCM`
	`Source_password`	Kennwort für das Benutzerkonto Wert: Freiformtext Beispiel: `Source_password=my_adminpassword1`
Ziel: Live-CMS	`Destination_CMS`	CMS, mit dem sich das Tool verbinden muss. Wert: Freiformtext Beispiel: `Destination_CMS=myCMS1:myCMS2`

Parametergruppe	Parameter	Beschreibung
	`Destination_username`	Benutzername des Kontos, den das Tool zum Herstellen einer Verbindung mit dem BI-Plattform-CMS verwenden muss. Wert: Freiformtext Beispiel: `Destination_username=admin LCM`
	`Destination_password`	Kennwort für das Benutzerkonto Wert: Freiformtext Beispiel: `Destination_password=my_adminpassword1`
Export	`exportQuery`	Abfragen, die die Hochstufverwaltung ausführt, um die erforderlichen Objekte für den Export zum Ziel-CMS zu ermitteln. Wert: 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.

Weitere Informationen

LCMBIAR-Datei auf einen Live-CMS [Seite 618]

Live-CMS in LCMBIAR-Datei [Seite 621]
Befehlszeilenparameter – Übersicht [Seite 628]

36.1.6.3.5 Befehlszeilenparameter – Übersicht

Die folgende Tabelle beschreibt alle verfügbaren Befehlszeilenparameter.

> **Hinweis**
>
> Innerhalb einer Befehlszeile sind Parameter an folgende Syntax gebunden: `-<parameterName><space><parameterValue>`. Innerhalb einer Eigenschaftendatei sind Parameter an folgende Syntax gebunden: `<parameterName>=<parameterValue>`.

Parametergruppe	Parameter	Beschreibung
Eigenschaftendatei	`lcmproperty`	Verweist auf die für die Ausführung eines Befehls erforderlichen Werte, die in einer Datei gespeichert sind. Wert: Der vollständige Pfad zum Speicherort der Eigenschaftendatei. Beispiel: `-lcmproperty C:\MyPropertyFile.properties`
Vorgangsart	`action`	Durchzuführender Vorgang über das Command Line Interface (CLI) Wert: `promote` oder `export` Beispiel: `action=promote`
LCM-Knoten	`LCM_CMS`	CMS für die Hochstufverwaltung Wert: Freiformtext Beispiel: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Benutzernamen des Kontos, den das Tool zum Herstellen einer Verbindung mit dem CMS der Hochstufverwaltung verwenden muss. Wert: Freiformtext Beispiel: `LCM_userName=adminLCM`
	`LCM_Password`	Kennwort für das Benutzerkonto Erforderlich in der Konsole, falls leer. Wert: Freiformtext Beispiel: `LCM_password=my_adminpassword1`

Parametergruppe	Parameter	Beschreibung
	`LCM_authentication`	Gibt den zu verwendenden Authentifizierungstyp an. Wert: secEnterprise, secWinAD, secLDAP, secSAPR3. Ist dieser nicht festgelegt, wird standardmäßig `secEnterprise` verwendet. Beispiel: `LCM_authentication=secEnterprise`
	`LCM_systemID` **Hinweis** Obligatorisch für die SAP-Authentifizierung.	Erforderlich nur für die SAP-Authentifizierung. Wert: System-ID Beispiel: `LCM_systemID=systemID`
	`LCM_clientID` **Hinweis** Obligatorisch für die SAP-Authentifizierung.	Erforderlich nur für die SAP-Authentifizierung. Wert: Client-ID Beispiel: `LCM_clientID=clientID`
Quelle: LCMBIAR-Datei	`importLocation`	Speicherort der LCMBIAR-Datei, die die hochzustufenden Objekte enthält. Wert: Freiformtext. Muss eine `<.lcmbiar>`-Erweiterung aufweisen. Beispiel: `importLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Ermöglicht die Ver- und Entschlüsselung von BIAR-Dateien mithilfe eines Kennworts. Wert: Freiformtext Beispiel: `lcmbiar=validlcmbiarpassword`
Quelle: Live-CMS	`Source_CMS`	CMS, mit dem sich die Hochstufverwaltung verbinden muss. Wert: Freiformtext Beispiel: `Source_CMS=myCMS.mydomain.sap:6400`

Parametergruppe	Parameter	Beschreibung
	`Source_UserName`	Benutzername des Kontos, den die Hochstufverwaltung zum Herstellen einer Verbindung mit dem BI-Plattform-CMS verwenden muss. Wert: Freiformtext Beispiel: `Source_username=adminLCM`
	`Source_password`	Kennwort für das Benutzerkonto Wert: Freiformtext Beispiel: `Source_password=my_adminpassword1`
	`Source_authentication`	Gibt den zu verwendenden Authentifizierungstyp an. Wert: secEnterprise, secWinAD, secLDAP, secSAPR3. Ist dieser nicht festgelegt, wird standardmäßig `secEnterprise` verwendet. Beispiel: `Source_authentication=secEnterprise`
	`Source_systemID` **Hinweis** Obligatorisch für die SAP-Authentifizierung.	Erforderlich nur für die SAP-Authentifizierung. Wert: System-ID Beispiel: `Source_systemID=systemID`
	`Source_clientID` **Hinweis** Obligatorisch für die SAP-Authentifizierung.	Erforderlich nur für die SAP-Authentifizierung. Wert: System-ID Beispiel: `Source_clientID=clientID`
Ziel: LCMBIAR-Datei	`exportLocation`	Gibt den Speicherort an, an dem die LCMBIAR-Datei abgelegt wird, nachdem die Objekte exportiert und gepackt wurden. Wert: Freiformtext. Muss eine `<.lcmbiar>`-Erweiterung aufweisen. Beispiel: `exportLocation=C:\Backup\New.lcmbiar`

Parametergruppe	Parameter	Beschreibung
	`lcmbiarpassword`	Ermöglicht die Ver- und Entschlüsselung von BIAR-Dateien mithilfe eines Kennworts. Wert: Freiformtext Beispiel: `lcmbiarpassword=validlcmbiarpassword`
Ziel: Live-CMS	`Destination_CMS`	CMS, mit dem sich das Tool verbinden muss. Wert: Gültiger CMS-Name Beispiel: `Destination_CMS=myCMS.mydomain.sap:6400`
	`Destination_username`	Benutzername des Kontos, den das Tool zum Herstellen einer Verbindung mit dem BI-Plattform-CMS verwenden muss. Wert: Gültiger Benutzername Beispiel: `Destination_username=adminLCM`
	`Destination_password`	Kennwort für das Benutzerkonto Wert: Gültiges Kennwort Beispiel: `Destination_password=my_adminpassword1`
	`Destination_authentication`	Gibt den zu verwendenden Authentifizierungstyp an. Wert: secEnterprise, secWinAD, secLDAP, secSAPR3. Ist dieser nicht festgelegt, wird standardmäßig `secEnterprise` verwendet. Beispiel: `Destination_authentication=secEnterprise`
	`Destination_systemID` **Hinweis** Obligatorisch für die SAP-Authentifizierung.	Erforderlich nur für die SAP-Authentifizierung. Wert: System-ID Beispiel: `Destination_systemID=systemID`

