IBM Cognos Analytics
Version 11.1.x

Installation & Konfiguration

©

Produktinformation

Dieses Dokument bezieht sich auf IBM Cognos Analytics Version 11.1.0 und gegebenenfalls auch auf nachfolgende Releases des Produkts.

Copyright

Licensed Materials - Property of IBM

© Copyright IBM Corp. 2015, 2021.

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der International Business Machines Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Herstellern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Website " Copyright and trademark information " unter www.ibm.com/legal/copytrade.shtml.

Die folgenden Namen sind Marken oder eingetragene Marken anderer Unternehmen:

- Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.
- Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.
- Intel, das Intel-Logo, Intel Inside, das Intel Inside-Logo, Intel Centrino, das Intel Centrino-Logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium und Pentium sind Marken oder eingetragene Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA oder anderen Ländern.
- Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.
- UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.
- Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

© Copyright International Business Machines Corporation .

Inhaltsverzeichnis

Kapitel 1. Vorbereiten der Installation..... 1
Überprüfen der unterstützten Umgebungen.....1
Überprüfen der Systemanforderungen..... 1
Speichereinstellungen.....3
Java-Anforderungen..... 4
Überprüfen der Standardporteinstellungen.....5
Richtlinien zum Erstellen des Content Store.....7
Empfohlene Einstellungen für die Erstellung des Content Store in IBM Db2 unter Linux, Windows und UNIX.....7
Empfohlene Einstellungen für die Erstellung des Content Store in IBM Db2 unter z/OS 9
Empfohlene Einstellungen für die Erstellung des Content Store in Oracle..... 10
Empfohlene Einstellungen für die Erstellung des Content Store in Microsoft SQL Server.....11
Vorgeschlagene Einstellungen für die Erstellung des Content Store im Datenbankserver von IBM Informix..... 12
Konfigurieren eines Benutzer- oder Netzservicekontos für IBM Cognos Analytics.....12
Web-Browser konfigurieren.....13

Kapitel 2. "Easy Install".....17

Kapitel 3. Einzelserverinstallation.....19

Kapitel 4. Verteilte Serverinstallation.....23
Installation der Inhaltsebene.....24
Installation der Anwendungsebene..... 27
Installation der Gatewayebene..... 28

Kapitel 5. Unbeaufsichtigte Installation, Deinstallation und Konfiguration..... 31
Verwenden einer unbeaufsichtigten Installation.....31
Verwenden einer Antwortdateivorlage..... 33
Verwenden einer unbeaufsichtigten Konfiguration..... 35
Verwenden einer unbeaufsichtigten Deinstallation.....36

Kapitel 6. Installation von IBM Cognos Analytics for Jupyter Notebook Server..... 39
Hardwarevoraussetzungen für Jupyter Notebook Server..... 39
Installation von Jupyter Notebook Server unter Linux.....40
Deinstallieren von Jupyter Notebook Server.....42
Installation von Jupyter Notebook Server unter Microsoft Windows 10.....42
Deinstallieren von Jupyter Notebook Server.....45
Installieren eines PiP-Pakets in einer Linux-Offlineumgebung.....45
Installieren eines PiP-Pakets in einer Windows-Offlineumgebung..... 46
Jupyter Notebook Server konfigurieren.....47
Konfigurieren des Cognos Analytics-Gateways für Jupyter Notebook Server..... 49
Jupyter Notebook Server schützen.....49
Upgrade für IBM Cognos Analytics for Jupyter Notebook Server..... 51
Upgrade der Installation für Linux..... 51
Upgrade der Installation für Microsoft Windows..... 52
Upgrades für Python-Pakete und R-Pakete.....52
Hinzufügen zusätzlicher Ubuntu-Betriebssystempackages..... 53
Fehlerbehebung für IBM Cognos Analytics for Jupyter Notebook Server..... 54

Kapitel 7. Verteilungsoptionen..... 55
Cognos Analytics-Komponenten..... 55
Serverkomponenten..... 55
Modellierungskomponenten..... 57
Erforderliche Datenbankkomponenten..... 59
Verteilen von Komponenten..... 59
Komponenten der Anwendungsebene und Content Manager auf separaten Computern..... 60
Konsolidieren von Servern für Linux auf System z..... 62
Installation für optionale Modellierungskomponenten..... 62
Hinweise zu Firewalls..... 62
Verteilen von Framework Manager-Komponenten..... 64
Verteilen von Transformer-Komponenten..... 64
IBM Cognos Analytics in Kombination mit anderen IBM Cognos-Produkten..... 66
IBM Cognos-Produkte, die in Kombination mit IBM Cognos Analytics verwendet werden können..... 67

Kapitel 8. Upgrade für Cognos Analytics..... 69
Upgrade für die aktuelle Version von Cognos Analytics 11..... 69
Datenaktualisierungstasks für Cognos Analytics Version 11.1..... 69
Dienstprogramm 'ParquetMigrate' ausführen..... 70
Beim Cognos Analytics-Upgrade beibehaltene Dateien und Ordner..... 72
Standardaktualisierungsprozess..... 74
Lesen der Dokumentation..... 76
Bewerten von Anwendungen in Ihrer Umgebung vor einer Aktualisierung..... 76
Installieren und Konfigurieren einer neuen Produktversion..... 77
Verschieben des Inhalts in die neue Produktversion..... 80
Upgrade des Content Store..... 81
Verschieben des Inhalts mit einem Bereitstellungsarchiv..... 82
Vergleichen von Berichten zwischen Produktversionen mithilfe von Lifecycle Manager..... 85

Kapitel 9. Konfigurieren von Serverkomponenten..... 87
Installationsreihenfolge für Serverkomponenten..... 89
Empfehlung - Installation und Konfiguration der Basisinstallation für verteilte Installationen..... 90
Installationsmodi..... 90
Installieren von Serverkomponenten unter UNIX oder Linux..... 91
Installieren von Serverkomponenten unter Windows..... 91
Installieren und Konfigurieren von Content Manager für das Inhaltsrepository..... 92
Aktive und Standby-Instanzen von Content Manager..... 93
Installieren von Content Manager unter UNIX oder Linux..... 94
Installieren von Content Manager unter Windows..... 95
Einrichten der Datenbankverbindung für die Content Store-Datenbank..... 96
Kritische Konfigurationsaktionen, die zuerst erledigt werden müssen!..... 102
Starten von IBM Cognos Configuration..... 103
Erstellen der Datenbankverbindungseigenschaften für den Content Store..... 103
Konfigurieren von Umgebungseigenschaften für Content Manager-Computer..... 107
Angeben einer Verbindung zu einem E-Mail-Server..... 108
Aktivieren der Sicherheit..... 110
Starten von Content Manager..... 110
Testen der Content Manager-Installation..... 111
Installieren und Konfigurieren der Anwendungsservices..... 111
Installieren der Anwendungsservicekomponenten..... 111
Einrichten der Datenbankverbindung für die Berichtsdatenbanken..... 113
Starten von IBM Cognos Configuration..... 116
Konfigurieren von Umgebungseigenschaften für Computer mit Anwendungsservicekomponente..... 117
Aktivieren der 64-Bit-Version des Berichtsservers..... 118

Starten der Anwendungsservicekomponenten....119
Testen der Anwendungsservicekomponenten....119

Kapitel 10. Konfigurieren des Gateways....121
Installieren des Cognos Analytics-Gateways....121
Cognos Analytics mit Ihrem Web-Server konfigurieren....122
32-Bit-Web-Gateway aktivieren....123
Dispatcher-URIs konfigurieren....124
Apache HTTP Server oder IBM HTTP Server konfigurieren....125
Konfigurieren von IBM HTTP Server V9....125
Konfigurieren von WebDAV auf einem IBM HTTP Server oder auf einem Apache HTTP Server....129
IBM HTTP Server mit SSL verwenden....130
Konfigurieren von Apache HTTP Server oder IBM HTTP Server für Cognos Analytics....133
Konfigurieren von Cognos Analytics mit Apache HTTP Server oder IBM HTTP Server....134
Lastausgleich für den Apache-Web-Server....135
Aktivieren von HTTP/2 für einen Web-Server....135
Konfigurieren Sie Microsoft Internet Information Services....136
Konfigurieren von WebDAV auf IIS....136
Konfigurieren von IIS mit SSL....138
Konfigurieren von IIS in Cognos Analytics....138
Konfigurieren des CGI-Gateways in IIS Version 7 oder neueren Versionen....144
Konfigurieren des Gateways und Web-Servers für die Verwendung bestimmter Namespaces....147
Konfigurieren eines Namespace, der mit IIS verwendet werden soll....147
Konfigurieren eines Namespace, der mit Apache oder IBM HTTP Server verwendet werden soll 148
Konfigurieren eines Gateway-Namespace....148
Gateway testen....149

Kapitel 11. Konfigurieren von optionalen Modellierungskomponenten....151
IBM Cognos Framework Manager....151
Systemanforderungen für IBM Cognos Framework Manager....151
Installieren von IBM Cognos Framework Manager....152
Konfigurieren von IBM Cognos Framework Manager....153
Festlegen von Variablen für Datenquellenverbindungen für Framework Manager....155
Testen der Framework Manager-Installation....157
IBM Cognos Transformer....157
Systemanforderungen für Cognos Transformer....158
Installieren von IBM Cognos Transformer....158
Konfigurieren der Kommunikation zwischen Transformer und Cognos Analytics....161
Einrichten von Datenquellen für Transformer....162
Testen der Transformer-Installation....164
Zusätzliche Konfigurationsaufgaben für Cognos Transformer....164

Kapitel 12. Konfigurationsoptionen....169
Starten von IBM Cognos Configuration....169
Kritische Konfigurationsaktionen, die zuerst erledigt werden müssen!....169
Ändern der von IBM Cognos Analytics-Komponenten verwendeten Java-Version....170
Ändern der Standardkonfigurationseinstellungen....171
Port- und URI-Einstellungen....172
Konfigurationseinstellungen überprüfen....174
Verwalten der Konfigurationsgruppe....175
Konfigurieren von kryptografischen Einstellungen....178
IBM Cognos Application Firewall....181
Verschlüsseln der Eigenschaften von temporären Dateien....183
Aktivieren und inaktivieren von Services....183
Konfigurieren von Abfrageeinstellungen....184
Konfiguration von Schriftarten....188
Ändern der Standardschriftart für PDF-Berichte....191

Konfigurieren der in PDF-Berichten eingebetteten Schriftarten ... 191
Gespeicherte Berichtsausgabe ... 192
Ändern des Verzeichnisses für die temporäre Berichtsausgabe ... 194
Position der traditionellen Map Manager-Landkarten für Reporting ändern ... 195
Ändern der Position von Datendateien ... 195
Optimieren von WebSphere Liberty Profile ... 196
Aktivieren der Sitzungsreplikation für Content Manager-Bereitschaftsservices ... 196
Verwenden eines externen Objektspeichers für Berichtsausgabe und Datasets ... 197
Überprüfen des Zugriffs auf den externen Objektspeicher ... 198
Anpassen des serverseitigen Drucks unter UNIX und Linux ... 198
Ändern der Benachrichtigungsdatenbank ... 199
Empfohlene Einstellungen für die Erstellung einer Benachrichtigungsdatenbank in IBM Db2 unter z/OS ... 200
Erstellen von Tabellenbereichen für eine Benachrichtigungsdatenbank für IBM Db2 für z/OS ... 200
Ändern der Verbindungseigenschaften für die Benachrichtigungsdatenbank ... 201
Zertifikatsmanagement in Cognos Analytics ... 202
ThirdPartyCertificateTool – Befehle und Verwendungsbeispiele ... 202
Konfigurieren von Cognos Analytics-Komponenten für die Verwendung einer anderen Zertifizierungsstelle ... 204
Konfigurieren des SSL-Protokolls für Cognos Analytics-Komponenten ... 208
Konfigurieren von SSL für Cognos Analytics-Komponenten ... 209
Gemeinsame Vertrauenswürdigkeit von Cognos Analytics-Servern und anderen Servern aktivieren ... 211
Auswählen und Einstufen von Cipher Suites für SSL ... 212
Verwendung des SSL-Protokolls für die Datenbankkommunikation ... 213
Aktivieren von SSL für die Kommunikation mit Db2- und Informix-Datenbanken ... 213
Aktivieren von SSL für die Kommunikation mit Microsoft SQL Server-Datenbanken ... 215
Aktivieren von SSL für die Kommunikation mit Oracle-Datenbanken ... 217
Schützen von JDBC-Datenservern mit SSL ... 218
Konfigurieren von JDBC-Datenservern für Single Sign-on mit Kerberos ... 218
Erstellen von Kerberos-Initialisierungsdateien ... 219
Erstellen eines SPN für den Abfrageservice ... 220
Erstellen einer Chiffrierschlüsseldatei ... 220
Konfigurieren des Kerberos-Anmeldemoduls ... 221
Verifizieren der Kerebos-Konfiguration ... 221
Verifizieren der JDBC-Treiberfunktionen ... 222
Konfigurieren von Datenserververbindungen für Single Sign-on mit Kerberos ... 222
Konfigurieren eines Repositorys für Protokollnachrichten ... 224
Richtlinien zum Erstellen einer Protokolldatenbank ... 225
Datenbankverbindungen für die Protokolldatenbank ... 227
Repositorys für Protokollnachrichten ... 228
Aktivieren der benutzerspezifischen Protokollierung ... 234
Ändern globaler Einstellungen ... 235
Anpassen der Sprachunterstützung an die Benutzeroberfläche ... 236
Anpassen der Währungsunterstützung ... 236
Anpassen der Unterstützung von Inhaltsländereinstellungen ... 237
Inhaltsländereinstellungen ... 238
Verknüpfen einer Produktländereinstellung ... 240
Anpassen der Zeitzone für den Server ... 240
Codierung für E-Mail-Nachrichten ... 241
Anpassen von Cookieeinstellungen ... 242
Ändern der IP-Adressversion ... 243
Festlegen der IP-Version ... 244
Manuelles Konfigurieren von IBM Cognos Configuration zum Starten mit der Option IPv6 ... 244
Konfigurieren von IBM Cognos Configuration, sodass es unter Windows immer mit der Option IPv6 gestartet wird ... 244
Konfigurieren des Collaboration Discovery-URI ... 244
Konfigurieren von IBM Cognos Workspace ... 245

Konfigurieren des Zugriffs auf IBM Cognos Workspace oder zugehörige Funktionen..... 246
Konfigurieren unterstützter MIME-Typen in Microsoft Internet Information Services..... 247
Erstellen von Tabellenbereichen für die Datenbank für benutzergeführte Aufgaben und Anmerkungen für IBM Db2 unter z/OS..... 247
Einrichten einer Datenbank für benutzergeführte Aufgaben und Anmerkungen..... 249
Konfigurieren von IBM Cognos Workspace für die Verwendung von IBM Cognos TM1-Daten..... 250
Ändern des Stils von Berichtsobjekten in IBM Cognos Workspace..... 253
Zugreifen auf die Beispiele für IBM Cognos Workspace..... 253
Konfigurieren des Routers für das Testen der Dispatcher-Verfügbarkeit..... 253
Konfigurieren von IBM Cognos Analytics zur Zusammenarbeit mit anderen IBM Cognos-Produkten. 253
Aktivieren von geplanten Berichten und Agenten für IBM Cognos Planning Contributor-Datenquellen..... 254
Konfigurieren des Software Development Kit..... 254