Parametergruppe	Parameter	Beschreibung
	`Destination_clientID` **Hinweis** Obligatorisch für die SAP-Authentifizierung.	Erforderlich nur für die SAP-Authentifizierung. Wert: Client-ID Beispiel: `Destination_clientID=clientID`
Auftrag	`JOB_CUID`	Weist das Tool an, alle Objekte im Auftrag in die LCMBIAR-Datei zu exportieren. Wert: CUID des gespeicherten Hochstufverwaltungs-Auftrags
	`Override`	Wird zum selektiven Abrufen von Objekten aus einer LCMBIAR-Datei verwendet. Wenn `true`: Ermöglicht das Überschreiben eines vorhandenen Auftrags. Wenn `false`: Ermöglicht die Erstellung eines neuen Auftrags mit dem Namen `<JOB_NAME>_<TIME_STAMP>` . Wert: `true` oder `false` Beispiel: `Override=true`
	`forceOverride` Verfügbar in SP4	Wird für das Überschreiben eines Auftrags mit demselben Namen und einer abweichenden CUID verwendet. Wert: `true` oder `false` Beispiel: `forceOverride=true`
	`Timeout` Verfügbar in SP4	Legt einen Wert für die Zeitüberschreitung des Hochstufungsvorgangs fest. Wert: Zeit (Sekunden) Beispiel: `timeout=30`
Export	`ExportDependencies`	Gibt die von dem Tool für den Export gesammelten Objektabhängigkeiten an. Nur anwendbar in Verbindung mit dem Kennzeichen `Source_CMS`. Wert: `true` oder `false`. Ist dieser nicht festgelegt, wird standardmäßig `false` verwendet. Beispiel: `ExportDependencies=false`

Parametergruppe	Parameter	Beschreibung
	`ExportQuery`	Abfragen, die die Hochstufverwaltung ausführt, um die erforderlichen Objekte für den Export zum Ziel-CMS zu ermitteln. Wert: 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.

	`ExportQueriesTotal`	Gibt die Anzahl der auszuführenden Exportabfragen an. Wenn Sie über x Exportabfragen verfügen und alle Abfragen ausführen möchten, muss dieser Parameter auf x festgelegt werden.
		
		Wert: Positive Ganzzahl. Ist dieser nicht festgelegt, wird standardmäßig 1 verwendet.
		
		Beispiel: `ExportQuery1=<your sql statement>`
		`ExportQuery2=<your sql statement>`
		`ExportQueriesTotal=2`

Parametergruppe	Parameter	Beschreibung
	`BatchJobQuery`	Wird in Verbindung mit `ExportQuery` verwendet. Erstellt und startet für jede Zeile, die durch die Auftragsabfrage zurückgegeben wird, einen Auftrag. Auftragsexportabfragen können durch Platzhalter erweitert werden, die auf Eigenschaften aus der Auftragsabfrage verweisen. Das Platzhalterformat ist $b:PPTY$ (der Eigenschaftsname unterliegt dabei nicht der Groß-/Kleinschreibung). Gültige Eigenschaften ("PPTY") sind "CUID", "NAME" und "ID". Es wird ein Fehler ausgegeben, wenn der Platzhalter nicht durch die Auftragsabfrage erkannt bzw. zurückgegeben wurde. Wert: Freiformtext Beispiel: `batchJobQuery=SELECT si_cuid,si_name FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)") AND SI_KIND='Folder' AND SI_NAME LIKE '%sample%' and SI_PARENTID=0` `exportQuery1= SELECT TOP 10000 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='$b:CUID$'")`
	`LimitQueryBatchSize`	Beschränkt die Anzahl der zurückgegebenen Objekte standardmäßig auf 1.000. Wenn dieser Parameter auf `false` festgelegt 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 `select TOP <number>` festlegen. Wert: `true` oder `false`. Ist dieser nicht festgelegt, wird standardmäßig `true` verwendet. Beispiel: `LimitQueryBatchSize=true`

Parametergruppe	Parameter	Beschreibung
Protokollierung	`consolelog`	Wird zur Anzeige des kompletten Protokolls des vom Benutzer ausgeführten Befehls im Befehlsprotokoll verwendet. Wert: `true` oder `false`. Ist dieser nicht festgelegt, wird standardmäßig `false` verwendet. Beispiel: `consolelog=true`
	`ResultFileName`	Der Name der Daei im lokalen Dateisystem, wenn der Parameter `consolelog` verwendet wird. Wert: Dateipfad des Auftragsergebnisses Beispiel: `ResultFileName=C:\Logs\ResultFile.txt`
	`LogFileName` Verfügbar in SP4	Ermöglicht die Verwendung eines statischen Dateipfads für die Protokolldatei. Wert: Protokolldateipfad Beispiel: `LogFileName=C:\Logs\LogFile.log`
Objektauswahl	`Selected_CUIDS`	Ermöglicht die Hochstufung ausgewählter Objekte (Berichte, Benutzer, Universen usw.) zusammen mit ihren Abhängigkeiten aus einer LCMBIAR-Datei anstelle von ganzen Dateien. Wert: CUIDs der hochzustufenden Objekte in der LCMBIAR-Datei
	`selectUser` Verfügbar in SP4	Filtert Benutzer nach Drittanbieter-Authentifizierung (LDAP, SAPR3, WindowsAD usw.) Wert: `all`, `none`, `excludeTP` oder `onlyTP`. Ist dieser nicht festgelegt, wird standardmäßig `all` verwendet. Beispiel: `selectUser=excludeTP`
	`selectGroup` Verfügbar in SP4	Filtert Benutzergruppen nach Drittanbieter-Authentifizierung (LDAP, SAPR3, WindowsAD usw.) Wert: `all`, `none`, `excludeTP` oder `onlyTP`. Standardmäßig `all`, sofern nicht abweichend definiert. Beispiel: `selectGroup=onlyTP`

Parametergruppe	Parameter	Beschreibung
Sicherheit	`IncludeApplicationSecurity`	Weist das Tool an, die mit den ausgewählten Anwendungen assoziierten Sicherheitseinstellungen zu exportieren oder zu importieren. Wert: `true` oder `false`. Ist dieser nicht festgelegt, wird standardmäßig `false` verwendet. Beispiel: `IncludeApplicationSecurity=true`
	`IncludeSecurity`	Weist das Tool an, die mit den ausgewählten Objekten und Benutzern assoziierten Sicherheitseinstellungen zu exportieren oder zu importierten. Wenn Zugriffsberechtigungen verwendet werden, werden diese hiermit ebenfalls exportiert bzw. importiert. Wert: `true` oder `false`. Ist dieser nicht festgelegt, wird standardmäßig `false` verwendet. Beispiel: `IncludeSecurity=true`
Kommentare	`IncludeComments`	Weist das Tool an, die mit den ausgewählten Objekten assoziierten Kommentare zu exportieren oder zu importieren. Wert: `true` oder `false`. Ist dieser nicht festgelegt, wird standardmäßig `false` verwendet. Beispiel: `IncludeComments=true`
Föderationsjobs	`IncludeFederationJobsRelationship`	Weist das Tool an, die Beziehungen der Föderationsjobs (Replikationslisten und Remote-Verbindungen) beizubehalten. Wenn dieser Wert auf `false` festgelegt ist, werden replizierte Objekte zu normalen Objekten, und das Föderationskennzeichen wird entfernt. Dies kann hilfreich sein, wenn das replizierte Objekte das einzig verfügbare Objekt ist und das Quellobjekt nicht länger zur Verfügung steht. Wert: `true` oder `false`. Ist dieser nicht festgelegt, wird standardmäßig `true` verwendet. Beispiel: `IncludeFederationJobsRelationship=false`

36.1.6.3.6 Rollback

Sie können den hochgestuften Auftrag im Zielsystem über die *Hochstufverwaltung* zurücksetzen.

Wenn Sie einen Auftrag z. B. über die *Hochstufverwaltung* hochgestuft haben, um BI 4.2 SP07 auf BI 4.3 zu aktualisieren, und wenn Sie diese Änderung später wieder rückgängig machen möchten, können Sie die

Befehlszeilenparameter verwenden, die in Befehlszeilenparameter nach Hochstufungsszenario [Seite 614] definiert wurden, und den Rollback-Vorgang ausführen.

Wenn Sie den Rollback-Vorgang ausführen, müssen Sie eine Eigenschaftendatei bereitstellen, die den Hochstufungsreihenfolge wie folgt definiert:

- Hochstufungs-Vorgangsart: Rollback
- Anmeldedaten für den CMS, der die Hochstufverwaltung hostet (bisher Lifecycle Management Tool (LCM) genannt)
- Anmeldedaten für den Quell-CMS
- Anmeldedaten für den Ziel-CMS
- Weitere erforderliche Parameter für die erfolgreiche CMS-Hochstufung, wie z. B. Sicherheits- und Abhängigkeitsparameter

Sie können weitere optionale Parameter einbinden, um andere Hochstufungsaufgaben zu erfüllen. Diese optionalen Parameter werden in Befehlszeilenparameter – Übersicht [Seite 628] beschrieben.

Sie können auf das unten aufgeführte Beispiel für eine Eigenschaftendatei verweisen, um einen Rollback-Vorgang auszuführen:

```
#
action=rollback
job_cuid=AWWxyVk5fkFKjtQnRAygAYg
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
LCM_authentication=secEnterprise
```

> **Hinweis**
>
> Sie finden die Eigenschaftsdatei `job_cuid` für einen hochgestuften Auftrag unter *CMC-Startseite* > *Hochstufverwaltung* > *Eigenschaften*.

Die folgende Tabelle enthält die obligatorischen Parameter, die eine Eigenschaftendatei zur erfolgreichen Hochstufung aus einer LCMBIAR-Datei auf einen Live-CMS benötigt:

Parametergruppe	Parameter	Beschreibung
Vorgangsart	`action`	Durchzuführender Vorgang über das Command Line Interface (CLI) Wert: Rollback Beispiel: `action=rollback`

Parametergruppe	Parameter	Beschreibung
Auftrag	`job_cuid`	Weist das Tool an, alle Objekte im Auftrag in die LCMBIAR-Datei zu exportieren. Wert: CUID des gespeicherten Hochstufverwaltungs-Auftrags Beispiel: `job_cuid=AWWxyVk5fkFKjtQnRAygAYg`
LCM-Knoten	`LCM_CMS`	CMS für die Hochstufverwaltung Wert: Freiformtext Beispiel: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Benutzernamen des Kontos, den das Tool zum Herstellen einer Verbindung mit dem CMS der Hochstufverwaltung verwenden muss. Wert: Freiformtext Beispiel: `LCM_userName=adminLCM`
	`LCM_password`	Kennwort für das Benutzerkonto Wert: Freiformtext Beispiel: `LCM_password=my_adminpassword1`
	`LCM_authentication`	Authentifizierungstyp für das Benutzerkonto Wert: Authentifizierungstyp Beispiel: `secEnterprise`