Kapitel 13. Konfigurieren von Authentifizierungsprovidern 257
Inaktivierung der anonymen Anmeldung..... 258
Beschränken des Benutzerzugriffs auf den Cognos-Namespace..... 258
Konfigurieren der Lightweight Third Party Authentication..... 259
Konfigurieren von LTPA mit einem LDAP-Namespace..... 260
Konfigurieren von LTPA mit einem Active Directory-Namespace..... 262
Konfigurieren von IBM Cognos-Komponenten für die Verwendung von Active Directory Server..... 263
Konfigurieren eines Active Directory-Namespace..... 264
Bereitstellen von benutzerdefinierten Active Directory-Benutzereigenschaften für IBM Cognos-Komponenten..... 265
Aktivieren der sicheren Kommunikation mit dem Active Directory Server 265
Ein- oder Ausschließen von Domänen, die erweiterte Eigenschaften verwenden..... 266
Aktivieren der Einzelanmeldung zwischen Active Directory Server und IBM Cognos-Komponenten..... 267
OpenID Connect-Authentifizierungsprovider..... 270
Konfigurieren eines OpenID Connect-Namespace 271
OIDC-Providertyp 'IBMid'..... 272
Generischer OIDC-Providertyp..... 273
OpenID Connect-Identitätsprovider mit SSO-Unterstützung..... 274
Konfigurieren von IBM Cognos für die Verwendung eines benutzerdefinierten Java-Authentifizierungsproviders..... 274
Konfigurieren eines benutzerdefinierten Java-Authentifizierungsnamespace..... 275
Ausblenden des Namespace von Benutzern während der Anmeldung..... 275
OpenID Connect-Authentifizierungsproxy 276
Konfigurieren von IBM Cognos für die Verwendung von IBM Cognos Series 7-Namespaces..... 276
Konfigurieren eines IBM Cognos Series 7-Namespace..... 277
Aktivieren der sicheren Kommunikation mit dem Verzeichnisserver, der vom IBM Cognos Series 7-Namespace verwendet wird..... 278
Aktivieren von Single Sign-on zwischen IBM Cognos Series 7 und IBM Cognos 278
IBM Cognos Series 7-Namespaces und IBM Cognos Series 7-Trusted-Signon-Plug-in..... 278
Konfigurieren von IBM Cognos-Komponenten für die Verwendung von LDAP..... 280
LDAP-Zuordnung..... 281
Konfigurieren eines LDAP-Namespace..... 282
Konfigurieren eines LDAP-Namespace für Active Directory Server..... 283
Konfigurieren eines LDAP-Namespace für IBM Directory Server..... 284
Konfigurieren eines LDAP-Namespace für Novell Directory Server..... 285
Konfigurieren eines LDAP-Namespace für Oracle Directory Server..... 287
Bereitstellen von angepassten Benutzereigenschaften für LDAP für IBM Cognos-Komponenten. 288
Aktivieren der sicheren Kommunikation mit dem LDAP-Server 288
Aktivieren von Single Sign-on zwischen LDAP und IBM Cognos-Komponenten..... 290
Ersetzungsoperation..... 290
Konfigurieren von IBM Cognos für die Verwendung von SAP..... 291
Konfigurieren eines SAP-Namespace..... 292

Aktivieren der Einzelanmeldung zwischen SAP und IBM Cognos 293
SiteMinder-Authentifizierungsprovider.....294
Konfigurieren eines SiteMinder-Namespace.....295
Löschen eines Authentifizierungsproviders.....296

Kapitel 14. Verwalten der Leistung.....299
Systemleistungsmetriken.....299
Externes Überwachen von Systemmetriken..... 299
Aktivieren von erforderlichen Services..... 300
Optimieren eines IBM Db2-Content Store.....303
Anpassen der Speicherressourcen für den IBM Cognos-Service..... 304
Reduzieren der Zustellzeit für Berichte in einem Netz.....304
Verlängern des asynchronen Zeitlimits in Umgebungen mit hoher Benutzerlast..... 305

Kapitel 15. Manuelles Konfigurieren von IBM Cognos Analytics unter UNIX- und Linux-Betriebssystemen..... 307
Manuelles Ändern von Standardkonfigurationseinstellungen..... 307
Hinzufügen von Komponenten zur Konfiguration.....308
Manuelles Ändern verschlüsselter Einstellungen.....309
Globale Einstellungen unter UNIX- und Linux-Betriebssystemen.....310
Manuelles Ändern der globalen Einstellungen unter UNIX- und Linux-Betriebssystemen.....311
Starten und Stoppen von Cognos Analytics im Hintergrundmodus unter UNIX und Linux.....312
Starten von Cognos Analytics im Hintergrundmodus unter den Betriebssystemen UNIX und Linux.....312
Stoppen von Cognos Analytics im Hintergrundmodus unter den Betriebssystemen UNIX und Linux..... 312

Kapitel 16. Deinstallieren von IBM Cognos Analytics.....313
Deinstallieren von IBM Cognos Analytics unter UNIX oder Linux.....313
Deinstallieren von Cognos Analytics unter Microsoft Windows-Betriebssystemen.....314
Wiederherstellung nach einer nicht erfolgreichen Deinstallation.....314

Kapitel 17. IBM Cognos content archival..... 317
Inhaltsarchivierung konfigurieren.....318
Dateiposition für ein Dateisystemrepository erstellen..... 318
Angepasste Klassen-Definitionen und -Eigenschaften in IBM FileNet Content Manager importieren..... 319
Angepasste Klassen-Definitionen und -Eigenschaften in IBM Content Manager 8 importieren.....320
Zur Verfügung stehende Zeit für die Ausführung des Archivierungsprozesses angeben..... 321
Threadausführungszeit angeben..... 321
Ausgewählte Formate von Berichtsausgaben archivieren.....322
Angeben, dass Berichtsspezifikationen nicht archiviert werden.....323

Anhang A. Befehlszeilenoptionen für IBM Cognos Configuration.....325

Anhang B. Fehlerbehebung..... 327
Fehlerbehebung bei Problemen.....327
Durchsuchen von Wissensbasen..... 329
Fixes abrufen.....329
Kontaktaufnahme zum IBM Support.....330
Austauschen von Informationen mit IBM..... 331
Abonnieren von Support-Aktualisierungen 332
Protokolldateien..... 333

Anhang C. Informationen zu diesem Handbuch.....337

Index..... 339

Kapitel 1. Vorbereiten der Installation

Vor der Installation von IBM® Cognos Analytics müssen Sie in Ihrer Umgebung Ressourcen einrichten, damit die Komponenten ausgeführt werden können. Sie müssen beispielsweise eine Datenbank für die Verwendung als Cognos Analytics-Content Store sowie ein Benutzerkonto für Cognos Analytics erstellen.

Wenn Sie die Option **Easy Install** (früher **Ready to Run!**) für die Installation von Cognos Analytics (nur unter Windows) verwenden, müssen Sie keine Content-Store-Datenbank erstellen und konfigurieren. Eine Informix-Datenbank ist bereits als Content Store konfiguriert und kann von Cognos Analytics unmittelbar verwendet werden.

Nachdem Sie diese Aufgaben abgeschlossen haben, fahren Sie mit Kapitel 9, „Konfigurieren von Server-komponenten", auf Seite 87 fort.

Überprüfen der unterstützten Umgebungen

Um sicherzustellen, dass Ihr Produkt ordnungsgemäß funktioniert, wenden Sie alle erforderlichen Programmkorrekturen für das Betriebssystem an und verwenden Sie ausschließlich die unterstützten Versionen der Software anderer Anbieter.

Eine aktuelle Liste der Umgebungen, die von den IBM Cognos Analytics Produkten unterstützt werden, einschließlich Informationen zu Betriebssystemen, Patches, Browsern, Webservern, Verzeichnisservern, Datenbankservern und Anwendungsservern, finden Sie auf der Seite IBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235).

Überprüfen der Systemanforderungen

Verwenden Sie die folgenden Tabellen, um die Mindestanforderungen im Hinblick auf Hard- und Software für die Installation und den Betrieb von IBM Cognos Analytics-Komponenten auf einem einzelnen Computer zu überprüfen. Für verteilte oder Produktionsumgebungen sind möglicherweise zusätzliche Ressourcen erforderlich.

In der folgenden Tabelle sind die Hardwarevoraussetzungen und -spezifikationen für die Installation auf einem einzelnen Computer aufgeführt.

Hardwarevoraussetzungen

Tabelle 1. Hardwarevoraussetzungen für eine Einzelcomputer-Installation

Anforderung	**Spezifikation**
Betriebssystem	Microsoft Windows UNIX Linux®
Verarbeitung	Minimum: 4 CPU-Cores pro Benutzer. Es wird dringend empfohlen, die Dimensionierung für jeden Einsatzfall zu testen.
RAM	Mindestens 10 GB. Weitere Informationen finden Sie im Abschnitt „Speichereinstellungen" auf Seite 3.
Betriebssystemspezifikationen	Grenzwert für Dateideskriptoren unter UNIX und Linux festgelegt auf 8192

Tabelle 1. Hardwarevoraussetzungen für eine Einzelcomputer-Installation (Forts.)	
Anforderung	**Spezifikation**
Plattenspeicherplatz	Es sind mindestens 7 Gigabyte freier Speicherplatz für die Softwareinstallation und 5 Gigabyte freier Speicherplatz auf dem Laufwerk erforderlich, das das von den IBM Cognos-Komponenten verwendete temporäre Verzeichnis enthält. Eine Umgebungsvariable zeigt auf das temporäre Verzeichnis. Bei Windows lautet diese Variable TMP. Bei UNIX und Linux lautet diese Variable IATEMPDIR. Alle Datenbanken werden im Laufe der Zeit größer. Stellen Sie sicher, dass der freie Plattenspeicherplatz auch zukünftigen Anforderungen genügt.
Drucker	Zum Sicherstellen, dass Berichte unter Windows ordnungsgemäß ausgedruckt werden, müssen Sie aufgrund der Anforderungen von Adobe Reader mindestens einen Drucker auf dem Computer konfigurieren, auf dem Sie die Komponenten der Anwendungsebene installieren. Alle Berichte werden unabhängig vom Druckformat, das Sie auswählen, zum Ausdrucken als temporäre PDF-Dateien an Adobe Reader gesendet.
E-Mail-Server	Zum Senden von Berichten per E-Mail müssen der Zugriff auf einen E-Mail-Server und dessen Nutzung möglich sein.

Softwarevoraussetzungen

In der folgenden Tabelle sind die Softwarevoraussetzungen und -spezifikationen für die Installation auf einem einzelnen Computer aufgeführt.

Tabelle 2. Softwarevoraussetzungen für eine Einzelcomputer-Installation	
Anforderung	**Spezifikation**
Java™ Runtime Environment (JRE)	Eine IBM JRE wird als Bestandteil der Installation von IBM Cognos Analytics unter allen Betriebssystemen bereitgestellt.
Datenbank	Eine der folgenden Datenbanken muss zum Speichern von IBM Cognos-Daten verfügbar sein: • Oracle • IBM Db2 • Microsoft SQL Server • Informix Mit der Option 'Easy Install' (früher 'Ready to Run!') wird eine Informix-Datenbank als Content Store installiert und konfiguriert. Für alle Datenbanktypen ist eine TCP-/IP-Verbindung erforderlich.

Tabelle 2. Softwarevoraussetzungen für eine Einzelcomputer-Installation (Forts.)	
Anforderung	**Spezifikation**
Web-Browser	Für alle Web-Browser muss Folgendes aktiviert sein: • Cookies • JavaScript Nur für Microsoft Internet Explorer muss Folgendes aktiviert sein: • ActiveX-Steuerelemente und Plug-ins ausführen • ActiveX-Steuerelemente ausführen, die für Scripting sicher sind • Active Scripting • META REFRESH zulassen

Anforderungen an die Kartendarstellungen

Die Karten, die Sie in Dashboards und Berichten erstellen, verwenden eine cloudbasierte Kachellandkarte und den Polygon-Service. Sie müssen von Ihrer Workstation über einen Internetzugang verfügen, damit Ihr Web-Browser über eine HTTPS-Verbindung auf den Service zugreifen kann.

Der Internetzugang zum Service ist nicht vom Cognos Analytics-Server erforderlich. Der Service stellt nur die Basiskarten und die Polygone zur Verfügung. An den Cloud-Service werden keine Benutzerdaten gesendet.

Speichereinstellungen

Speichereinstellungen sind von vielen Faktoren abhängig, beispielsweise vom Umfang der erwarteten Aktivitäten auf dem Server, der Komplexität der IBM Cognos-Anwendungen, der Anzahl von Benutzern und Anforderungen und der zulässigen Antwortzeiten.

Wenn Ihre Umgebung mehr als 100 benannte Benutzer unterstützt, komplex ist, Zeiten mit hoher hoher Systemauslastung durchläuft oder eine Kombination dieser Faktoren aufweist, sollten Sie einen Kapazitätsplan aufstellen. Weitere Informationen finden Sie in IBM Cognos Analytics-Services (www.ibm.com/software/analytics/cognos/services/).

Um die Einstellungen zu bestimmen, die optimal auf Ihre Umgebung zugeschnitten sind, sollte ein Leistungstest durchgeführt werden.

Verwenden Sie die folgenden Speichereinstellungen als Ausgangspunkt und passen Sie sie entsprechend der Speicherbelegung Ihres Systems an.

- 2 GB für das Basisbetriebssystem und die zugehörige Software, wie z. B. Virenschutz- und Sicherungssoftware sowie Management-Software für Unternehmen
- 8 GB für die Dispatcher-JVM (Content Manager oder Anwendungsebene)
- 2 GB für die Cognos Graphics Service-JVM
- 8 GB für die Abfrageservice- / Dataset-Service-JVM
- 2 GB pro BIBus für Berichtsserverprozesse
- 1 GB Anfangsgröße des Heapspeichers für Berechnungsservice für Datasets / 8 GB Maximum (Standardeinstellungen)

Festlegen der ulimit-Werte unter UNIX- und Linux-Betriebssystemen

Das Festlegen der entsprechenden ulimit-Werte unter dem verwendeten UNIX- oder Linux-Betriebssystem kann sich auf die Leistung von IBM Cognos Analytics auswirken.

Unter Linux-Betriebssystemen gehören zu den Problemen, die durch die ulimit-Einstellungen für den Stack verursacht werden, beispielsweise Fehler aufgrund von ungewöhnlich hoher Speicherbelegung durch BIBusTKServerMain oder BIBusTKServerMain bei der Verarbeitung großer Berichte.

Wenn Sie den Berichtsservice unter Linux-Betriebssystemen verwenden, können laufende Berichte oder inaktive BIBusTKServerMain-Prozesse den gesamten verfügbaren Arbeitsspeicher belegen.

Unter UNIX-Betriebssystemen können dagegen Probleme auftreten, wenn die ulimit-Einstellungen für den Stack zu niedrig sind.

Diese Probleme können durch die korrekten ulimit-Einstellungen für den Stack verhindert werden.

Die empfohlenen ulimit-Einstellungen für eine Neuinstallation sind nachfolgend aufgeführt:

IBM AIX

- CPU-Zeit (Sekunden): ulimit -t unlimited
- Dateigröße (Blöcke): ulimit -f unlimited
- Maximale Speichergröße (KB): ulimit -m unlimited
- Maximale Anzahl an Benutzerprozessen: ulimit -u unlimited
- Geöffnete Dateien: ulimit -n 8192 (Mindestwert)
- Stackgröße (KB): ulimit -s 8192 (Mindestwert)
- Virtuelle Speicher (KB): ulimit -v unlimited

Linux (x, z und p)

- CPU-Zeit (Sekunden): ulimit -t unlimited
- Dateigröße (Blöcke): ulimit -f unlimited
- Maximale Speichergröße (KB): ulimit -m unlimited
- Maximale Anzahl an Benutzerprozessen: ulimit -u unlimited
- Geöffnete Dateien: ulimit -n 8192 (Mindestwert)
- Stackgröße (KB): ulimit -s unlimited
- Virtuelle Speicher (KB): ulimit -v unlimited

Anmerkung: Diese Einstellungen müssen während des Lebenszyklus der Anwendung möglicherweise für die jeweilige Umgebung angepasst werden.

Java-Anforderungen

Damit die Verschlüsselungsservices in IBM Cognos Analytics unterstützt werden, müssen Sie Ihre Java-Version eventuell aktualisieren oder die Umgebungsvariable JAVA_HOME festlegen. Abhängig von den Anforderungen in Ihrer Sicherheitsrichtlinie müssen Sie möglicherweise auch die nicht eingeschränkte Java Cryptography Extension-Richtliniendatei (JCE-Richtliniendatei) installieren.

Sie können eine vorhandene Java Runtime Environment (JRE) verwenden oder die JRE, die mit IBM Cognos Analytics geliefert wird.