36.1.6.4 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>
```

> **Hinweis**
>
> Enthält die `Eigenschaften`-Datei keine persönlichen Informationen, wird der Benutzer von der LCM-Befehlzeilenschnittstelle in der Konsole aufgefordert, diese einzugeben.

36.1.7 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)

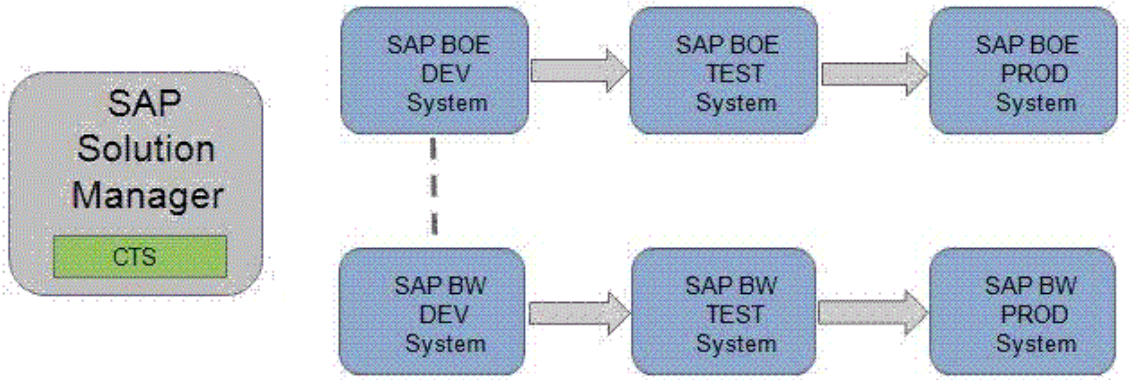
Weitere Informationen über CTS+- und ABAP-fremde Transporte finden Sie unter Transporting Non-ABAP Objects in Change and Transport System

36.1.7.1 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 im 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.
5. Die SAP-Business-Warehouse-Transportlandschaft (SAP-BW-Transportlandschaft) wurde im Change and Transport System (CTS) konfiguriert.
6. 1692417 und 1860594 wurden auf dem Rechner implementiert, der als Host für den Webdienst CTS Deploy fungiert.

36.1.7.2 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.

Weitere Informationen

Aktivieren des Webdiensts für den CTS-Export [Seite 641]
Konfigurieren von CTS+-Einstellungen im Hochstufverwaltungstool [Seite 642]
Konfigurieren der BI-Plattform und CTS+-Integration [Seite 640]

36.1.7.2.1 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.

36.1.7.2.2 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.
   - *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, der in der CTS-Konfiguration verwendet wird >`

- `<IP-Nummer des Quellsystems von SAP BI>@<CMS-Portnummer> = <logischer Name für das Quellsystem, der in der CTS-Konfiguration verwendet wird >`

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.

36.1.7.2.3 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.
   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.

36.1.7.2.4 Exportieren von der BI-Plattform nach CTS+ mit SSL

36.1.7.2.4.1 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.

36.1.7.2.4.2 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`.
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.

36.1.7.2.4.3 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).

36.1.7.2.4.4 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.

36.1.7.2.5 Importieren von CTS+ zur BI-Plattform mit SSL

36.1.7.2.5.1 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 2048 -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=John Smith, OU=Accounting, 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>:<SSLPORTNUMMER>`

Weitere Informationen

Konfigurieren von SSL für CTS+ [Seite 645]

36.1.7.2.5.2 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 645]

36.1.7.2.5.3 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.

36.1.7.3 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.

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.

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:

       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 586]
Verwalten der Abhängigkeiten eines Auftrags [Seite 592]

36.1.8 Verwendung des Hochstufverwaltungs-Assistenten

Mit dem Hochstufverwaltungs-Assistenten können Sie Business-Intelligence-(BI-)Ressourcen mit nur wenigen Klicks unkompliziert von einem Repository in ein anderes kopieren.

Der Hochstufverwaltungs-Assistent unterstützt folgende Hochstufungsszenarios:

- BI-Ressourcen aus einem Quellsystem in eine LCMBIAR-Datei exportieren
- BI-Ressourcen aus einem Quellsystem in ein Zielsystem replizieren
- LCMBIAR-Dateien in ein Zielsystem importieren

Mit dem Hochstufverwaltungs-Assistenten können Sie nun alle oder nur selektive Inhalte eines Repository ohne Verwendung der Befehlszeile hochstufen. Die benutzerfreundliche grafische Oberfläche des Hochstufverwaltungs-Assistenten unterstützt Sie bei der Arbeit als Administrator.

Zusatzinformationen zu den Best Practices für den Hochstufverwaltungs-Assistenten finden Sie in SAP-Hinweis 2531264.

> ⚠ Achtung
>
> Der Hochstufverwaltungs-Assistent unterstützt kein Rollback. Dies bedeutet, dass Sie nach dem Hochstufen von BI-Ressourcen das Zielsystem nicht in seinen vorherigen Zustand zurücksetzen können.

> ⓘ Hinweis
>
> Prüfen Sie den Speicherwert, bevor Sie mit dem Hochstufen von Objekten beginnen. Der Wert "Xms" muss kleiner als der Wert "Xmx" sein oder diesem entsprechen.

> ⓘ Hinweis
>
> Richten Sie das Zielsystem entsprechend ein, wenn Sie über QaaWs-Objekte verfügen.

> → Tipp
>
> Deaktivieren Sie die Auditing- und Überwachungsdienste in der CMC des Zielsystems, um die Performance zu verbessern. Weitere Informationen finden Sie im Abschnitt "Auditing" des Administratorhandbuchs für SAP BusinessObjects Business Intelligence.

36.1.8.1 Objekte von der Hochstufung ausschließen

Sie können die Objekte aus der unten bereitgestellten Liste auswählen, und diese von einem Hochstufungsauftrag ausschließen, um Speicherplatz zu sparen und die Migrationszeit zu verringern.

Ein Hochstufungsauftrag migriert jedes BI-Asset aus der Quelle in das Zielsystem. Dadurch werden auch die Assets migriert, die spezifisch für das Quellsystem und im Zielsystem nicht von Nutzen sind. Um BI-Assets von der Hochstufung auszuschließen, führen Sie die folgenden Schritte aus.

1. Rufen Sie `<INSTALLVERZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` auf.
2. Öffnen Sie die *PromotionManagementWizard.ini* in einem Texteditor.

3. Suchen Sie nach der Zeichenfolge *# Liste der automatisch auszuschließenden Arten von vollständigem/selektivem Export.*
   Der Code `-Dcom.sap.businessobjects.pmw.exclude.kind={}` befindet sich unter der Zeichenfolge.
4. Fügen Sie die auszuschließenden Objekte gemäß der untenstehenden Liste zwischen den geschweiften Klammern `{}` ein.
5. Speichern Sie die Datei.

Die im Code genannten Objekte werden beim Ausführen eines Hochstufungsauftrags ausgeschlossen.

Die Liste der Objekte, die von einem Hochstufungsauftrag ausgeschlossen werden können, finden Sie in der folgenden Tabelle.

Benutzerdefinierte Attribute	DFS-Parameter	Discussions	DSGVO-Objekt
LCM JOBS	LCM Overrides	LCM Scan History	LCM Settings
LANDSCAPE	LANDSCAPE Connection	LIVE Office	MoN.MBEAN Config
MON.ManagedEntity Status	MON.MonAppDataStore	Mon.Probe	Mon.Subscription
NotificationScheduleObject	Eintrag überschreiben	Status PlatformSearchApplication	PlatformSearchContentExtractor
PlatformSearchContentStore	PlatformSearchIndexEngine	PlatformSearchQueue	PlatformSearchScheduling
PlatformSearchSearchAgent	PlatformSearchServiceSession	TaskTemplate	VisualDifferenceComprator
XL.XcelsiusApplication	busobjectreporter	Explorer	Lumira Extensions

36.1.8.2 Anwendungsbeispiele für den Hochstufverwaltungs-Assistenten

Für die Hochstufverwaltung stehen Ihnen mehrere Optionen zur Verfügung. Die folgende Tabelle hilft Ihnen, zu entscheiden, ob der Hochstufverwaltungs-Assistent die richtige Lösung für Ihre Anforderungen ist.

Optionen für die Hochstufverwaltung

	Hochstufverwaltungs-Assistent	**Hochstufverwaltung mit Befehlszeilenoption**	**Hochstufverwaltung in der Central Management Console**
Zweck	Einmalige Hochstufung	Automatisierung	Projekt
Hochstufungsumfang	Alle wichtigen BI-Ressourcen	Alle wichtigen BI-Ressourcen	Einige BI-Ressourcen
Auftrag	Sie können keine Aufträge erstellen, die vom Jobserver erneut ausgeführt werden können.	Sie können Aufträge erstellen, die vom Jobserver ausgeführt werden.	Sie können Aufträge erstellen, die vom Jobserver ausgeführt werden.

> **Hinweis**
>