Verschlüsselungsstandards

Die IBM Cognos®-Verschlüsselungsservices verwenden eine spezielle JAR-Datei (Java-Archivdatei) mit dem Namen `bcprovpkix-XXX.jar`, die sich in der verwendeten Java Runtime Environment befinden muss. Diese Datei stellt zusätzliche Verschlüsselungs- und Entschlüsselungsroutinen bereit, die nicht im Rahmen einer JVM-Standardinstallation (JVM = Java Virtual Machine) zur Verfügung stehen. Zur Gewährleistung der Sicherheit muss die Verschlüsselungsdatei von der JVM über das Java-Erweiterungsverzeichnis geladen werden.

1. Wechseln Sie in das Verzeichnis `installationsverzeichnis/ibm-jre/jre/lib/ext`.
2. Kopieren Sie die Datei `bcprovpkix-XXX.jar` in das Verzeichnis `$JAVA_HOME/lib/ext`.

Standardmäßig wird IBM Cognos Analytics so konfiguriert, dass es den Sicherheitsstandard NIST SP800-131a unterstützt. Aus Konformitätsgründen muss Ihre JRE diesen Standard ebenfalls unterstützen.

Weitere Informationen zu den von IBM Cognos Analytics unterstützten Java-Versionen finden Sie auf der Website IBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235).

Weitere Informationen zu diesem Sicherheitsstandard finden Sie unter IBM SDK, Java Technology Edition Knowledge Center (www.ibm.com/support/knowledgecenter/SSYKE2/welcome_javasdk_family.html).

JAVA_HOME

Die Umgebungsvariable JAVA_HOME müssen Sie festlegen, wenn Sie die eigene Java-Umgebung verwenden möchten.

Stellen Sie sicher, dass die JRE-Version von IBM Cognos-Produkten unterstützt wird.

Wenn Sie unter Microsoft Windows keine JAVA_HOME-Variable festlegen, werden die mit der Installation bereitgestellten JRE-Dateien verwendet.

Lesen Sie die Informationen in IBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235) um zu prüfen, ob die verwendete JRE-Umgebung unterstützt wird.

Nicht eingeschränkte JCE-Richtliniendatei

JREs enthalten eine eingeschränkte Richtliniendatei, die die Verwendung bestimmter kryptografischer Algorithmen und Cipher Suites vorschreibt. Wenn Sie ein breiteres Spektrum an Verschlüsselungsalgorithmen und Cipher-Suites benötigen, stehen Ihnen nun standardmäßig Richtliniendateien ohne Einschränkungen ('Unlimited') zur Verfügung. Diese befinden sich an den folgenden Speicherpositionen:

- `installationsposition/ibm-jre/jre/lib/security/policy/unlimited/US_export_policy.jar`
- `installtionsposition/ibm-jre/jre/lib/security/policy/unlimited/local_policy.jar`

Darüber hinaus stehen für das von IBM bereitgestellte Java JCE-Richtliniendateien ohne Einschränkungen auch hier zur Verfügung.

Überprüfen der Standardporteinstellungen

Nach der Installation können Sie die IBM Cognos Analytics-Standardeinstellungen mithilfe des Konfigurationstools ändern. Der Installationstyp **Easy Install** wählt die Porteinstellungen für Sie aus.

Wichtig: Diese Ports müssen für eingehenden und ausgehenden Datenverkehr geöffnet sein.

Standardporteinstellungen für Cognos Analytics-Komponenten

In der folgenden Tabelle werden die Standardeinstellungen für die Ports und den URI für IBM Cognos Analytics aufgeführt.

Tabelle 3. Standardporteinstellungen für Cognos Analytics-Komponenten

Einstellung	Standardwert	Beschreibung
Content Manager-URI	`http://localhost:9300/p2pd/servlet`	Der URI zu Content Manager.
Gateway-URI	`http://`*`Computername`*`:`*`Port`*`/bi/v1/disp`	Der URI zum Gateway.

Tabelle 3. Standardporteinstellungen für Cognos Analytics-Komponenten (Forts.)		
Einstellung	**Standardwert**	**Beschreibung**
Dispatcher-URI (Intern, Extern)	`http://localhost:9300/p2pd/servlet/dispatch`	Der URI zum Dispatcher.
Dispatcher-URI für externe Anwendungen	`http://localhost:9300/bi/v1/disp`	Der URI zum Dispatcher.
Protokollserver-Port	9362	Der vom lokalen Protokollserver verwendete Port.
Mitgliedersynchronisationsport	4300	Der lokale Port, der für die Netzkommunikation verwendet wird und über den Konfigurationsinformationen zwischen den Servern übertragen und synchronisiert werden.
Mitgliederkoordinationsport	5701	Der lokale Port, der für die Netzkommunikation zur Gruppenkoordination verwendet wird. Dieser Port wird dazu verwendet, eine Gruppe zu erkennen und zu verknüpfen und eine aktuelle Liste der Konfigurationsgruppenmitglieder zu verwalten.
Port für Dataset-Service	9301	Der lokale Port, der für die Kommunikation zwischen Prozessen verwendet wird. Dieser Port wird beim erstmaligen Starten von Cognos Analytics zugeordnet. Die Portnummer errechnet sich aus dem Dispatcher-Port von Cognos Analytics plus 1. Beispiel: 9300 +1 = 9301.
Portnummer des Berechnungsservice	0	Der lokale Port, der vom Berechnungsservice verwendet wird. Stellen Sie sicher, dass Sie einen Port angeben, der noch nicht verwendet wird. Der Wert muss im Bereich von 0 bis 65535 liegen. Wenn Sie den Wert 0 angeben, ordnet der Berechungsservice den Port dynamisch zu. Bei allen anderen Werten verwendet der Berechnungsservice den von Ihnen angegebenen Wert.

Weitere Informationen finden Sie im Abschnitt „Port- und URI-Einstellungen” auf Seite 172.

Richtlinien zum Erstellen des Content Store

Beim Content Store handelt es sich um eine Datenbank, die zum Speichern von globalen Konfigurationsdaten, globalen Einstellungen (wie die auf der Benutzeroberfläche angezeigten Sprach- und Währungsformate), Datenquellenverbindungen und produktspezifischem Inhalt verwendet wird. In einer Produktionsumgebung müssen Sie eine unterstützte, für Unternehmen geeignete Datenbank als Content Store verwenden.

Designmodelle und Protokolldateien werden nicht im Content Store gespeichert.

Sie müssen den Content Store erstellen, bevor Sie das IBM Cognos Analytics-Produkt verwenden können. Wenn Sie die Option 'Easy Install' (früher 'Ready to Run!') verwenden, wird Informix installiert und zur Verwendung als Ihr Content Store konfiguriert.

Wenn Sie IBM Db2 als Content Store verwenden, können Sie eine DDL generieren, mit deren Hilfe Datenbankadministratoren eine Db2-Datenbank erstellen können, die sich für den Content Store eignet. Weitere Informationen finden Sie im Abschnitt „Generieren einer Scriptdatei zur Erstellung einer Datenbank für einen IBM Db2-Content Store” auf Seite 97.

Datenbankeigenschaften

Zum Erstellen der Content Store-Datenbank müssen Sie eine der in der folgenden Tabelle aufgeführten Datenbanken verwenden.

Die folgende Tabelle zeigt, welche Zeichencodierung und Protokolle die einzelnen Datenbanktypen jeweils verwenden.

Tabelle 4. Zeichencodierung und Protokolle für die Content Store-Datenbank

Datenbank	Zeichencodierung	Protokoll
Db2	UTF-8	TCP/IP
Oracle	AL32UTF8 oder AL32UTF16	TCP/IP
Microsoft SQL Server	UTF-8 oder UTF-16	TCP/IP
Informix	UTF-8	TCP/IP

Sortierfolge

Cognos Analytics verwendet eine einzige Sortierfolge, die die Regeln angibt, nach denen die Datenbank die Zeichendaten interpretiert, sammelt, vergleicht und darstellt. Eine Sortierfolge definiert beispielsweise, ob der Buchstabe A kleiner, gleich oder größer als der Buchstabe B ist und ob bei der Sortierfolge die Groß-/Kleinschreibung oder die Akzente beachtet werden. Weitere Informationen zu Sortierung und Sortierfolgen finden Sie auf der Website von ICU - International Components for Unicode (http://site.icu-project.org/). Wählen Sie dort 'User Guide (Benutzerhandbuch) aus und suchen Sie nach 'Collation'.

Empfohlene Einstellungen für die Erstellung des Content Store in IBM Db2 unter Linux, Windows und UNIX

Die Datenbank, die Sie unter den Betriebssystemen Microsoft Windows, Linux oder UNIX für den Content Store erstellen, muss die angegebenen Konfigurationseinstellungen aufweisen.

Um eine erfolgreiche Installation sicherzustellen, gehen Sie bei der Erstellung des Content Store anhand der folgenden Richtlinien vor. Dieselben Richtlinien gelten auch, wenn Sie eine Datenbank für Protokollnachrichten erstellen möchten.

Richtlinien zum Erstellen des Content Store

Verwenden Sie die folgende Prüfliste, um den Content Store unter Db2 einzurichten.

- Legen Sie die entsprechenden, in der folgenden Tabelle aufgeführten Umgebungsvariablen für Db2 fest.

Tabelle 5. Umgebungsvariablen für Db2

Umgebungsvariable	**Beschreibung**
DB2PATH	Das Verzeichnis der obersten Ebene, das die Datenbank-Client-Software bzw. die vollständige Datenbankinstallation enthält.
LD_LIBRARY_PATH	Der Bibliotheks-Ladepfad. Fügen Sie die Treiberposition zum Pfad hinzu und ersetzen Sie das doppelte Hash-Symbol durch `64-bit`. Für Windows: `LD_LIBRARY_PATH= $DB2_location/sqllib/lib##: $LD_LIBRARY_PATH` Für Linux:`LD_LIBRARY_PATH= $DB2DIR/lib##: $LD_LIBRARY_PATH` Für AIX: `LIBPATH=$DB2DIR/lib##:$LIBPATH`
DB2INSTANCE	Die standardmäßige Datenbankserver-Verbindung.
DB2CODEPAGE	Wenn Sie diese optionale Umgebungsvariable auf den Wert 1208 setzen, werden mehrsprachige Datenbanken unterstützt. Informationen darüber, ob diese Umgebungsvariable verwendet werden sollte, finden Sie in der Db2-Dokumentation.

- Verwenden Sie beim Erstellen der Datenbank **UTF-8** als Wert für die Zeichencodierung.

  Um zu überprüfen, ob für die Datenbank der richtige codierte Zeichensatz festgelegt ist, geben Sie in der Befehlszeile folgenden Befehl ein:

  `db2 get database configuration for` *`Datenbankname`*

  Der Wert für den codierten Zeichensatz sollte UTF-8 und der Wert für die Codepage 1208 betragen.

- Stellen Sie sicher, dass die folgenden Konfigurationsparameter wie in der folgenden Tabelle angegeben festgelegt sind.

Tabelle 6. Konfigurationsparameter für Db2

Eigenschaft	**Einstellung**
Größe des Cache für Anwendungen (applheapsz)	Unbeaufsichtigt oder mindestens 1024 KB Eine zu geringe Größe des Cache für Anwendungen kann zu Fehlernachrichten aufgrund von zu wenig Speicherplatz führen, wenn viele Benutzer angemeldet sind.

Tabelle 6. Konfigurationsparameter für Db2 (Forts.)	
Eigenschaft	**Einstellung**
Sperrenzeitlimit (locktimeout)	240 Sekunden Legen Sie keinen unbegrenzten Zeitlimitwert fest.
Db2-Registrierungsvariable (DB2_IN-LIST_TO_NLJN)	JA Durch Festlegen dieser Variable auf JA wird die Leistung verbessert.

- Erstellen Sie einen Pufferpool mit einer Seitengröße von 32 KB und einen zweiten mit einer Seitengröße von 8 KB.
- Erstellen Sie einen temporären Systemtabellenbereich unter Verwendung des im vorigen Schritts erstellten 32-KB-Pufferpools.
- Erstellen Sie einen temporären Benutzertabellenbereich unter Verwendung des erstellten 8-KB-Pufferpools.

  Im temporären Benutzertabellenbereich werden globale temporäre Tabellen erstellt.
- Gewähren Sie dem von IBM Cognos Analytics für den Zugriff auf die Datenbank verwendeten Benutzerkonto die folgenden Berechtigungen:
  - Mit Datenbank verbinden
  - Tabellen erstellen
  - Schemas implizit erstellen

  Tipp: Wenn Sie mehr als einen Content Store in Ihrer Db2-Instanz betreiben und zur gleichen Zeit verwenden möchten, verwenden Sie für jeden Content Store ein anderes Benutzerkonto um sicherzustellen, dass jede IBM Cognos Analytics-Instanz vollständig von den anderen isoliert ist.
- Stellen Sie sicher, dass das Benutzerkonto über Nutzungsberechtigungen für den temporären Benutzertabellenbereich sowie andere der Datenbank zugeordnete Tabellenbereiche verfügt.
- Erstellen Sie ein Schema für das Benutzerkonto, das IBM Cognos Analytics für den Zugriff auf die Datenbank verwendet, und stellen Sie sicher, dass der Benutzer für das Schema über Berechtigungen zum Erstellen, Löschen und Ändern verfügt.
- Erstellen Sie ein Profil, das das Profil `sqllib/db2profile` aus dem Ausgangsverzeichnis des Db2-Benutzers als Quelle verwendet. Der Inhalt des Profils kann zum Beispiel wie folgt lauten:

```
   if
[ -f /home/db2user/sqllib/db2profile ]; then
./home/db2user/sqllib/db2profile
fi
```

- Ihr Datenbankadministrator muss die IBM Cognos Analytics-Datenbanken in regelmäßigen Abständen sichern, da diese die IBM Cognos-Daten enthalten. Um die Sicherheit und die Integrität der Datenbanken zu gewährleisten, müssen diese vor nicht autorisierten und unerwünschten Zugriffen geschützt werden.

Empfohlene Einstellungen für die Erstellung des Content Store in IBM Db2 unter z/OS

Die Datenbank, die Sie für den Content Store erstellen, muss die angegebenen Konfigurationseinstellungen aufweisen.

Um eine erfolgreiche Installation sicherzustellen, gehen Sie bei der Erstellung des Content Store anhand der folgenden Richtlinien vor.

Verwenden Sie die folgende Prüfliste, um den Content Store in Db2 unter z/OS einzurichten.

- Melden Sie sich am z/OS-System als Benutzer an, der über Systemadministrator- (SYSADM) oder Systemsteuerungsberechtigung (SYSCTRL) in Db2 verfügt, um die Datenbank zu erstellen.
- Erstellen Sie eine Datenbankinstanz, eine Speichergruppe und ein Benutzerkonto für den Content Store.

  IBM Cognos Analytics verwendet die Berechtigungsnachweise des Benutzerkontos, um mit dem Datenbankserver zu kommunizieren.
- Stellen Sie sicher, dass Sie einen Pufferpool mit einer Seitengröße von 32 KB und einen zweiten Pufferpool mit einer Seitengröße von 4 KB für die Datenbankinstanz reservieren.
- Administratoren müssen ein Script zur Erstellung von Tabellenbereichen ausführen, in denen große Objekte und andere Daten für den Content Store aufbewahrt werden. Dann müssen sie die Benutzerberechtigungen für die Tabellenbereiche gewähren. Weitere Informationen zur Ausführung des Scripts finden Sie in „Erstellen von Tabellenbereichen für einen Content Store in IBM Db2 for z/OS ” auf Seite 97.
- Ihr Datenbankadministrator muss den Content Store in regelmäßigen Abständen sichern, da er die IBM Cognos-Datenanwendung und die zugehörigen Sicherheitsinformationen enthält. Um die Sicherheit und die Integrität der Content Store-Datenbank zu gewährleisten, müssen Sie sie vor nicht autorisierten und unerwünschten Zugriffen schützen.

Empfohlene Einstellungen für die Erstellung des Content Store in Oracle

Die Datenbank, die Sie für den Content Store erstellen, muss die angegebenen Konfigurationseinstellungen aufweisen.

Um eine erfolgreiche Installation sicherzustellen, gehen Sie bei der Erstellung des Content Store anhand der folgenden Richtlinien vor. Dieselben Richtlinien gelten auch, wenn Sie eine Datenbank für Protokollnachrichten erstellen möchten.

Verwenden Sie die folgende Liste, um den Content Store unter Oracle einzurichten.

- Stellen Sie sicher, dass der Parameter der Datenbank für die Kompatibilität mit Datenbankinstanzen auf 9.0.1 oder höher gesetzt ist.

  Beispielsweise können Sie die Einstellung des Initialisierungsparameters COMPATIBLE überprüfen, indem Sie die folgende SQL-Anweisung ausgeben:

  ```
  SELECT name, value, description FROM v$parameter WHERE name='compatible';
  ```

  Informationen zum Ändern von Instanzkonfigurationsparametern finden Sie in der Oracle-Dokumentation.
- Ermitteln Sie, ob die Datenbank in Unicode vorliegt.

  Tipp: Geben Sie dazu beispielsweise folgende Select-Anweisung ein:

  ```
  select * from NLS_DATABASE_PARAMETERS
  ```

  Wenn der Ergebnissatz ein NLS_CHARACTERSET zurückgibt, das nicht Unicode ist, erstellen Sie eine neue Datenbank und geben Sie für die Zeichensatzparameter der Datenbank den Wert AL32UTF8 an.

  Wenn Sie den kompatiblen Abfragemodus verwenden, empfiehlt es sich möglicherweise, die Umgebungsvariable COGUDA_EXTENDEDCHAR_SUPPORT mit dem WertT oder `t` anzugeben. Diese Variable ersetzt die 'substring'-Ausdrücke für Oracle durch SUBSTRC, damit korrekte Ergebnisse zurückgegeben werden, wenn die Zeichenfolge ergänzende Unicode-Zeichen enthält.
- Ermitteln Sie, welches Benutzerkonto für den Zugriff auf die Datenbank verwendet wird.

  Tipp: Wenn Sie mehr als einen Content Store auf Ihrer Oracle-Instanz betreiben und zur gleichen Zeit verwenden möchten, verwenden Sie für jeden Content Store ein anderes Benutzerkonto, um sicherzustellen, dass jede IBM Cognos Analytics-Instanz vollständig von den anderen isoliert ist.
- Stellen Sie sicher, dass das Benutzerkonto, mit dem auf die Datenbank zugegriffen wird, über Berechtigungen für folgende Aufgaben verfügt:
  - Herstellen einer Verbindung zur Datenbank
  - Erstellen, Ändern und Löschen von Auslösern, Ansichten, Vorgehensweisen und Reihenfolgen

  - Erstellen und Ändern von Tabellen
  - Einfügen, Aktualisieren und Löschen von Daten in Datenbanktabellen
- Ihr Datenbankadministrator muss die IBM Cognos Analytics-Datenbanken in regelmäßigen Abständen sichern, da diese die Cognos-Daten enthalten. Um die Sicherheit und die Integrität der Datenbanken zu gewährleisten, müssen diese vor nicht autorisierten und unerwünschten Zugriffen geschützt werden.

Empfohlene Einstellungen für die Erstellung des Content Store in Microsoft SQL Server

Die Datenbank, die Sie für den Content Store erstellen, muss die angegebenen Konfigurationseinstellungen aufweisen.

Um eine erfolgreiche Installation sicherzustellen, gehen Sie bei der Erstellung des Content Store anhand der folgenden Richtlinien vor. Dieselben Richtlinien gelten auch, wenn Sie eine Datenbank für Protokollnachrichten erstellen möchten.

Verwenden Sie die folgende Checkliste, um den Content Store unter Microsoft SQL Server einzurichten.

- Wichtig: In Sortierungsfolgen wird die Groß-/Kleinschreibung nicht beachtet.

  Bei der benutzerdefinierten Installation wählen Sie beim Einrichten von Microsoft SQL Server eine Sortierung aus, die u. a. Zeichensätze und die Sortierfolge enthält. Bei der Standardinstallation wird für die Sortierung die vom Installationsprogramm ermittelte Ländereinstellung verwendet. Diese Einstellung kann nicht nachträglich geändert werden.
- Verwenden Sie die Microsoft SQL-Serverauthentifizierung, wenn Sie die Verbindung mit Microsoft SQL Server Management Studio herstellen.

  Wenn Sie eine Verbindung mithilfe der Authentifizierung unter dem Microsoft Windows-Betriebssystem herstellen, wird von der Datenbank, die Sie erstellen, auch die Windows-Authentifizierung verwendet. In diesem Fall müssen Sie die Datenbankverbindung in IBM Cognos Configuration mit dem Datenbanktyp **Microsoft SQL Server-Datenbank (Windows-Authentifizierung)** konfigurieren.
- Erstellen Sie unter **Sicherheit** ein neues Benutzerkonto für den Datenbankzugriff und verwenden Sie dazu folgende Einstellungen:
  - Wählen Sie **SQL Server-Authentifizierung** aus.
  - Inaktivieren Sie das Kontrollkästchen **Kennwortrichtlinie erzwingen**.

  Tipp: Wenn Sie mehr als einen Content Store auf Ihrer Microsoft SQL Server-Instanz betreiben und zur gleichen Zeit verwenden möchten, verwenden Sie für jeden Content Store ein anderes Benutzerkonto, um sicherzustellen, dass jede IBM Cognos Analytics-Instanz vollständig von den anderen isoliert ist.
- Bei Microsoft SQL Server müssen Sie dem Benutzerkonto, das auf die Datenbank zugreift, Ausführungsberechtigungen gewähren.
- Erstellen Sie unter **Datenbanken** eine neue Datenbank für den Content Store.
- Erstellen Sie unter **Sicherheit** ein neues Schema für die neue Datenbank und weisen Sie einen Namen zu.
- Erstellen Sie unter **Sicherheit** einen neuen Benutzer für die neue Datenbank und verwenden Sie dazu folgende Einstellungen:
  - Geben Sie unter **Benutzername** den neuen Anmeldenamen an, den Sie für das Benutzerkonto erstellt haben.
  - Geben Sie unter **Standardschema** das neue Schema an.
  - Wählen Sie unter **Schemas im Besitz** das neue Schema aus.
  - Wählen Sie unter **Rollenmitglieder** die Mitglieder **db_datareader**, **db_datawriter** und **db_ddladmin** aus.

Vorgeschlagene Einstellungen für die Erstellung des Content Store im Datenbankserver von IBM Informix

Die Datenbank, die Sie für den Content Store von IBM Cognos Analytics erstellen, muss spezielle Konfigurationseinstellungen enthalten.

Orientieren Sie sich beim Erstellen des Content Store an den folgenden Richtlinien. Dieselben Richtlinien gelten auch, wenn Sie eine Datenbank für Protokollnachrichten erstellen möchten.

Verwenden Sie die folgende Checkliste, um den Content Store in der Datenbank des IBM Informix-Datenbankservers einzurichten.

- Legen Sie die folgenden Umgebungsvariablen fest:
  - Legen Sie für **GL_USEGLU** den Wert 1 fest, um ICU (International Components for Unicode) im Informix-Datenbankserver zu aktivieren.
  - Geben Sie für **DB_LOCALE** den Wert `en_us.utf8` an, um Unicode als Ländereinstellung der Datenbank festzulegen.
- Erstellen Sie bei aktivierter Protokollierung eine Datenbank im ANSI-Modus.
- Gewähren Sie dem Benutzerkonto, das Sie für den Zugriff auf die Datenbank verwenden, DBA-Datenbankberechtigungen.

  Wichtig: Wenn Sie mehr als eine Datenbank auf Ihrer Informix-Instanz speichern und gleichzeitig verwenden möchten, verwenden Sie für jede Datenbank ein anderes Benutzerkonto. Darüber hinaus müssen Sie das Benutzerkonto in jeder Instanz der Anwendung IBM Cognos Configuration definieren, indem Sie einen erweiterten Eigenschaftenparameter erstellen und das Benutzerkonto als Wert angeben. Bei mehreren Content Store-Datenbanken nennen Sie die Eigenschaft **CMSCRIPT_CS_ID**. Bei mehreren Protokolldatenbanken nennen Sie die Eigenschaft **IPFSCRIPTIDX**.

Konfigurieren eines Benutzer- oder Netzservicekontos für IBM Cognos Analytics

Sie können entweder ein Benutzer- oder ein Netzservicekonto für IBM Cognos Analytics konfigurieren.

Das Benutzer- oder Netzservicekonto zur Ausführung von IBM Cognos Analytics muss:

- über Zugriff auf alle erforderlichen Ressourcen, z. B. Drucker, verfügen
- über die Berechtigungen zum Anmelden als Service und zum Fungieren als Teil eines Betriebssystems verfügen

Darüber hinaus muss das Benutzerkonto ein Mitglied der lokalen Administratorengruppe sein.

Um zum Beispiel das Benutzerkonto zum Drucken von Berichten über einen Netzdrucker zu verwenden, muss das Benutzerkonto Zugriff auf den Netzdrucker haben oder Sie müssen dem IBM Cognos-Service ein Anmeldekonto zuweisen.

Konfigurieren eines Benutzerkontos

Unter dem Microsoft Windows-Betriebssystem weisen Sie dem IBM Cognos-Service ein Anmeldekonto zu. Sie können den IBM Cognos-Service für die Verwendung eines speziellen Benutzerkontos konfigurieren, indem Sie unter Windows im Fenster "Services" in der Liste der Services den IBM Cognos-Service auswählen. Anschließend können Sie die Eigenschaften für das Benutzerkonto festlegen.

Unter dem UNIX- oder dem Linux-Betriebssystem erstellen Sie eine neue UNIX- oder Linux-Gruppe namens "cognos". In dieser Gruppe muss der Besitzer der IBM Cognos-Dateien Mitglied sein. Ändern Sie die Eigentumsrechte der Gruppe an den IBM Cognos-Dateien so, dass diese auf die Gruppe "cognos" übergehen, und ändern Sie die Dateiberechtigungen für alle IBM Cognos-Dateien in GROUP READABLE/WRITABLE/EXECUTABLE.

Konfigurieren eines Netzserviceskontos

Das Netzservicekonto ist das im Betriebssystem integrierte Konto "NT AUTHORITY\NetworkService". Der Administrator muss weder ein Kennwort verwalten, noch das Konto bearbeiten.

Verwenden Sie ein Konto mit Administratorberechtigungen, wenn Sie die Installation unter Windows Server-Systemen vornehmen.

Sie müssen den Web-Server konfigurieren, um den Anwendungspool zu verwenden. Weitere Informationen finden Sie im Abschnitt über das Konfigurieren des Web-Servers. Zum Installieren im Verzeichnis müssen Sie außerdem über die entsprechende Schreibberechtigung verfügen.

Web-Browser konfigurieren

IBM Cognos Analytics -Komponenten verwenden Standardbrowserkonfigurationen. Zusätzliche erforderliche Einstellungen sind für den Browser spezifisch.

Browsereinstellungen für Cognos Analytics erforderlich

In der folgenden Tabelle sind die Einstellungen aufgeführt, die aktiviert werden müssen.

Tabelle 7. Aktivierte Browsereinstellungen

Browser	**Einstellung**
Alle Browser	Pop-ups für alle Cognos Analytics -Seiten zulassen
Internet Explorer Kante	Cookies zulassen Active Scripting Meta-Aktualisierung zulassen ActiveX-Steuerelemente und Plug-ins ausführen ActiveX-Steuerelemente für Scripts, die für Scripting sicher sind Binärdateien und Script-Verhalten Zugriff über programmgesteuerte Zwischenablage zulassen Benutzerdatenpersistenz
Firefox	Cookies zulassen Java aktivieren JavaScript aktivieren Bilder laden
Safari 5	Java aktivieren JavaScript aktivieren Cookies blockieren: Nie
Google Chrome	Cookies: Lassen Sie die lokalen Daten festlegen Bilder: Alle Bilder anzeigen JavaScript: Alle Sites für die Ausführung von JavaScript zulassen

Reporting und Query Studio verwenden die native XML-Unterstützung von Microsoft Internet Explorer, die eine Komponente des Browsers ist. Die ActiveX-Unterstützung muss aktiviert sein, da Microsoft -Anwendungen XML mit ActiveX implementieren. Cognos Analytics stellt keine ActiveX-Steuerelemente bereit oder lädt sie nicht herunter. Über diese Konfiguration werden nur die ActiveX-Steuerelemente aktiviert, die als Teil von Internet Explorer installiert werden.

Wenn Sie Microsoft Internet Explorer verwenden, können Sie die URL für Ihre Gateway (en) zur Liste der vertrauenswürdigen Sites hinzufügen. Beispiel: `http:// < Servername>: < portnummer> /ibm-cognos`. Dies ermöglicht die automatische Bedienerführung für Dateidownloads.

Von Cognos Analytics -Komponenten verwendete Cookies

Cognos Analytics verwendet die folgenden Cookies, um Benutzerinformationen zu speichern.

Tabelle 8. Von Cognos Analytics -Komponenten verwendete Cookies

Cookie	**Typ**	**Zweck**
AS_TICKET	Sitzung temporär	Wird erstellt, wenn Cognos Analytics für die Verwendung eines IBM Cognos Series 7-Namespace konfiguriert ist.
Caf	Sitzung temporär	Enthält Informationen zum Sicherheitsstatus
Cam_Pass	Sitzung temporär	Speichert einen Verweis auf eine Benutzersitzung, die auf dem Content Manager-Server gespeichert ist. Administratoren können das Attribut HTTPOnly festlegen, um Scripts beim Lesen oder Manipulieren des CAM-Passport-Cookies während der Sitzung eines Benutzers mit ihrem Web-Browser zu blockieren. Weitere Informationen finden Sie im *IBM Cognos Analytics Administration and Security Guide*.
cc_session	Sitzung temporär	Enthält Sitzungsinformationen
cc_state	Sitzung temporär	Enthält Informationen während Bearbeitungsoperationen, wie z. B. Schnitt, Kopieren und Einfügen
CRN	Sitzung temporär	Enthält die Informationen zum Inhalt und zur Produktländereinstellung und wird für alle IBM Cognos -Benutzer festgelegt.
CRN_RS	Persistent	Speichert die Auswahl, die der Benutzer für den Ordner 'View members' in Reporting vornimmt.

Tabelle 8. Von Cognos Analytics -Komponenten verwendete Cookies (Forts.)		
Cookie	**Typ**	**Zweck**
ORDNER PAT_CURRENT_	Persistent	Speichert den aktuellen Ordnerpfad, wenn der lokale Dateizugriff verwendet wird, und wird nach der Verwendung des Dialogfensters "Öffnen" oder "Speichern" aktualisiert.
Qs	Persistent	Speichert die Einstellungen, die der Benutzer für Benutzerschnittstellenelemente wie Menüs und Symbolleisten herstellt.
userCapabilities	Sitzung temporär	Enthält alle Funktionen und die Signatur für den aktuellen Benutzer.
usersessionid	Sitzung temporär	Enthält eine eindeutige Kennung für die Benutzersitzung, die für die Dauer der Browsersitzung gültig ist.
XSRF (Cross-Site Request Forgery)	Sitzung temporär	XSRF bietet einen Webbrowser an, um eine zerstörerische Aktion auf einer vertrauenswürdigen Site auszuführen, für die der Benutzer derzeit authentifiziert ist. XSRF nutzt das Vertrauen, das eine Site im Browser eines Benutzers hat. Verhindert, dass eine von Domäne X geladene Webseite Anforderungen an die Domäne Y stellt, vorausgesetzt, der Benutzer ist bereits für die Domäne Y authentifiziert. Bei der ersten Authentifizierung mit Cognos Analyticswird XSRF-Cookie gesetzt. Ab diesem Zeitpunkt müssen für alle Anforderungen sowohl das XSRF-TOKEN-Cookie als auch ein HTTP-Header mit dem Namen X-XSRF-TOKEN erforderlich sein.