> LCMBIAR-Dateien können mit allen Hochstufverwaltungs-Optionen verwendet werden, unabhängig davon, welche Sie auswählen.

36.1.8.2.1 Einstellungen für die Hochstufverwaltung definieren

1. Nehmen Sie die erforderlichen Einstellungen für die Hochstufverwaltung vor. Die benötigten Informationen können Sie folgender Tabelle entnehmen:

Einstellung	Beschreibung
Temporärer Ordner	ⓘ Hinweis Ordnen Sie für den temporären Ordner ausreichend freien Speicherplatz zu. Der freier Speicherplatz muss mindestens doppelt so groß wie der erforderliche Speicherplatz sein.
Protokollspeicherort	Der Protokollspeicherort wird standardmäßig vorbelegt. Sie können den Protokollspeicherort später ändern. Die in den Einstellungen der Hochstufverwaltung vorgenommenen Änderungen werden umgehend angewendet.
Protokollierungsebene	Sie können die Protokollierungsebene wie folgt festlegen: • Standard • Niedrig • Mittel • Hoch Die Protokollierungsebene wird, sofern nicht von Ihnen geändert, auf "Standard" festgelegt.
Sprache	Sie können die bevorzugte Sprache des Hochstufverwaltungs-Assistenten festlegen.

2. Wählen Sie *Weiter*.

36.1.8.3 Szenario

Der Hochstufverwaltungs-Assistent unterstützt die folgenden drei Hochstufungsszenarios:

- Live-System in LCMBIAR-Datei: Kopiert die Objekte von einem Live-CMS in eine LCMBIAR-Datei.
- Live-CMS in Live-Hochstufung: Stuft die Objekte aus einem Live-CMS-Quellsystem in ein Live-CMS-Zielsystem hoch.
- LCMBIAR-Datei in Live-System: Importiert die Objekte aus einer LCMBIAR-Datei in ein Live-CMS-Zielsystem.

36.1.8.3.1 Objekte aus einem Live-CMS-Quellsystem in eine LCMBIAR-Datei hochstufen

Gehen Sie wie folgt vor, um Objekte von einem Live-CMS in eine LCMBIAR-Datei hochzustufen:

1. Wählen Sie *Exportieren*.
2. Um den Quell-CMS zu definieren, führen Sie eine der folgenden Aktionen aus:
   - Um den zentralen CMS als Quell-CMS zu verwenden, aktivieren Sie das Kontrollkästchen *Zentralen CMS zum Quell-CMS machen*.
   - Geben Sie im Bereich *Quelle* folgende Informationen ein:
     - CMS-Name
     - Benutzer
     - Kennwort
     - Authentifizierung
3. Wählen Sie im Feld *Ziel* die Option *Wählen*, um den Speicherort der LCMBIAR-Datei auszuwählen.
4. (Optional) Geben Sie ein Kennwort ein, um die LCMBIAR-Datei zu verschlüsseln.

   > **Hinweis**
   >
   > Wenn Sie die LCMBIAR-Datei verschlüsseln, benötigt der Hochstufungsprozess mehr Zeit.

5. Klicken Sie auf *Weiter*, und wählen Sie anschließend die Objekte aus, die Sie exportieren möchten.

36.1.8.3.2 Objekte aus einem Live-CMS-Quellsystem in ein Live-CMS-Zielsystem hochstufen

Gehen Sie wie folgt vor, um Objekte aus einem Live-CMS-Quellsystem in ein Live-CMS-Zielsystem hochstufen:

1. Wählen Sie *Hochstufen*.
2. Um den Quell-CMS zu definieren, führen Sie eine der folgenden Aktionen aus:
   - Um den zentralen CMS als Quell-CMS zu verwenden, aktivieren Sie das Kontrollkästchen *Zentralen CMS zum Quell-CMS machen*.
   - Geben Sie im Bereich *Quelle* folgende Informationen ein:
     - CMS-Name
     - Benutzer
     - Kennwort
     - Authentifizierung
3. Um den Ziel-CMS zu definieren, führen Sie eine der folgenden Aktionen aus:
   - Um den zentralen CMS als Ziel-CMS zu verwenden, aktivieren Sie das Kontrollkästchen *Zentralen CMS zum Ziel-CMS machen*.
   - Geben Sie im Bereich *Ziel* folgende Informationen ein:
     - CMS-Name

    - Benutzer
    - Kennwort
    - Authentifizierung
4. Klicken Sie auf *Weiter*, und wählen Sie anschließend die Objekte aus, die Sie aus dem Quellsystem in das Zielsystem kopieren möchten.

36.1.8.3.3 Objekte aus einer LCMBIAR-Datei in ein Live-CMS-Zielsystem hochstufen

Gehen Sie wie folgt vor, um Objekte aus einer LCMBIAR-Datei in ein Live-CMS hochzustufen:

1. Wählen Sie *Importieren*.
2. Um den Ziel-CMS zu definieren, führen Sie eine der folgenden Aktionen aus:
    - Aktivieren Sie im Bereich *Ziel* das Kontrollkästchen *Zentralen CMS zum Ziel-CMS machen*.
    - Geben Sie im Bereich *Ziel* folgende Informationen ein:
        - CMS-Name
        - Benutzer
        - Kennwort
        - Authentifizierung
3. Wählen Sie im Bereich *Ziel* die Option *Wählen*, um die zu importierende LCMBIAR-Datei auszuwählen.
4. (Optional) Geben Sie ein Kennwort ein, um die LCMBIAR-Datei zu verschlüsseln.

    > **Hinweis**
    >
    > Wenn Sie die LCMBIAR-Datei verschlüsseln, benötigt der Hochstufungsprozess mehr Zeit.

5. Klicken Sie auf *Weiter*, und wählen Sie anschließend die Objekte aus, die Sie importieren möchten.

36.1.8.4 Objekte

Der Hochstufverwaltungs-Assistent unterstützt die folgenden zwei Inhaltshochstufungen:

- Hochstufung des gesamten Inhalts
- Hochstufung von selektivem Inhalt

In der folgenden Tabelle werden beide Arten erläutert:

Art der Inhaltshochstufung	Hochgestufter Inhalt	Inhaltsabhängigkeiten
Hochstufung des gesamten Inhalts	Der gesamte Inhalt des Quellsystems wird in das Zielsystem hochgestuft: • Objekte (Benutzer, Dokumente, Universen, Verbindungen, usw.) • Instanzen • Beziehungen zwischen Objekten • Objektsicherheit	Die Abhängigkeiten müssen nicht ausgewertet werden, da alle Beziehungen beibehalten werden. Sie fahren nach dem aktuellen Schritt "Objekte" direkt mit dem Schritt "Übersicht" fort.
Hochstufung von selektivem Inhalt	Ausgewählte Inhalte des Quellsystems werden in das Zielsystem hochgestuft. Dies können folgende Inhalte sein: • Objekte (Benutzer, Dokumente, Universen, Verbindungen, usw.) • Instanzen • Beziehungen zwischen Objekten • Objektsicherheit	Die Abhängigkeiten müssen ausgewertet werden, da nicht alle Inhalte aus dem Quellsystem in das Zielsystem hochgestuft werden.

36.1.8.4.1 Gesamten Inhalt hochstufen

Um den vollständigen Inhalt vom Quellsystem in das Zielsystem hochzustufen:

1. Wählen Sie *Hochstufung des gesamten Inhalts*.

   Alle Objekte werden zur Hochstufung ausgewählt.
2. Klicken Sie auf *Weiter*, um den Inhalt zu prüfen, den Sie ausgewählt haben.

36.1.8.4.2 Informationen zur Hochstufung von selektivem Inhalt

Bevor Sie selektiven Inhalt aus einem Quellsystem in ein Zielsystem hochstufen können, müssen Sie die Exportoptionen definieren. Durch Definition der Exportoptionen können Sie die Einstellungen aus dem Quellsystem, das Sie in das Zielsystem hochstufen möchten, abrufen.

36.1.8.4.2.1 Informationen zu Exportoptionen

Wenn Sie Einstellungen abrufen möchten, die im Quellsystem festgelegt sind, und diese an das Zielsystem weitergeben möchten, müssen Sie die folgenden Parameter in den Exportoptionen festlegen:

- Objektinstanzen
- Objektabhängigkeiten
- Sicherheit
- Kommentar
- Föderations-Aufträge
- Konflikt bei der Namensauflösung

Objektinstanzen

Objektinstanzen	Beschreibung
Alle Instanzen eines Objekts exportieren, wenn das Objekt ausgewählt wird	Sie exportieren die ausgewählten Objekte mit allen zugehörigen Instanzen.
Nur die wiederkehrenden Instanzen eines Objekts exportieren, wenn das Objekt ausgewählt wird	Sie exportieren die ausgewählten Objekte nur mit den wiederkehrenden Instanzen. Wenn Sie beispielsweise eine wöchentliche und ein monatliche Aktualisierung für ein Dokument zeitgesteuert verarbeitet haben, werden dieses Dokument und seine beiden wiederkehrenden Instanzen in den Export einbezogen.
Objektinstanzen nicht exportieren	Sie exportieren nur die ausgewählten Objekte. Ihre Instanzen werden nicht exportiert.

Objektabhängigkeiten

Objektabhängigkeiten	Beschreibung