Nach dem Upgrade oder der Installation neuer Software starten Sie den Web-Browser erneut und beraten Benutzer, um ihren Browser-Cache zu löschen.

Kapitel 2. "Easy Install"

Diese Installationsoption soll Sie dabei unterstützen, IBM Cognos Analytics innerhalb kürzester Zeit in Betrieb zu nehmen, ohne zusätzliche Konfigurationen vornehmen oder unterstützende Software installieren zu müssen. Diese Option wird nicht für die Produktion empfohlen.

Informationen zu diesem Vorgang

Wichtig: "Easy Install" ist nur unter Windows verfügbar.

Anmerkung: Wenn Sie eine der unterstützten Datenbanken für den Content Store, Audits und Benachrichtigungen in Produktionsumgebungen verwenden möchten, müssen Sie die Konfiguration entsprechend ändern. Die im Produktpaket enthaltene und vorkonfigurierte Informix-Datenbank ist nicht für den Einsatz in Produktionsumgebungen vorgesehen.

Diese Installationsoption soll Sie dabei unterstützen, IBM Cognos Analytics innerhalb kürzester Zeit in Betrieb zu nehmen, ohne zusätzliche Konfigurationen vornehmen oder unterstützende Software installieren zu müssen. Auf einem Computer kann jeweils nur eine **Easy Install**-Installation durchgeführt werden. Mit dieser Installationsoption erhalten Sie die folgenden Komponenten mit der gesamten bereits vorgenommenen Konfiguration:

- Vollversion der IBM Cognos Analytics-Software mit allen neuen Funktionen zum Testen.
- Informix 12.10, das nur zur Verwendung als Content-Store-Datenbank ebenfalls installiert und konfiguriert wird.
- Apache Directory Server zur Erstellung und Verwaltung von Benutzern (Benutzer des lokalen Servers).
- Cognos Analytics-Beispiele (nur Basisbeispiele).

Diese Installationsoption unterstützt Folgendes **nicht**:

- Verwaltung oder Konfiguration des bereitgestellten Apache Directory Server.
- Verwaltung oder Konfiguration der bereitgestellten Informix-Datenbank.
- Audits mithilfe der bereitgestellten Informix-Datenbank.

Anmerkung: Damit der Informix-Benutzer und die Informix-Gruppe lokal erstellt werden können, muss das Cognos-Installationsprogramm als **lokaler Administrator**ausgeführt werden.

Vorgehensweise

1. Laden Sie die ausführbare Datei des Installationsprogramms und die komprimierte Repository-Datei von https://www.ibm.com/software/passportadvantage/index.html herunter.
2. Führen Sie das Installationsprogramm aus und folgen Sie den Eingabeaufforderungen.
3. Folgendes kann während des Installationsprozesses angepasst werden:
   - Installationsposition
   - Verknüpfungsname
   - Verknüpfungs-Verfügbarkeit
4. Wählen Sie eine Benutzer-ID und ein Kennwort aus, die für die Anmeldung verwendet werden.

   Die Kennwortanforderung ist:

   Mindestens ein Großbuchstabe, ein Kleinbuchstabe und mindestens eine Ziffer.

   Mindestens ein Sonderzeichen zwischen (!@#$) und Kennwortlänge zwischen 15 -20 Zeichen.

   Wichtig: 11.1.7 Die Mindestkennwortlänge beträgt jetzt 15 Zeichen entsprechend dem Industriestandard.
5. Überprüfen Sie die Optionen und klicken Sie auf **Installieren**.

6. Überprüfen Sie die Nachrichten, um den Installationserfolg sicherzustellen.
7. Bei Bedarf überprüfen Sie die Protokolle unter `installLocation/uninstall/logs`.
8. Klicken Sie auf **Fertig**.

Ergebnisse

Sie können jetzt **IBM Cognos Analytics** über die Programmverknüpfung starten.

Kapitel 3. Einzelserverinstallation

Vorgehensweise zur Installation von IBM Cognos Analytics in einer Einzelserverumgebung. Wählen Sie mithilfe des Installationsassistenten die zu installierenden Serverkomponenten sowie den Pfad auf Ihrem Computer aus, in dem sie installiert werden sollen.

Wichtig: Sie müssen vollständig qualifizierte Hostnamen in den Werten für die folgenden Felder von Cognos Configuration angeben. Jeder Wert, den Sie angeben, muss auch im Feld **Subject Alternative Name** > **DNS-Namen** oder im Feld **Subject Alternative Name** > **IP-Adressen** angezeigt werden.

- **Umgebung**
  - **Gateway-URI**
  - **Externer Dispatcher-URI**
  - **Interner Dispatcher-URI**
  - **Dispatcher-URI für externe Anwendungen**
  - **Content Manager-URIs**
- **Umgebung** > **Konfigurationsgruppe**
  - **Gruppenkontakthost**
  - **Host für die Koordination von Mitgliedern**
- **Zugriffsschutz** > **Verschlüsselung** > **Cognos**
  - **Allgemeiner Servername**
  - **Subject Alternative Name** > **DNS-Namen**
  - **Subject Alternative Name** > **IP-Adressen**

Vorbereitende Schritte

1. Erforderlich:

   Beim Content Store handelt es sich um eine Datenbank, die Content Manager zum Speichern von globalen Konfigurationsdaten, globalen Einstellungen (wie die auf der Benutzeroberfläche angezeigten Sprach- und Währungsformate), Datenquellenverbindungen und produktspezifischem Inhalt verwendet. In einer Produktionsumgebung müssen Sie eine unterstützte, für Unternehmen geeignete Datenbank als Content Store verwenden.

   Weitere Informationen finden Sie in Kapitel 3 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.
2. Diese Konfigurationsaktionen sind für den Erfolg der Installation entscheidend. Nach der Installation der Komponenten führen Sie folgende erforderlichen Aktionen aus.

   Weitere Informationen finden Sie in Kapitel 1 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Installation*.
3. Für die authentifizierte Anmeldung müssen Sie IBM Cognos Analytics-Komponenten mit einem geeigneten Namespace für den Typ des Authentifizierungsproviders in Ihrer Umgebung konfigurieren. Sie können mehrere Namespaces für die Authentifizierung konfigurieren und anschließend bei der Ausführung bestimmen, welche Namespaces verwendet werden sollen.

   Weitere Informationen finden Sie in Kapitel 7 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.
4. Optional:

   a. Sie können eine Auditdatenbank erstellen, um Protokollnachrichten zu speichern.

      Weitere Informationen finden Sie in Kapitel 3 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.

b. Web-Server:

i) Sie müssen Ihren Web-Server konfigurieren, bevor Benutzer eine Verbindung zum IBM® Cognos® Analytics-Portal herstellen können. Für IBM Cognos Analytics für die Berichterstellung müssen Sie außerdem das Ablaufdatum für Inhalte für das Imageverzeichnis in Ihrem Web-Server festlegen, damit der Web-Browser den Imagetatus nach dem ersten Zugriff nicht überprüft.

Weitere Informationen finden Sie in Kapitel 4 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.

ii) Dieses Tool automatisiert die Konfigurationsschritte auf Grundlage des IBM Knowledge Center-Artikels zum Konfigurieren von IIS mit Cognos Analytics.

Weitere Informationen finden Sie unter automatisiertes Script für Internet Information Services

iii) Um in Reporting Images anzuzeigen oder nach ihnen zu suchen, konfigurieren Sie Web Distributed Authoring and Versioning (WebDAV) auf Ihrem Web-Server. Berichtsersteller können ähnlich wie beim Durchsuchen eines Dateisystems nach Bildern suchen, die zu Berichten hinzugefügt werden sollen. Auf Web-Servern mit Microsoft Internet Information Services (IIS) müssen Sie zunächst die WebDAV-Funktion aktivieren und den Web-Server danach so konfigurieren, dass er auf das Bildverzeichnis zugreifen kann.

Weitere Informationen finden Sie in Kapitel 4 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.

iv) Um in Reporting Images anzuzeigen oder nach ihnen zu suchen, konfigurieren Sie Web Distributed Authoring and Versioning (WebDAV) auf Ihrem Web-Server. Berichtsersteller können ähnlich wie beim Durchsuchen eines Dateisystems nach Bildern suchen, die zu Berichten hinzugefügt werden sollen. Auf einem IBM HTTP Server oder einem Apache HTTP Server müssen Sie der Serverkonfigurationsdatei Anweisungen hinzufügen und danach den Verzeichniszugriff konfigurieren.

Weitere Informationen finden Sie in Kapitel 4 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.

v) Nachdem Sie diese Web-Server-Prozedur ausgeführt haben, kann der Server Anforderungen für statische Dateien (wie beispielsweise .js, .html, .css), Lastausgleichsanforderungen an IBM Cognos Analytics und SSO-Weiterleitungsanforderungen durch den IBM Cognos Analytics-Gatewaycode bearbeiten.

Weitere Informationen finden Sie in Kapitel 4 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.

c. Konfigurieren Sie Ihren IBM® Cognos® Analytics-Mail-Server für das Senden von Benachrichtigungen mit IBM Cognos Event Studio.

Weitere Informationen finden Sie in Kapitel 1 des *Event Studio-Benutzerhandbuchs* zu IBM Cognos Analytics.

d. Der Benachrichtigungsserver verwendet standardmäßig dieselbe Datenbank, die Content Manager für den Content Store verwendet. Sie können separate Datenbanken für die Benachrichtigung verwenden, wenn Sie große Mengen an Stapelberichten und -E-Mails ausführen müssen.

Weitere Informationen finden Sie in Kapitel 6 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.

Vorgehensweise

1. Laden Sie das Installationsprogramm und das Repository herunter.

   Laden Sie sie von Passport Advantage herunter.
2. Klicken Sie doppelt auf die Installationsdatei.
3. Folgen Sie den Anweisungen im Installationsassistenten, um die Dateien auf Ihren Computer zu kopieren und dort zu installieren.
4. Installationsprotokolldateien finden Sie hier: `<installLocation/uninstall/logs>`

5. Navigieren Sie nach Abschluss zu dem Ordner **Treiber** unter <InstallLocation\drivers> und legen Sie dort die entsprechenden JDBC-Treiber für die **Content Store**- und die **Audit**-Datenbank ab.
6. Navigieren Sie zur Verknüpfungsposition und starten Sie **Cognos Configuration**.
7. Wenn die Option **Gateway** ausgewählt wurde, ändern Sie den **Gateway-URI** in das folgende Format: <http://applicationTierServer:applicationTierPort/bi/v1/disp
   a) Verwenden Sie **HTTPS**, wenn SSL verwendet wird.
   b) Weitere Informationen finden Sie in Kapitel 6 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.
8. Konfigurieren Sie die Auditdatenbank.
   a) Klicken Sie mit der rechten Maustaste auf **Protokollierung** > **Neue Ressource** > **Ziel**.
   b) Legen Sie den Namen auf **Audit** fest.
   c) Legen Sie den Typ auf **Datenbank** fest.
   d) Klicken Sie mit der rechten Maustaste auf**Neue Ressource** > **Datenbank** > **Audit**.
   e) Legen Sie den Namen auf **Audit** fest.
   f) Wählen Sie den **Datenbanktyp** aus.
   g) Wählen Sie den Datenbankserver und die Portnummer aus.
   h) Legen Sie die Datenbankbenutzer-ID und das Kennwort fest.
   i) Legen Sie den Datenbanknamen und die Verschlüsselung fest.
9. Konfigurieren Sie den Authentifizierungsprovider.
   a) Klicken Sie mit der rechten Maustaste auf **Authentifizierungsquelle** > **Neue Ressource** > **Namespace**. Legen Sie Folgendes fest:
      - Name
      - Typ (Gruppe)
      - Typ
   b) Weitere Details zur Authentifizierung finden Sie in Kapitel 7 der Veröffentlichung *Cognos Analytics - Konfiguration* .
10. Wenn der Content Store Db2 ist, füllen Sie die folgenden Felder aus:
    a) Datenbankserver und Portnummer.
    b) Benutzer-ID und Kennwort für die Datenbank.
    c) Datenbankname und Verschlüsselung.
11. Wenn der Content Store nicht Db2 ist, füllen Sie die folgenden Felder aus:
    a) Klicken Sie mit der rechten Maustaste auf **Content Manager** und wählen Sie **Löschen** aus. Bestätigen Sie den Löschvorgang.
    b) Klicken Sie mit der rechten Maustaste auf **Content Manager** > **Neue Ressource** > **Datenbank**. Legen Sie Folgendes fest:
       - Name
       - Typ (Gruppe)
       - Datenbankserver und Portnummer.
       - Benutzer-ID und Kennwort für die Datenbank.
       - Datenbankname und Verschlüsselung.
12. Konfigurieren Sie einen Mail-Server.
    a) Klicken Sie auf **Benachrichtigung**.
       - Legen Sie den SMTP-Mail-Server fest.
       - Legen Sie Konto und Kennwort fest, falls zutreffend.
       - Legen Sie bei Bedarf den Standardabsender fest.

- Legen Sie den Wert 'SSL-Verschlüsselung aktiviert' fest.

13. Konfigurieren Sie einen Notification Store.
    a) Klicken Sie mit der rechten Maustaste auf **Benachrichtigung** > **Neue Ressource** > **Datenbank**. Füllen Sie Folgendes aus:
    - Legen Sie den Namen **Notification Store** fest.
    - Typ: Wählen Sie Ihren Notification Store-Datenbanktyp aus.
    - Datenbankserver und Portnummer.
    - Benutzer-ID und Kennwort.
    - Datenbankname.
    - Verschlüsselung.
14. **Testen** Sie die Konfiguration, um sicherzustellen, dass die Einstellungen gültig sind.
    a) Klicken Sie auf **Konfiguration** > **Aktionsmenü** > **Test**

Ergebnisse

Wenn Sie kein **Gateway** festgelegt haben, können Sie jetzt hier auf IBM Cognos Analytics zugreifen: `serverName:9300/bi` .

Kapitel 4. Verteilte Serverinstallation

Vorgehensweise zur Installation von IBM Cognos Analytics in einer verteilten Umgebung. Bei der Installation von IBM® Cognos® Analytics-Serverkomponenten können Sie angeben, wo die Komponenten für Anwendungsebene, Datenebene (Content Manager) und Gatewayebene angeordnet werden sollen. Wählen Sie diese Option, um die Leistung, Verfügbarkeit, Kapazität oder die Sicherheit basierend auf den Verarbeitungseigenschaften Ihres Unternehmens zu optimieren.

Wichtig: Sie müssen vollständig qualifizierte Hostnamen in den Werten für die folgenden Felder von Cognos Configuration angeben. Jeder Wert, den Sie angeben, muss auch im Feld **Subject Alternative Name** > **DNS-Namen** oder im Feld **Subject Alternative Name** > **IP-Adressen** angezeigt werden.

- **Umgebung**
  - **Gateway-URI**
  - **Externer Dispatcher-URI**
  - **Interner Dispatcher-URI**
  - **Dispatcher-URI für externe Anwendungen**
  - **Content Manager-URIs**
- **Umgebung** > **Konfigurationsgruppe**
  - **Gruppenkontakthost**
  - **Host für die Koordination von Mitgliedern**
- **Zugriffsschutz** > **Verschlüsselung** > **Cognos**
  - **Allgemeiner Servername**
  - **Subject Alternative Name** > **DNS-Namen**
  - **Subject Alternative Name** > **IP-Adressen**

Vorbereitende Schritte

1. Erforderlich:

   Beim Content Store handelt es sich um eine Datenbank, die Content Manager zum Speichern von globalen Konfigurationsdaten, globalen Einstellungen (wie die auf der Benutzeroberfläche angezeigten Sprach- und Währungsformate), Datenquellenverbindungen und produktspezifischem Inhalt verwendet. In einer Produktionsumgebung müssen Sie eine unterstützte, für Unternehmen geeignete Datenbank als Content Store verwenden.

   Weitere Informationen finden Sie in Kapitel 3 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.
2. Diese Konfigurationsaktionen sind für den Erfolg der Installation entscheidend. Nach der Installation der Komponenten führen Sie folgende erforderlichen Aktionen aus.