Abhängigkeiten bei der Auswahl von Objekten einbeziehen	Sie exportieren die ausgewählten Objekte mit allen zugehörigen Abhängigkeiten. **Hinweis** Diese Option ist standardmäßig markiert.
Abhängigkeiten bei der Auswahl von Objekten ausschließen	Sie exportieren nur die ausgewählten Objekte ohne alle zugehörigen Abhängigkeiten.

Sicherheit

Sicherheit	Beschreibung
Objektsicherheit einbeziehen	Sie exportieren die ausgewählten Objekte mit ihren Einstellungen für die Objektsicherheit.
Benutzersicherheit einbeziehen	Sie exportieren die ausgewählten Objekte mit ihren Einstellungen für die Benutzersicherheit.

Sicherheit	Beschreibung
Anwendungssicherheit einbeziehen	Sie exportieren die ausgewählten Objekte mit ihren Einstellungen für die Anwendungssicherheit.
Sicherheit auf oberster Ebene einbeziehen	Sie exportieren die Sicherheitseinstellungen, die im Stammordner definiert wurden. **⚠ Achtung** Diese Option überschreibt die Sicherheitseinstellungen, die im Zielsystem definiert wurden. Sie sollten diese Option sparsam verwenden.

Kommentar

Kommentar	Beschreibung
Kommentare einbeziehen	Sie exportieren die ausgewählten Objekte mit allen zugehörigen Kommentaren.
Benutzergruppen-BI-Launchpad-Einstellungen	Wenn Sie das Kontrollkästchen aktivieren, werden die Benutzergruppen-BI-Launchpad-Einstellungen des Quellsystems und die Standardeinstellungen im Zielsystem festgelegt.

Benutzergruppen-BI-Einstellungen

Benutzergruppen-BI-Einstellungen	Beschreibung
Benutzergruppen-BI-Einstellungen überschreiben	Wenn Sie das Kontrollkästchen aktivieren, werden die Benutzergruppen-BI-Launchpad-Einstellungen des Quellsystems und die Standardeinstellungen im Zielsystem festgelegt. **ⓘ Hinweis** Wenn Sie ein Web-Intelligence-Dokument hochstufen, das mittels einer BIAR-Datei angepasst wurde, sollten Sie diese Option aktivieren, um die Anpassungen zu importieren.

Föderations-Aufträge

Föderations-Aufträge	Beschreibung
Föderations-Aufgabenbeziehungen einbeziehen	Sie importieren die ausgewählten Objekte mit ihren gepflegten Föderations-Aufgabenbeziehungen.

Konflikt bei der Namensauflösung

Konflikt bei der Namensauflösung	Beschreibung
Konflikt bei der Namensauflösung	Wenn ein ausgewähltes Objekt denselben Namen wie ein Objekt im Zielsystem besitzt, jedoch eine abweichende CUID, wird eine Kopie des ausgewählten Objekts im Zielsystem angelegt. Wenn Sie diese Option nicht aktivieren, wird das ausgewählte Objekt, dessen Name, nicht jedoch die CUID mit einem Objekt im Zielsystem übereinstimmt, nicht in das Zielsystem kopiert.

36.1.8.4.2.2 Selektiven Inhalt hochstufen

Gehen Sie wie folgt vor, um selektive Inhalte aus einem Quellsystem in das Zielsystem hochzustufen:

1. Wählen Sie *Selektive Hochstufung des Inhalts*.
2. Wählen Sie *Optionen*, um die *Exportoptionen* zu definieren.
3. (Optional) Aktivieren Sie die Option *Zeitfilter anwenden*, wenn Sie Objekte nach Datum und Zeitbereich filtern möchten.
4. Wählen Sie die zu exportierenden Objekte aus.
5. Um die Abhängigkeiten eines Objekts auszuwerten, aktivieren Sie das zugehörige Kontrollkästchen unterhalb des Abhängigkeitssymbols.

   > ⓘ Hinweis
   >
   > Standardmäßig sind alle Abhängigkeiten ausgewählt. Wenn Sie die Abhängigkeiten eines Objekts nicht auswerten möchten, deaktivieren Sie das Kontrollkästchen.

6. Wählen Sie *Weiter*, um die Abhängigkeiten auszuwerten.

36.1.8.5 Abhängigkeiten

Beim Hochstufen von selektivem Inhalt aus einem Quell- in ein Zielsystem können die Abhängigkeiten des selektiven Inhalts ausgewertet werden. Der Schritt *Abhängigkeiten* bietet eine Übersicht über die ausgewählten Objekte, die als Abhängigkeiten identifiziert werden.

Sie können folgende Informationen zu den Abhängigkeiten der ausgewählten Objekte anzeigen:

- Titel
- CUID
- Datum

Sie können als Abhängigkeiten identifizierte Objekte wie folgt auswählen:

1. Abhängig davon, welche Detailebene Sie anzeigen möchten, führen Sie einen der folgenden Schritte aus:

- Wählen Sie *Alles aufklappen*, um die Details jeder Abhängigkeit anzuzeigen.
- Wählen Sie *Alles zuklappen*, um nur die abhängigen Objekte anzuzeigen.

2. Wählen Sie die Abhängigkeiten aus, die Sie hochstufen möchten.

> **Hinweis**
>
> Standardmäßig sind alle Abhängigkeiten ausgewählt. Wenn Sie die Abhängigkeiten eines Objekts nicht hochstufen möchten, deaktivieren Sie das Kontrollkästchen.

3. Wählen Sie *Weiter*, um die für die Hochstufung ausgewählten Objekte zu prüfen.

36.1.8.6 Zusammenfassung

Bevor Sie die Hochstufung ausführen, müssen Sie die Objekte prüfen, die Sie für die Hochstufung ausgewählt haben.

Sie können die folgenden Informationen zu jedem Objekt anzeigen:

- Titel
- CUID
- Datum

> **Achtung**
>
> Stellen Sie sicher, dass alle Objekte enthalten sind, die Sie kopieren möchten, da Sie den Hochstufungsprozess nach Beginn der Hochstufung nicht abbrechen können. Der Hochstufverwaltungs-Assistent unterstützt kein Rollback.

Sie können die Objekte prüfen:

1. Abhängig davon, welche Detailebene Sie prüfen möchten, führen Sie einen der folgenden Schritte aus:
   - Wählen Sie *Alles aufklappen*, um die Details jedes Objekts anzuzeigen.
   - Wählen Sie *Alles zuklappen*, um das übergeordnete Objekt zu jedem Objekt anzuzeigen.

   > **Hinweis**
   >
   > Die Detailebene in der CSV-Datei mit den Hochstufungsergebnissen variiert abhängig davon, ob Sie *Alles aufklappen* oder *Alles zuklappen* ausgewählt haben.

2. Um sicherzustellen, dass auf Ihrer Festplatte ausreichender Speicherplatz für die Hochstufung verfügbar ist, prüfen Sie *Benötigter temporärer Mindestspeicherplatz*.
3. Klicken Sie auf *Start*, um die Objekte hochzustufen.

   Nachdem Sie die Hochstufung gestartet haben, können Sie den Prozess nicht mehr abbrechen.

36.1.8.7 (Optional) Eigenschaftendatei

Sie können folgende Parameter in der Eigenschaftendatei des Hochstufverwaltungs-Assistenten konfigurieren:

- SSL-Einstellungen
- Parameter

Die Eigenschaftendatei des Hochstufverwaltungs-Assistenten liegt unter: `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`.

36.1.8.7.1 SSL-Einstellungen konfigurieren

Wenn Sie SSL verwenden, müssen Sie die SSL-Einstellungen des Hochstufverwaltungs-Assistenten unter folgendem Pfad konfigurieren:

`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

1. Öffnen Sie die `PromotionManagementWizard.ini` in einem Texteditor.
2. Um den SSL-Modus zu aktivieren, entkommentieren Sie die Zeilen, die mit "-D" beginnen.
3. Geben Sie die Werte für jede Einstellung ein.

Einstellung	Wert
`-Dbusinessobjects.orb.oci.protocol`	Wert: ssl **Hinweis** Bei Eingabe dieses Werts wird die SSL-Kommunikation aktiviert.
`-DcertDir`	Der Speicherort von Schlüsseln und Zertifikaten
`-DtrustedCert`	Der Name der Datei mit dem vertrauenswürdigen Zertifikat **Hinweis** Wenn Sie mehrere Dateien angeben, trennen Sie diese durch ein Semikolon (zum Beispiel DateiA; DateiB).
`-DsslCert`	Das SDK-Zertifikat
`-DsslKey`	Der private Schlüssel des SDK-Zertifikats
`-Dpassphrase`	Der Speicherort der Datei, die den Kennsatz für den privaten Schlüssel enthält.
`-Dpsecert`	Die PSE-Zertifikatdatei

> ⚠ Achtung
>
> Fügen Sie keine anderen Einstellungen oder Werte hinzu, und bearbeiten Sie die Einstellungen und Werte nicht.

4. Speichern Sie die Datei `PromotionManagementWizard.ini`.

Beispiel: SSL-Einstellungen in `PromotionManagementWizard.ini`

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:/SSL
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dpsecert=temp.pse
```

36.1.8.7.2 Parameter konfigurieren

Sie können die Optionen des Hochstufverwaltungs-Assistenten unter folgendem Pfad Ihren Anforderungen entsprechend in der Eigenschaftendatei konfigurieren:

`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

1. Öffnen Sie die `PromotionManagementWizard.ini` in einem Texteditor.
2. Um die Optionen zu aktivieren, entkommentieren Sie die Zeilen, die mit "-D" beginnen.
3. Geben Sie die Parameter für jede Einstellung ein.

Parameter	Wert
`-Dbusinessobjects.connectivity.directory`	Der Speicherort des Connection-Server-Verzeichnisses
`-Dcom.businessobjects.mds.cs.ImplementationID`	`csEX` ⓘ Hinweis Dieser Wert darf nicht geändert oder bearbeitet werden.
`-Xms8g`	Der Speicherwert ist standardmäßig auf 8 GB festgelegt. Der Wert "Xms" muss kleiner als der Wert "Xmx" sein oder diesem entsprechen.
`-Xmx10g`	Der Speicherwert ist standardmäßig auf 10 GB festgelegt.

Parameter	Wert
	Ein Speicher von 10 GB ist ausreichend für ein Repository mit 65.000 Objekten.
`-Dbobj.biar.suggestSplit=512`	Standardwert (empfohlen) Es wird empfohlen, den Parameter `-Dbobj.biar.suggestSplit` zu verwenden. Wenn Sie Objekte von einem Live-CMS in eine LCMBIAR-Datei hochstufen, können Sie die LCMBIAR-Datei mit dieser Einstellung in mehrere LCMBIAR-Dateien aufteilen.
`-Dbobj.biar.forceSplit=768`	Standardwert (empfohlen) Wenn der Parameter `-Dbobj.biar.suggestSplit` nicht angewendet werden kann, dient der Parameter `-Dbobj.biar.forceSplit` als Fallback-Lösung.
`-Dcom.businessobjects.lcm.commit`	• `KEEP_TS`: Standardwert. Mit diesem Wert können Sie das Änderungsdatum der Quelle beibehalten. • `LEGACY`: Das Änderungsdatum entspricht dem Ausführungsdatum im Zielsystem. Dies entspricht dem Standardverhalten von BI vor 4.2 SP 5.
`-Dcom.sap.businessobjects.pmw.exclude.list`	Mit diesem Parameter können Sie Objekte dauerhaft ausschließen, wenn Sie Objekte aus einem Quellsystem in ein Zielsystem hochstufen oder aus einem Quellsystem in eine LCMBIAR-Datei exportieren. Der Wert (CUID) kann einem Objekt entsprechen (Dokument, Ordner, usw.). Wenn Sie einen Ordner angeben, werden alle untergeordneten Elemente des Ordners ausgeschlossen.

4. Speichern Sie die Datei `PromotionManagementWizard.ini`.

Beispiel: Optionen des Hochstufverwaltungs-Assistenten in `PromotionManagementWizard.ini`

```
-Dbusinessobjects.connectivity.directory=C:\Program Files (x86)\SAP
BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer
-Dcom.businessobjects.mds.cs.ImplementationID=csEX
-Xms2g
-Xmx10g
-Dbobj.biar.suggestSplit=512
-Dcom.businessobjects.lcm.commit=KEEP_TS
-Dcom.sap.businessobjects.pmw.exclude.list="c:/
PromotionManagementWizardExcludedItems.txt"
# Exclusion List AY2ygq4hFJhJmZMQNlQh8OI # Report Samples
AeN4lEu0h_tAtnPEjFYxwi8 # WebIntelligence Samples
```

36.1.8.8 Hochstufverwaltungs-Assistent unter Linux

Sie können den Hochstufverwaltungs-Assistenten unter Linux ausführen.

Bevor Sie den Hochstufverwaltungs-Assistenten unter Linux starten, stellen Sie sicher, dass Sie die Java-Laufzeitumgebung in der Systemvariable `PATH` festgelegt haben.

Gehen Sie wie folgt vor, um den Hochstufverwaltungs-Assistenten unter Linux zu starten:

1. Öffnen Sie eine Shell, und navigieren Sie zum Installationsverzeichnis, zum Beispiel:

   ```
   /usr/sap_bobj/enterprise_xi40
   ```

2. Führen Sie den folgenden Befehl aus:

   ```
   ./PromotionManagementWizard
   ```

   Der Hochstufverwaltungs-Assistent wird gestartet.

   Weitere Details zur Verwendung von SSH und dem X11-Forwarding finden Sie in Ihrer Betriebssystemdokumentation.

36.2 Versionsverwaltung

36.2.1 Mehrere Versionen von BI-Ressourcen verwalten

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.

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“.
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 im CMS sind nicht davon betroffen.

   > **Hinweis**
   >
   > Wenn Sie ein InfoObject sperren, können Sie keine Aktionen für dieses InfoObject ausführen.