   Weitere Informationen finden Sie in Kapitel 1 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Installation*.
3. Der Benachrichtigungsserver verwendet standardmäßig dieselbe Datenbank, die Content Manager für den Content Store verwendet. Sie können separate Datenbanken für die Benachrichtigung verwenden, wenn Sie große Mengen an Stapelberichten und -E-Mails ausführen müssen.

   Weitere Informationen finden Sie in Kapitel 6, Seite 131 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.
4. Für die authentifizierte Anmeldung müssen Sie IBM Cognos Analytics-Komponenten mit einem geeigneten Namespace für den Typ des Authentifizierungsproviders in Ihrer Umgebung konfigurieren. Sie können mehrere Namespaces für die Authentifizierung konfigurieren und anschließend bei der Ausführung bestimmen, welche Namespaces verwendet werden sollen.

Weitere Informationen finden Sie in Kapitel 7 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.

5. Optional:
   a. Sie können eine Auditdatenbank erstellen, um Protokollnachrichten zu speichern.

      Weitere Informationen finden Sie in Kapitel 3 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.

   b. Web-Server:

      i) Sie müssen Ihren Web-Server konfigurieren, bevor Benutzer eine Verbindung zum IBM® Cognos® Analytics-Portal herstellen können. Für IBM Cognos Analytics für die Berichterstellung müssen Sie außerdem das Ablaufdatum für Inhalte für das Imageverzeichnis in Ihrem Web-Server festlegen, damit der Web-Browser den Imagetatus nach dem ersten Zugriff nicht überprüft.

      Weitere Informationen finden Sie in Kapitel 4 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.

      ii) Dieses Tool automatisiert die Konfigurationsschritte auf Grundlage des IBM Knowledge Center-Artikels zum Konfigurieren von IIS mit Cognos Analytics.

      Weitere Informationen finden Sie unter Automatisiertes Script für Information Server

      iii) Um in Reporting Images anzuzeigen oder nach ihnen zu suchen, konfigurieren Sie Web Distributed Authoring and Versioning (WebDAV) auf Ihrem Web-Server. Berichtsersteller können ähnlich wie beim Durchsuchen eines Dateisystems nach Bildern suchen, die zu Berichten hinzugefügt werden sollen. Auf Web-Servern mit Microsoft Internet Information Services (IIS) müssen Sie zunächst die WebDAV-Funktion aktivieren und den Web-Server danach so konfigurieren, dass er auf das Bildverzeichnis zugreifen kann.

      Weitere Informationen finden Sie in Kapitel 4 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.

      iv) Um in Reporting Images anzuzeigen oder nach ihnen zu suchen, konfigurieren Sie Web Distributed Authoring and Versioning (WebDAV) auf Ihrem Web-Server. Berichtsersteller können ähnlich wie beim Durchsuchen eines Dateisystems nach Bildern suchen, die zu Berichten hinzugefügt werden sollen.

      Weitere Informationen finden Sie in Kapitel 4 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.

      v) Nachdem Sie diese Prozedur ausgeführt haben, kann der Server Anforderungen für statische Dateien (wie beispielsweise .js, .html, .css), Lastausgleichsanforderungen an IBM Cognos Analytics und SSO-Weiterleitungsanforderungen durch den IBM Cognos Analytics-Gatewaycode bearbeiten.

      Weitere Informationen finden Sie in Kapitel 4 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.

   c. Konfigurieren Sie Ihren IBM® Cognos® Analytics-Mail-Server für das Senden von Benachrichtigungen mit IBM Cognos Event Studio.

      Weitere Informationen finden Sie in Kapitel 1 der IBM Cognos Analytics-Veröffentlichung *Event Studio - Benutzerhandbuch*.

Ergebnisse

Installation der Inhaltsebene

Vorgehensweise zum Installieren der Inhaltsebene von IBM Cognos Analytics 11.1.x

Wichtig: Sie müssen vollständig qualifizierte Hostnamen in den Werten für die folgenden Felder von Cognos Configuration angeben. Jeder Wert, den Sie angeben, muss auch im Feld **Subject Alternative Name** > **DNS-Namen** oder im Feld **Subject Alternative Name** > **IP-Adressen** angezeigt werden.

- **Umgebung**
  - **Gateway-URI**
  - **Externer Dispatcher-URI**
  - **Interner Dispatcher-URI**
  - **Dispatcher-URI für externe Anwendungen**
  - **Content Manager-URIs**
- **Umgebung** > **Konfigurationsgruppe**
  - **Gruppenkontakthost**
  - **Host für die Koordination von Mitgliedern**
- **Zugriffsschutz** > **Verschlüsselung** > **Cognos**
  - **Allgemeiner Servername**
  - **Subject Alternative Name** > **DNS-Namen**
  - **Subject Alternative Name** > **IP-Adressen**

Vorgehensweise

1. Laden Sie die ausführbare Datei und die komprimierten Repository-Dateien herunter.
   Laden Sie sie von Passport Advantage herunter.
2. Klicken Sie doppelt auf die Installationsdatei.
3. Wählen Sie **IBM Cognos Analytics** und die gewünschte Installationsposition aus.
4. Markieren Sie das entsprechende Kontrollkästchen, wenn eine Verknüpfung allen Benutzern zur Verfügung stehen soll.
5. Legen Sie den **Installationstyp** als **Benutzerdefiniert** fest und klicken Sie auf **Weiter**.
6. Markieren Sie **Inhaltsebene**.
7. Überprüfen Sie die Installationsoptionen und klicken Sie auf **Installieren**.
8. Überprüfen Sie alle Nachrichten nach der Installation.
9. Installationsprotokolldateien finden Sie hier: `<installLocation/uninstall/logs>`
10. Klicken Sie auf **Fertig**.
11. Navigieren Sie zum Ordner **Treiber** unter `<InstallLocation\drivers>` und legen Sie die entsprechenden JDBC-Treiber für die **Content Store** - und die **Audit**-Datenbank ab.
12. Wenn SSL implementiert wird, importieren Sie SSL-Zertifikate. Informationen hierzu finden Sie in der
13. Navigieren Sie zur Verknüpfungsposition und starten Sie **Cognos Configuration**.
    a) Klicken Sie auf **Umgebung**.
    b) Geben Sie unter **Weitere URI-Einstellungen** den **Dispatcher-URI für externe Anwendungen** zu dem Server und Port an, wo die Anwendungsebene installiert wird.
       Das Format des URI ist `<http://applicationTierServer:applicationTier-Port/bi/v1/disp`
    c) Verwenden Sie **HTTPS**, wenn SSL verwendet wird.
14. Konfigurieren Sie die Auditdatenbank.
    a) Klicken Sie mit der rechten Maustaste auf **Protokollierung** > **Neue Ressource** > **Ziel**.
    b) Legen Sie den Namen auf **Audit** fest.
    c) Legen Sie den Typ auf **Datenbank** fest.
    d) Klicken Sie mit der rechten Maustaste auf**Neue Ressource** > **Datenbank** > **Audit**.
    e) Legen Sie den Namen auf **Audit** fest.
    f) Wählen Sie den **Datenbanktyp** aus.
    g) Wählen Sie den Datenbankserver und die Portnummer aus.

h) Legen Sie die Datenbankbenutzer-ID und das Kennwort fest.

i) Legen Sie den Datenbanknamen und die Verschlüsselung fest.

15. Konfigurieren Sie den Authentifizierungsprovider.
    a) Klicken Sie mit der rechten Maustaste auf **Authentifizierungsquelle** > **Neue Ressource** > **Namespace**. Legen Sie Folgendes fest:
       - Name
       - Typ (Gruppe)
       - Typ
16. Wenn der Content Store Db2 ist, füllen Sie die folgenden Felder aus:
    a) Datenbankserver und Portnummer.
    b) Benutzer-ID und Kennwort für die Datenbank.
    c) Datenbankname und Verschlüsselung.
17. Wenn der Content Store nicht Db2 ist, füllen Sie die folgenden Felder aus:
    a) Klicken Sie mit der rechten Maustaste auf **Content Manager** und wählen Sie **Löschen** aus. Bestätigen Sie den Löschvorgang.
    b) Klicken Sie mit der rechten Maustaste auf **Content Manager** > **Neue Ressource** > **Datenbank**. Legen Sie Folgendes fest:
       - Name
       - Typ (Gruppe)
       - Datenbankserver und Portnummer.
       - Benutzer-ID und Kennwort für die Datenbank.
       - Datenbankname und Verschlüsselung.
18. Konfigurieren Sie einen Mail-Server.
    a) Klicken Sie auf **Benachrichtigung**.
       - Legen Sie den SMTP-Mail-Server fest.
       - Legen Sie Konto und Kennwort fest, falls zutreffend.
       - Legen Sie bei Bedarf den Standardabsender fest.
       - Legen Sie den Wert 'SSL-Verschlüsselung aktiviert' fest.
19. Konfigurieren Sie einen Notification Store.
    a) Klicken Sie mit der rechten Maustaste auf **Benachrichtigung** > **Neue Ressource** > **Datenbank**. Füllen Sie Folgendes aus:
       - Legen Sie den Namen **Notification Store** fest.
       - Typ: Wählen Sie Ihren Notification Store-Datenbanktyp aus.
       - Datenbankserver und Portnummer.
       - Benutzer-ID und Kennwort.
       - Datenbankname.
       - Verschlüsselung.
20. **Testen** Sie die Konfiguration, um sicherzustellen, dass die Einstellungen gültig sind.
    a) Klicken Sie auf **Konfiguration** > **Aktionsmenü** > **Test**

    Der Mail-Server-Verbindungstest schlägt fehl, wenn der Mail-Server nicht konfiguriert ist.
21. **Starten** Sie die Inhaltsebene.

    Informationen hierzu finden Sie in der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.

Installation der Anwendungsebene

Vorgehensweise zum Installieren der Anwendungsebene von IBM Cognos Analytics 11.1.x

Wichtig: Sie müssen vollständig qualifizierte Hostnamen in den Werten für die folgenden Felder von Cognos Configuration angeben. Jeder Wert, den Sie angeben, muss auch im Feld **Subject Alternative Name** > **DNS-Namen** oder im Feld **Subject Alternative Name** > **IP-Adressen** angezeigt werden.

- **Umgebung**
  - **Gateway-URI**
  - **Externer Dispatcher-URI**
  - **Interner Dispatcher-URI**
  - **Dispatcher-URI für externe Anwendungen**
  - **Content Manager-URIs**
- **Umgebung** > **Konfigurationsgruppe**
  - **Gruppenkontakthost**
  - **Host für die Koordination von Mitgliedern**
- **Zugriffsschutz** > **Verschlüsselung** > **Cognos**
  - **Allgemeiner Servername**
  - **Subject Alternative Name** > **DNS-Namen**
  - **Subject Alternative Name** > **IP-Adressen**

Vorgehensweise

1. Laden Sie die ausführbare Datei und die komprimierten Repository-Dateien herunter.
   Laden Sie sie von Passport Advantage herunter.
2. Klicken Sie doppelt auf die Installationsdatei.
3. Wählen Sie **IBM Cognos Analytics** und die gewünschte Installationsposition aus.
4. Wenn die Verknüpfung für alle Benutzer verfügbar sein soll, markieren Sie das entsprechende **Kontrollkästchen**.
5. Legen Sie den **Installationstyp** als **Benutzerdefiniert** fest und klicken Sie auf **Weiter**.
6. Markieren Sie **Anwendungsebene**.
7. Überprüfen Sie die Installationsoptionen und klicken Sie auf **Installieren**.
8. Überprüfen Sie alle Fehlernachrichten.
9. Installationsprotokolldateien finden Sie hier: `<installLocation/uninstall/logs>`
10. Klicken Sie auf **Fertig**.
11. Legen Sie im Ordner **Treiber** unter `<InstallLocation\drivers>` die entsprechenden JDBC-Treiber für die **Content Store**- und die **Audit**-Datenbank ab.
12. Starten Sie **Cognos Configuration**.
13. Klicken Sie auf **Umgebung**.
14. Ändern Sie **HTTP** in **HTTPS** , wenn SSL verwendet wird.
    Informationen hierzu finden Sie in der Weitere Informationen finden Sie in Kapitel 6 der IBM Cognos Analytics-Veröffentlichung *Cognos Analytics - Konfiguration*.
15. Wenn ein Gateway installiert werden soll, ändern Sie den **Gateway-URI** unter Verwendung des folgenden Formats: `<webserverName:webserverPort/alias/bi/v1/disp>`
16. Wenn der Anwendungsserver auf demselben Server als weitere Instanz von **IBM Cognos Analytics** installiert wird und diese Instanz zum Zeitpunkt der Installation der Anwendungsebene nicht aktiv war, achten Sie darauf, die folgenden Ports für das Öffnen anzupassen:
    - Externer Dispatcher-URI

- Interner Dispatcher-URI
- Portnummer des Dataset-Service
- Dispatcher-URI für externe Anwendungen

17. Klicken Sie mit der rechten Maustaste auf **Konfigurationsgruppe** > **Abrufen**
    - Legen Sie die Benutzer-ID, das Kennwort, den Namespace und die URL gemäß der Konfiguration durch die **Inhaltsebene** fest.
    - Legen Sie den **Mitgliedersynchronisationsport** und den **Mitgliederkoordinationsport** fest.
18. Klicken Sie auf **Protokollierung** und passen Sie die Portnummer des lokalen Serverports an.
19. Klicken Sie unter **Weitere URI-Einstellungen** auf neben **Content Manager-URIs** und fügen Sie den Server und Port für die **Inhaltsebene** hinzu, die zuvor installiert wurde.
20. Konfigurieren Sie die Auditdatenbank.
    a) Klicken Sie mit der rechten Maustaste auf **Protokollierung** > **Neue Ressource** > **Ziel**.
    b) Legen Sie den Namen auf **Audit** fest.
    c) Legen Sie den Typ auf **Datenbank** fest.
    d) Klicken Sie mit der rechten Maustaste auf**Neue Ressource** > **Datenbank** > **Audit**.
    e) Legen Sie den Namen auf **Audit** fest.
    f) Wählen Sie den **Datenbanktyp** aus.
    g) Wählen Sie den Datenbankserver und die Portnummer aus der Einrichtung der **Inhaltsebene** aus.
    h) Legen Sie die Datenbankbenutzer-ID und das Kennwort aus der **Inhaltsebene** fest.
    i) Legen Sie den Datenbanknamen und die Verschlüsselung aus der **Inhaltsebene** fest.
21. Konfigurieren Sie einen Notification Store.
    a) Klicken Sie mit der rechten Maustaste auf **Benachrichtigung** > **Neue Ressource** > **Datenbank**. Füllen Sie Folgendes aus:
        - Legen Sie den Namen **Notification Store** fest.
        - Typ: Wählen Sie Ihren Notification Store-Datenbanktyp aus.
        - Datenbankserver und Portnummer.
        - Benutzer-ID und Kennwort.
        - Datenbankname.
        - Verschlüsselung.
22. **Testen** Sie die Konfiguration, um sicherzustellen, dass die Einstellungen gültig sind.
    a) Klicken Sie auf **Konfiguration** > **Aktionsmenü** > **Test**
    Der Mail-Server-Verbindungstest schlägt fehl, wenn der Mail-Server nicht konfiguriert ist.
23. **Starten** Sie die **Anwendungsebene**.
24. Sie können jetzt unter `<apllicationtierserver:portnumber/bi>` auf Cognos Analytics zugreifen.

Installation der Gatewayebene

Vorgehensweise zum Installieren des Gateways für IBM Cognos Analytics 11.1.x.

Installieren Sie das Gateway, wenn Sie erweiterte Optionen einrichten möchten, wie z. B. Single Sign-on mit Kerberos-Sicherheit mit IIS oder eine Architektur, bei der der Web-Server außerhalb einer Firewall öffentlich zugänglich ist. IBM Cognos Analytics verwendet den Web-Server für den Lastausgleich bestimmter Anforderungen zusätzlich zum Hosting und zur Bereitstellung statischer Inhalte wie Symbole und Bilddateien.

Wichtig: Sie müssen vollständig qualifizierte Hostnamen in den Werten für die folgenden Felder von Cognos Configuration angeben. Jeder Wert, den Sie angeben, muss auch im Feld **Subject Alternative Name** > **DNS-Namen** oder im Feld **Subject Alternative Name** > **IP-Adressen** angezeigt werden.

- **Umgebung**
  - **Gateway-URI**
  - **Externer Dispatcher-URI**
  - **Interner Dispatcher-URI**
  - **Dispatcher-URI für externe Anwendungen**
  - **Content Manager-URIs**
- **Umgebung** > **Konfigurationsgruppe**
  - **Gruppenkontakthost**
  - **Host für die Koordination von Mitgliedern**
- **Zugriffsschutz** > **Verschlüsselung** > **Cognos**
  - **Allgemeiner Servername**
  - **Subject Alternative Name** > **DNS-Namen**
  - **Subject Alternative Name** > **IP-Adressen**

Vorgehensweise

1. Laden Sie das Installationsprogramm und das Repository herunter.
   Laden Sie sie von Passport Advantage herunter.
2. Doppelklicken Sie auf die Installationsdatei und verweisen Sie auf das Repository, wenn Sie dazu aufgefordert werden.
3. Wählen Sie **IBM Cognos Analytics** und die gewünschte Installationsposition aus.
4. Wählen Sie **Gateway** aus, wenn Sie dazu aufgefordert werden, und führen Sie die Installationsschritte aus.
5. Navigieren Sie zur Verknüpfungsposition und starten Sie **Cognos Configuration**.
6. Klicken Sie auf **Umgebung**.
7. Geben Sie unter **Gateway-Einstellungen** den Dispatcher-URI für das Gateway zum Server/Port an, auf dem die **Anwendungsebene** installiert wurde.
   Beispielformat: `<http://applicationTierServer:applicationTierPort/bi/v1/disp>`
8. Klicken Sie auf **Lokale Konfiguration** > **Aktionsmenü** > **Test**, um die Konfiguration zu testen.
9. **Speichern** Sie die Konfiguration.
10. Starten Sie die **Inhaltsebene**.

Kapitel 5. Unbeaufsichtigte Installation, Deinstallation und Konfiguration

Verwenden Sie eine unbeaufsichtigte Installation, Deinstallation und Konfiguration, um die folgenden Schritte auszuführen:

- Installieren einer identischen Konfiguration auf mehreren Computern im Netz
- Automatisieren des Installations- und Konfigurationsprozesses durch Angabe von Optionen und Einstellungen für Benutzer
- Installation und Konfiguration von Komponenten in einer UNIX- oder Linux-Umgebung, die nicht über XWindows verfügt
- Deinstallation von IBM Cognos Analytics.

Bevor Sie eine unbeaufsichtigte Installation und Konfiguration einrichten, müssen Sie sicherstellen, dass alle Systemanforderungen und Voraussetzungen erfüllt und alle weiteren benötigten Programme installiert und konfiguriert sind.

Verwenden einer unbeaufsichtigten Installation

Verwenden Sie die unbeaufsichtigte Installation, um ein Duplikat einer Installation auf einem Computer auf einem anderen Computer zu erstellen, ohne Informationen eingeben zu müssen.

Vorgehensweise

1. Stellen Sie sicher, dass die Umgebungsvariable **DISPLAY** nicht festgelegt ist.
2. Verwenden Sie entweder die Angaben in „Verwenden einer Antwortdateivorlage" auf Seite 33 oder führen Sie den Installationsassistenten über eine Befehlszeile aus und verwenden Sie dabei einen Parameter zum Speichern einer Antwortdatei.

   Beispiel:

   Windows: `analytics-installer-2.0.<build>-win.exe -DREPO=<RepoZipPath> -r "C:\ResponseFile\ResponseFile.properties"`.

   UNIX oder Linux: `analytics-installer-<build>-<platform>.bin -DREPO=<RepoZipPath> -r "./ResponseFile/ResponseFile.properties"`

   Anmerkung:

   - Das Verzeichnis, z. B. `C:\ResponseFile`, muss vorhanden sein, bevor der Installationsassistent ausgeführt wird.
   - <RepoZipPath> bezieht sich auf die Speicherposition der komprimierten Datei `repository.zip`. Stellen Sie beim Aktualisieren von Cognos Analytics sicher, dass der Pfad auf die Version der für die neue Version des Produkts heruntergeladenen Datei verweist.
   - Zusätzliche Befehlszeilenoptionen finden Sie hier: Befehlszeilenoptionen (https://helpnet.flexerasoftware.com/installanywhere2017/Content/helplibrary/ia_ref_command_line_install_uninstall.htm).

   Sie müssen keine vollständige Installation ausführen, um eine Antwortdatei zu erstellen. Sie können die Installation mit der Option -r starten, bis zur Zusammenfassungsanzeige ausführen und dann abbrechen. Die Antworteigenschaftendatei wird beim Beenden der Installation erstellt.
3. Ändern Sie nach dem Abschluss der Installation die Antwortdatei nach Bedarf.

   Die in der Antwortdatei enthaltenen Werte entsprechen den Werten, die verwendet wurden, als der Installationsassistent zum Erstellen der Antwortdatei ausgeführt wurde. Das während der Installation angegebene Kennwort wird in der Antwortdatei verschlüsselt.

4. Führen Sie auf dem Computer, auf dem Sie die Software installieren möchten, eine der folgenden Aktionen aus.
   - Legen Sie den entsprechenden Produktinstallationsdatenträger ein und kopieren Sie den Inhalt des Datenträgers auf Ihren Computer.
   - Kopieren Sie die heruntergeladenen Produktinstallationsdateien auf Ihren Computer.
5. Wechseln Sie in einem Befehls- oder Terminalfenster in das Betriebssystemverzeichnis, in das Sie die Installationsdateien kopiert haben, und geben Sie den folgenden Befehl ein:
   - Unter Windows, wobei *Position* das Verzeichnis angibt, in dem Sie die Datei *Name der Antwortdatei* erstellt bzw. in das Sie diese Datei kopiert haben:

     `analytics-installer-2.0.<build>-win.exe -DREPO=<RepoZipPath> -f Position\Name der Antwortdatei -i silent`

     Tipp:

     Starten Sie die Antwortdatei für eine unbeaufsichtigte Installation über eine Stapeldatei. Dabei wartet der Installationsprozess so lange mit der Rückgabe, bis die Installation vollständig abgeschlossen ist. Fügen Sie außerdem einen Zurückmeldebefehl des Typs `%errorlevel%` am Ende der Stapeldatei hinzu, um den Beendigungscode der Einträge der Installationsbatchdatei zu kennen. Beispiel: `install_location\analytics-installer-2.0.<build>-win.exe -DREPO=<RepoZipPath> -i silent -f Position\Name der Antwortdatei echo %errorlevel%`

     Falls bei der Installation ein Fehler auftritt, kann das Installationsfenster mit Eingabeaufforderung ohne Verzögerung einige wichtige Informationen anzeigen. Bei Erfolg ist der angezeigte Beendigungscode 0 (null). Wenn der Beendigungscode nicht 0 ist, gibt es zwei Möglichkeiten:

     a. Das Installationsprotokoll kann unter `Installationsposition\logs\IBM_Cognos_Analytics_Install_<timestamp>.log` eingesehen werden.
     b. Öffnen Sie ein weiteres Ausgabeprotokoll im temporären Ordner des Benutzers und lesen Sie es: `%TEMPDIR%\install_output_log_cognos_analytics.txt`. In dieser Protokolldatei wird eine Liste der möglichen Beendigungscodes samt Beschreibungen angezeigt. Für weitere Details können Sie auch nach der Wortfolge `Installationsfehler:` suchen.
   - Unter UNIX oder Linux:

     `analytics-installer-<build>-<platform>.bin -DREPO=<RepoZipPath> -f Position/Name der Antwortdatei -i silent`
   - Zur Installation in einer unterstützten Sprache verwenden Sie die Option `-l <Sprachencode>`.

     Beispiel: Zum Installieren in der französischen Sprache und Erstellen einer Antwortdatei:

     Windows: `analytics-installer-2.0.<build>-win.exe -DREPO=<RepoZipPath> -l <lang_code> –r Position\Name der Antwortdatei.`

     UNIX oder Linux: `analytics-installer-<build>-<platform>.bin -DREPO=<RepoZipPath> -l <lang_code> –r Position/Name der Antwortdatei`

     Geben Sie zum Verwenden der Antwortdatei und Installieren in französischer Sprache unter Windows zum Beispiel Folgendes an:

     `analytics-installer-2.0.<build>-win.exe -DREPO=<RepoZipPath> -l fr -i silent -f c:\responselocation\responsefile.properties echo %errorlevel%`

Tabelle 9. Unterstützte Sprachencodes	
Code	**Sprache**
en	Englisch
es	Spanisch
fr	Französisch

Tabelle 9. Unterstützte Sprachencodes (Forts.)	
Code	**Sprache**
it	Italienisch
ja	Japanisch
ko	Koreanisch
pt_BR	Portugiesisch (Brasilien)
zh_CN	Vereinfachtes Chinesisch
zh_TW	Traditionelles Chinesisch

Ergebnisse

Wenn ein anderer Rückgabestatus als null (0) zurückgegeben wird, prüfen Sie die Protokolldateien auf Fehlernachrichten. Fehler werden im Verzeichnis *Installationsposition*\logs in einer zusammenfassenden Fehlerprotokolldatei erfasst. Der Dateiname hat das Format tl-*Produktcode-Version-jjjjmmtt-hhmm*_summary-error.txt.

Wenn Fehler vor einer ausreichenden Initialisierung auftreten, werden die Protokollnachrichten an eine Protokolldatei im Temp-Verzeichnis gesendet. Der Dateiname hat das Format tl-*Produktcode-Version-jjjjmmtt-hhmm*.txt.

Nachdem alle Fehler behoben sind, können Sie eine unbeaufsichtigte Konfiguration einrichten.

Verwenden einer Antwortdateivorlage

Sie können eine Vorlage verwenden, um eine Antwortdatei zu erstellen, anstatt eine Installation zur Generierung der Antwortdatei auszuführen.

Dieses Thema enthält drei Antwortdateivorlagen für die folgenden Typen von Installationen: benutzerdefinierte Installation, Installation des Typs Easy Install und Clientinstallation.

Vorgehensweise

1. Sie können die Antwortdatei, die Sie für eine benutzerdefinierte Installation oder eine Installation des Typs Easy Install verwenden möchten, mithilfe der Vorlagen in diesem Abschnitt erstellen, indem Sie den entsprechenden Text ausschneiden und kopieren.
2. Nehmen Sie Änderungen an der erstellten Antwortdatei vor, indem Sie die entsprechenden Anleitungen in der Datei befolgen.

Antwortdateivorlage für benutzerdefinierte Installation

```
#Antwortdateivorlage für die unbeaufsichtigte Installation der IBM Cognos Analytic-Software
#
#Diese Vorlage bezieht sich auf eine benutzerdefinierte Installation. Wenn Sie eine Installa
tion des Typs
#Easy Install durchführen möchten, verwenden Sie die andere, weiter unten angeführte Vorlage.
#
#(C) Copyright IBM(R) Corp. 2016. All rights reserved.

#Erstellen Sie eine Kopie dieser Datei, bevor Sie sie bearbeiten.

#Ändern Sie die folgende Variable nicht, da es sich hierbei um eine benutzerdefinierte In
stallation handelt.
BISRVR_INSTALLTYPE_CUSTOM=1

#Erforderlich - Installationstyp für benutzerdefinierte Installation
#-------------------------------------------------------------
#Wählen Sie einen der folgenden Installationstypen aus.
#Für "Benutzerdefinierte Installation/Erstinstallation" legen Sie für
#BISRVR_CUSTOM_FIRST den Wert 1 fest, für die andere Option den Wert 0.
```

```
#Für "Benutzerdefinierte Installation/Verbindung herstellen und installieren"
#legen Sie für BISRVR_CUSTOM_EXPAND den Wert 1 fest, für die andere Option den Wert 0.
#-----------------------------------------------------------
BISRVR_CUSTOM_FIRST=
BISRVR_CUSTOM_EXPAND=

#Erforderlich - Features
#-------------------------------------------------------------------------
#Für "Benutzerdefinierte Installation/Erstinstallation" muss das Feature DATATIER
#ausgewählt werden. Andere Features können gleichzeitig ausgewählt werden.
#Für eine benutzerdefinierte Erweiterungsinstallation muss mindestens eines der Features aus
gewählt werden.
#
#BISRVR_FEATURE_DATATIER wird bei der GUI-Installation als "Inhaltsrepository" bezeichnet.
#BISRVR_FEATURE_APPTIER wird bei der GUI-Installation als "Anwendungsservices" bezeichnet.
#BISRVR_FEATURE_GATEWAY wird bei der GUI-Installation als "Optionales Gateway" bezeichnet.
#-------------------------------------------------------------------------
REPO=<RepoZipPath>
BISRVR_FEATURE_DATATIER=
BISRVR_FEATURE_APPTIER=
BISRVR_FEATURE_GATEWAY=

#Erforderlich - Installationsposition
#-------------------------------------------
#Installationsverzeichnis
#In der GUI als Installationsposition bezeichnet
# Standardeinstellung:
#   unter UNIX und Linux
#         /opt/ibm/cognos/analytics
#   unter Windows
#   C:\\Programme\\ibm\\cognos\\analytics
#-------------------------------------------
USER_INSTALL_DIR=


#Optional - Optionen für Windows-Installation
#-------------------------------------------------------------------------------
#Die beiden folgenden Einträge beziehen sich ausschließlich auf Windows.
#BISRVR_SHORTCUT wird bei der GUI-Installation als "Programmordner" bezeichnet.
#BISRVR_ALLUSERS wird bei der GUI-Installation als "Verknüpfung für alle Benutzer im
#Startmenü sichtbar machen" bezeichnet. 1 angeben, wenn die Verknüpfung sichtbar sein soll.
#-------------------------------------------------------------------------------
#BISRVR_SHORTCUT=
#BISRVR_ALLUSERS=

#Ende der Vorlage für eine benutzerdefinierte Installation.
#-------------------------------------------------------------------------------
```

Antwortdateivorlage für Installation des Typs "Easy Install"

```
#Antwortdateivorlage für die unbeaufsichtigte Installation der IBM Cognos Analytic-Software
#
#Diese Vorlage bezieht sich auf eine Installation des Typs "Easy Install". Wenn Sie eine
benutzerdefinierte
#Installation durchführen möchten, verwenden Sie die andere, oben angeführte Vorlage.
#
#(C) Copyright IBM(R) Corp. 2016. All rights reserved.

#Erstellen Sie eine Kopie dieser Datei, bevor Sie sie bearbeiten.

#Erforderlich - Installationstyp für "Easy Install"
#-----------------------------------------------------------------
#Wählen Sie einen der folgenden Installationstypen aus.
#Für eine Installation des Typs "Easy Install/Erstinstallation"
#legen Sie für BISRVR_INSTALLTYPE_READY den Wert 1 fest, für die andere Option den Wert 0.
#Für eine Installation des Typs "Easy Install/Verbindung herstellen und installieren"
#legen Sie für BISRVR_INSTALLTYPE_EXPAND den Wert 1 fest, für die andere Option den Wert 0.
#-----------------------------------------------------------------
REPO=<RepoZipPath>
BISRVR_INSTALLTYPE_READY=
BISRVR_INSTALLTYPE_EXPAND=

#Erforderlich - Installationsposition
#-------------------------------------------
#Installationsverzeichnis
#In der GUI als Installationsposition bezeichnet
# Standardeinstellung:
#   unter UNIX und Linux
#         /opt/ibm/cognos/analytics
```

```
#   unter Windows
#   C:\\Programme\\ibm\\cognos\\analytics
#-------------------------------------------
USER_INSTALL_DIR=

#Erforderlich - Für "Easy Install" erforderliche Eingabe
#-------------------------------------------------------------------------
#Cognos-Administratorberechtigungsnachweise sind für "Easy Install" erforderlich.
#BISRVR_COGNOSUSER wird bei der GUI-Installation als "Cognos-Administrator-ID" bezeichnet.
#BISRVR_COGNOSUSER_PASSWORD wird bei der GUI-Installation als "Kennwort" bezeichnet.
#Das Kennwort muss verschlüsselt sein. Es kann durch Aufzeichnen einer GUI-Installation er
mittelt werden.
#-------------------------------------------------------------------------
BISRVR_COGNOSUSER=
BISRVR_COGNOSUSER_PASSWORD=

#Optional - Optionen für Windows-Installation
#-------------------------------------------------------------------------
#Die beiden folgenden Einträge beziehen sich ausschließlich auf Windows.
#BISRVR_SHORTCUT wird bei der GUI-Installation als "Programmordner" bezeichnet.
#BISRVR_ALLUSERS wird bei der GUI-Installation als "Verknüpfung für alle Benutzer im
#Startmenü sichtbar machen" bezeichnet. 1 angeben, wenn die Verknüpfung sichtbar sein soll.
#-------------------------------------------------------------------------
#BISRVR_SHORTCUT=
#BISRVR_ALLUSERS=

#Ende der Vorlage für eine Easy Install-Installation.
#-------------------------------------------------------------------------
```