10. Wenn die Version auf dem CMS neuer ist als die Version auf dem VMS, wird dies neben dem aktualisierten InfoObject gekennzeichnet. 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.
13. Sie können in der *Versionsverwaltung* nach BI-Assets suchen. Mithilfe der Optionen *Alle Felder suchen*, *Titel suchen*, *Schlüsselwort suchen* und *Beschreibung suchen* können Sie die Suche eingrenzen und auf diese Weise beschleunigen.

    > **Hinweis**
    >
    > Die Suchfunktion in der *Versionsverwaltung* ist kontextspezifisch. Wenn Sie beispielsweise einen Ordner wie *Auditing* auswählen und nach einer bestimmten Zeichenfolge suchen, sucht die BI-

> Plattform ausschließlich im Ordner *Auditing*. Wenn Sie stattdessen *Alle Ordner* auswählen und eine Suche durchführen, sucht die BI-Plattform in allen Ordnern nach dem InfoObject.

36.2.2 Apache Subversion als Versionsverwaltungssystem verwenden

Sie können Apache Subversion als Versionsverwaltungssystem festlegen und die entsprechenden Einstellungen in der Central Management Console konfigurieren.

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`
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.

36.2.3 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.

36.2.4 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 4.2 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:/Program Files (x86)/SAP BusinessObjects/SAPBusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository" < c:/dumrepo
   ```

   ```
   svnadmin.exe upgrade "C:/Program Files (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.
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.

Weitere Informationen zum Upgrade von Apache Subversion finden Sie in den Apache Subversion 1.10 Release Notes (Englisch).

Ausschlussklauseln und rechtliche Aspekte

Hyperlinks

Einige Links werden durch ein Symbol und/oder einen Quick-Info-Text klassifiziert. Über diese Links erhalten Sie weitere Informationen.
Informationen zu den Symbolen:

- Links zum Symbol : Sie rufen eine Website auf, die nicht von SAP gehostet wird. Durch die Nutzung solcher Links stimmen Sie Folgendem zu (sofern sich nicht aus Ihren Vereinbarungen mit SAP etwas anderes ergibt):
  - Der Inhalt der verlinkten Site ist keine SAP-Dokumentation. Basierend auf diesen Informationen ergibt sich für Sie keinerlei Produkthaftungsanspruch gegen SAP.
  - Weder widerspricht SAP dem Inhalt auf der verlinkten Site noch stimmt SAP ihm zu. Außerdem übernimmt SAP keine Gewährleistung für dessen Verfügbarkeit und Richtigkeit. SAP übernimmt keine Haftung für Schäden, die durch die Nutzung solchen Inhalts verursacht wurden, es sei denn, dass diese Schäden von SAP grob fahrlässig oder vorsätzlich verursacht wurden.
- Links zum Symbol : Sie verlassen die Dokumentation für das jeweilige SAP-Produkt oder den jeweiligen SAP-Service und rufen eine von SAP gehostete Website auf. Durch die Nutzung solcher Links stimmen Sie zu (sofern sich nicht aus Ihren Vereinbarungen mit SAP etwas anderes ergibt), dass sich basierend auf diesen Informationen für Sie keinerlei Produkthaftungsanspruch gegen SAP ergibt.

Videos, die auf externen Plattformen gehostet werden

Einige Videos verweisen möglicherweise auf Video-Hosting-Plattformen von Drittanbietern. SAP kann die zukünftige Verfügbarkeit von Videos, die auf diesen Plattformen gespeichert sind, nicht garantieren. Außerdem unterliegen alle Werbungen und anderen Inhalte, die auf diesen Plattformen gehostet werden (z.B. empfohlene Videos oder Navigation zu anderen gehosteten Videos auf derselben Site), nicht der Kontrolle oder Verantwortlichkeit von SAP.

Beta und andere experimentelle Funktionen

Experimentelle Funktionen sind nicht Teil des offiziellen Lieferumfangs, den SAP für künftige Releases garantiert. Dies bedeutet, dass experimentelle Funktionen von SAP jederzeit, aus beliebigen Gründen und ohne vorherige Ankündigung geändert werden können. Experimentelle Funktionen sind nicht zur Nutzung in einem Produktivsystem vorgesehen. Die experimentellen Funktionen dürfen nicht für Demonstrationen, Tests, Untersuchungen, Bewertungen oder anderweitige Zwecke in einer Produktivumgebung oder in Verbindung mit Daten, die nicht ausreichend gesichert wurden, verwendet werden.
Der Zweck der experimentellen Funktionen besteht darin, frühzeitig Feedback zu erhalten und so Kunden und Partnern die Möglichkeit zu geben, das zukünftige Produkt entsprechend zu beeinflussen. Durch die Abgabe von Feedback (z.B. über SAP Community) stimmen Sie zu, dass die geistigen Eigentumsrechte der Beiträge oder daraus abgeleiteten Werke im ausschließlichen Besitz von SAP verbleiben.

Beispielcode

Bei dem Quelltext und/oder den Code-Snippets handelt es sich ausschließlich um beispielhafte Darstellungen. Sie sind nicht zur Nutzung in einem Produktivsystem vorgesehen. Der Beispielcode dient ausschließlich dem Zweck, Syntax- und Verphrasungsregeln besser zu erläutern und zu visualisieren. SAP übernimmt keine Gewährleistung für die Richtigkeit und Vollständigkeit des Beispielcodes. SAP übernimmt keine Haftung für Fehler oder Schäden, die durch die Nutzung des Beispielcodes verursacht wurden, es sei denn, dass diese Fehler oder Schäden von SAP grob fahrlässig oder vorsätzlich verursacht wurden.

Vorurteilsfreie Sprache

SAP unterstützt eine Kultur der Vielfalt und Integration. Wann immer möglich, verwenden wir in unserer Dokumentation unvoreingenommene Sprache, um auf Menschen aller Kulturen, ethnischen Zugehörigkeiten, Geschlechter und Fähigkeiten zu verweisen.

www.sap.com/contactsap

© 2024 SAP SE 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 SAP SE oder ein SAP-Konzernunternehmen nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.

Die von SAP SE oder deren Vertriebsfirmen angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehersteller enthalten. Produkte können länderspezifische Unterschiede aufweisen.

Die vorliegenden Unterlagen werden von der SAP SE oder einem SAP-Konzernunternehmen bereitgestellt und dienen ausschließlich zu Informationszwecken. Die SAP SE oder ihre Konzernunternehmen übernehmen keinerlei Haftung oder Gewährleistung für Fehler oder Unvollständigkeiten in dieser Publikation. Die SAP SE oder ein SAP-Konzernunternehmen steht lediglich für Produkte und Dienstleistungen nach der Maßgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt ist. Keine der hierin enthaltenen Informationen ist als zusätzliche Garantie zu interpretieren.

SAP und andere in diesem Dokument erwähnte Produkte und Dienstleistungen von SAP sowie die dazugehörigen Logos sind Marken oder eingetragene Marken der SAP SE (oder von einem SAP-Konzernunternehmen) in Deutschland und verschiedenen anderen Ländern weltweit. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen.

Zusätzliche Informationen zur Marke und Vermerke finden Sie auf der Seite https://www.sap.com/germany/about/legal/trademark.html.

THE BEST RUN SAP