Antwortdateivorlage für Clientinstallation

Zu den Clientanwendungen gehören: Framework Manager (CA_FM), Lifecycle Manager (CA_LCM), Cognos Cube Designer (CA_DCUBEMODEL), Dynamic Query Analyzer (CA_DQA) und Cognos Analytics for Jupyter Notebook Server (CA_JUPYTER).

```
#Antwortdateivorlage für die unbeaufsichtigte Installation der IBM Cognos Analytic-Software#
#Diese Vorlage bezieht sich auf eine Installation von Client-Tools.#
#(C) Copyright IBM(R) Corp. 2016. All rights reserved.

#Erstellen Sie eine Kopie dieser Datei, bevor Sie sie bearbeiten.

#Ändern Sie diesen Variablenwert nicht, da dies keine CA-Installation ist
#-----
BISRVR_CA_INSTALL=0

#Ändern Sie dies nicht, da diese Antwortdatei für Tools verwendet wird
#----
BISRVR_CA_TOOLS_INSTALL=1

#Legen Sie nur ein Client-Tool fest, das Sie für 1 installieren müssen
#-----
CA_FM=
CA_LCM=
CA_DCUBEMODEL=
CA_DQA=
CA_JUPYTER=

#Geben Sie die Installationsposition an
USER_INSTALL_DIR=

#Vollständiger Pfad der ZIP-Datei
REPO=
```

Nächste Schritte

Führen Sie die Antwortdatei aus, wie in den Anweisungen im Abschnitt „Verwenden einer unbeaufsichtigten Installation” auf Seite 31 beschrieben.

Verwenden einer unbeaufsichtigten Konfiguration

Zur Verwendung einer unbeaufsichtigten Konfiguration müssen Sie eine Konfiguration aus einer vorhandenen Installation exportieren, die dieselben IBM Cognos Analytics-Komponenten umfasst. Anschließend können Sie IBM Cognos Configuration im Hintergrundmodus ausführen.

Die exportierte Konfiguration enthält die Eigenschaften der IBM Cognos Analytics-Komponenten, die Sie auf einem Computer installiert haben.

Vorbereitende Schritte

Vergewissern Sie sich, dass die Konfigurationseinstellungen auf dem Computer, auf dem Sie den Export der Konfiguration durchführen, für die Verwendung auf einem anderen Computer mit den gleichen installierten Komponenten geeignet sind. Wenn Sie zum Beispiel den Hostnamen in der Eigenschaft **Gateway-URI** von "localhost" in eine IP-Adresse oder einen Computernamen ändern, müssen Sie sicherstellen, dass diese Einstellung für die Konfiguration des neuen Computers geeignet ist.

Vorgehensweise

1. Klicken Sie in IBM Cognos Configuration im Menü **Datei** auf **Exportieren als**.
2. Klicken Sie in der Eingabeaufforderung auf **Ja**, um den Inhalt unverschlüsselt zu exportieren.
3. Wenn die aktuelle Konfiguration in einen anderen Ordner exportiert werden soll, können Sie diesen im Feld **Suchen in** suchen und öffnen.
4. Geben Sie im Feld **Dateiname** einen Namen für die Konfigurationsdatei ein.
5. Klicken Sie auf **Speichern**.
6. Kopieren Sie die exportierte Konfigurationsdatei in das Verzeichnis *installationsposition*/configuration auf den Computer, auf dem eine unbeaufsichtigte Konfiguration durchgeführt werden soll.
7. Ändern Sie den Namen der Datei in `cogstartup.xml`.
8. Wechseln Sie in das Verzeichnis *installationsposition*/bin oder *installationsposition*/bin64.
9. Geben Sie den folgenden Befehl ein:
   - Geben Sie unter UNIX oder Linux Folgendes ein:

     ```
     ./cogconfig.sh -s
     ```
   - Geben Sie unter Windows Folgendes ein:

     ```
     cogconfig.bat -s
     ```

   Tipp: Um Protokollnachrichten anzuzeigen, die während einer unbeaufsichtigten Konfiguration generiert wurden, öffnen Sie die Datei `cogconfig_response.csv` im Verzeichnis *installationsposition*/logs.

   Sie können prüfen, ob die unbeaufsichtigte Konfiguration erfolgreich war, indem Sie den Rückgabestatus überprüfen. Bei Erfolg wird der Wert null (0) zurückgegeben, alle anderen Werte weisen auf einen Fehler hin.

Ergebnisse

IBM Cognos Configuration wendet die in der Datei `cogstartup.xml` angegebenen Konfigurationseinstellungen an, verschlüsselt Berechtigungsnachweise, generiert digitale Zertifikate und startet gegebenenfalls den IBM Cognos-Service oder -Prozess.

Verwenden einer unbeaufsichtigten Deinstallation

Verwenden Sie eine unbeaufsichtigte Deinstallation zum automatischen Entfernen von Komponenten auf mehreren Computern, die über dieselben Komponenten verfügen, oder zum Entfernen von Komponenten in einer UNIX- oder Linux-Umgebung, die nicht über XWindows verfügt.

Tipp: Wenn Überwachungstools, wie z. B. Process Explorer oder MMC (Microsoft Management Console), während der Deinstallation aktiv sind, beeinträchtigen sie das Löschen der Services. Dies gilt für alle Services im Allgemeinen. Zum Beispiel werden nach der Deinstallation von Cognos Analytics Produktservices, wie z. B. ApacheDS, IBM Cognos und Informix, nicht vollständig entfernt, sondern werden in der Serviceanzeige als gestoppt und inaktiviert angezeigt. Um dies zu vermeiden, sorgen Sie dafür, dass

keine Überwachungstools während der Deinstallation aktiv sind. Wenn diese Überwachungstools nach der Deinstallation beendet werden, wird auch das Entfernen der Services abgeschlossen.

Vorgehensweise

Führen Sie den Deinstallationsassistenten über eine Befehlszeile mit den folgenden Parametern aus:

Windows: *Installationsposition*/uninstall/Uninstall_IBM_Cognos_Analytics.exe -i silent.

UNIX oder Linux: ./*Installationsposition*/uninstall/Uninstall_IBM_Cognos_Analytics -i silent

Kapitel 6. Installation von IBM Cognos Analytics for Jupyter Notebook Server

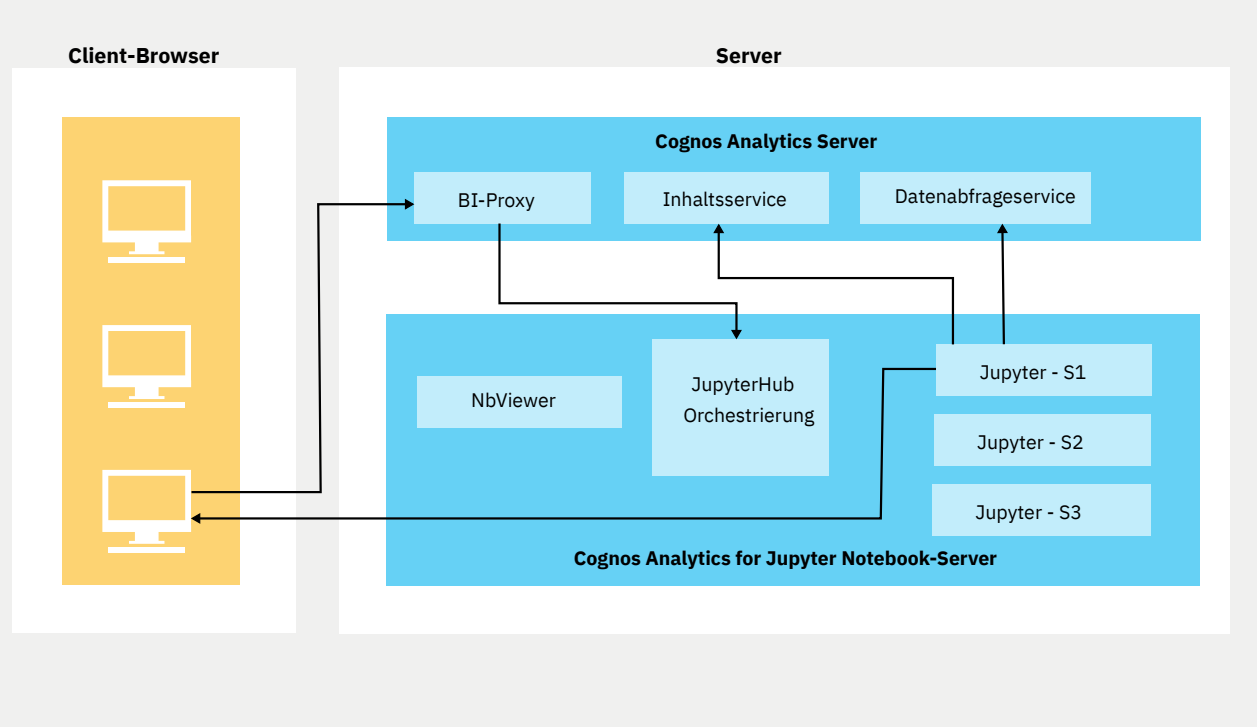
IBM Cognos Analytics enthält eine Version von Jupyter Notebook, die als separater Installer verfügbar ist.

Nach der Installation von Jupyter Notebook Server können Cognos Analytics-Benutzer Jupyter Notebook in Cognos Analytics erstellen und bearbeiten.

Die beiden Hauptkomponenten von Jupyter Notebook Server sind JupyterHub und der Notebook-Viewer (NbViewer). JupyterHub ist der Orchestrator, der mehrere Serverinstanzen verwaltet.

IBM Cognos Analytics for Jupyter Notebook Server kann auf demselben Computer wie IBM Cognos Analytics Server oder auf einem anderen Computer installiert werden. Das folgende Diagramm zeigt die Serverarchitektur.

Architektur von IBM Cognos Analytics for Jupyter Notebook



Bevor Sie Cognos Analytics for Jupyter Server installieren, ermitteln Sie Ihre Hardwarevoraussetzungen.

Nach der Installation und Konfiguration von IBM Cognos Analytics for Jupyter Notebook Server muss der Administrator die folgenden Tasks ausführen:

- Zuweisen der Funktion 'Notebook' zu den entsprechenden Benutzern. Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung*.
- Aktivieren von IBM Cognos Analytics for Jupyter Notebook. Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung*.

Hardwarevoraussetzungen für Jupyter Notebook Server

Die Hardwarevoraussetzungen für eine Installation von Cognos Analytics for Jupyter Server hängen von der Anzahl der gleichzeitig angemeldeten Notebook-Benutzer und der Komplexität ihrer Arbeitsaktivitäten ab.

Beachten Sie die folgenden beiden Faktoren, um die Dimensionierungsanforderungen Ihrer Installation von Cognos Analytics Jupyter Server zu bestimmen:

- Die Anzahl der aktiven Notebook-Sitzungen, die gleichzeitig ausgeführt werden
- Die Komplexität der in Notebook ausgeführten Operationen

Dieser Abschnitt enthält grobe Schätzungen für Dimensionierungsbeispiele.

Anmerkung: In den folgenden Dimensionierungsbeispielen gelten die ersten drei für einen einzelnen Cognos Analytics Jupyter Server. Sie können jedoch auch eine Clusterarchitektur hinter einem Reverse Proxy bereitstellen. Eine Beschreibung findet sich in diesem High-Failover-Beispiel (https://community.ibm.com/community/user/businessanalytics/blogs/antonio-marziano/2019/06/18/setup-failover-jupyter-using-nginx-reverse-proxy).

Dimensionierungsbeispiel 1

- **Verwendungsmuster:** Für 10 - 20 Data-Scientists mit ungefähr fünf gleichzeitigen Notizbuch-Sitzungen (Bearbeitung/Ausführung/Zeitplanung).
- **Dimensionierungsanforderungen:** Minimal.

  Anmerkung: Notebook-Konsumenten, wie z. B. Widgets in Berichten/Dashboards, oder Benutzer, die Notebooks im Nur-Lese-Modus (nbViewer) anzeigen, haben keinen wesentlichen Einfluss auf die Ressourcenanforderungen. Nur Notebook-Benutzer, die Notebooks gleichzeitig bearbeiten, ausführen und planen, haben einen erhöhten Ressourcen bedarf.

Dimensionierungsbeispiel 2

- **Verwendungsmuster:** Für Verwendungsmuster mit geringer Komplexität, wie z. B. Datenbereinigung und Visualisierungen.
- **Dimensionierungsanforderungen:**
  - Anzahl der CPU-Cores: 4
  - RAM: 16 Gb

Dimensionierungsbeispiel 3

- **Verwendungsmuster:** Für Verwendungsmuster mit mittlerer Komplexität, wie z. B. Profildatenqualität, Random-Forest-Klassifikationsmerkmal, KNN-Klassifikation und Entscheidungsbäume.
- **Dimensionierungsanforderungen:**
  - Anzahl der CPU-Cores: 16
  - RAM: 64 Gb

Dimensionierungsbeispiel 4

- **Verwendungsmuster:** Für Verwendungsmuster mit höherer Komplexität, wie z. B. Deep-Learning-Modelle oder neuronale Netze mit pyTorch/TensorFlow.
- **Dimensionierungsanforderungen:**
  - Verwendungsmuster mit hoher Komplexität haben ein anderes Ressourcenprofil.
  - Im Folgenden finden Sie z. B. die Mindestvoraussetzungen für eine IBM DSX-Local-Installation mit vier Knoten (https://www.ibm.com/support/knowledgecenter/SSAS34_1.2.1/local/requirements.html?view=kc#requirements__5node).

Installation von Jupyter Notebook Server unter Linux

Sie können IBM Cognos Analytics for Jupyter Notebook Server auf demselben Computer oder einem anderen Computer als dem, auf dem Cognos Analytics installiert ist, installieren.

Jupyter Notebook Server unterstützt Linux- und Windows 10-Plattformen und setzt voraus, dass Docker installiert ist.

Anmerkung: Docker CE (Community Edition), Docker EE (Enterprise Edition) und Docker Desktop (CE) werden zum gegenwärtigen Zeitpunkt unterstützt.

Wenn Sie das Installationsscript herunterladen und ausführen, laden und starten Sie Docker-Container. Mit diesen Containern können Cognos Analytics-Benutzer Jupyter Notebook erstellen und bearbeiten. Standardmäßig ist Cognos Analytics für Jupyter Server mit vielen der gängigsten Python-Pakete für Datascience und Analyse konfiguriert. In Cognos Analytics on Premises 11.1.2 enthält Jupyter Server Pakete von Versionen von Anaconda und PixieDust.

Tipp: Sie können später in Ihrer vorhandenen Installation ein Upgrade der Python-Pakete durchführen.

Vorbereitende Schritte

Installieren Sie Docker unter Linux, bevor Sie Jupyter Notebook Server installieren. Für weitere Informationen folgen Sie den Prozeduren für eine dieser Linux-Distributionen:

- Docker CE for CentOS installieren
- Docker CE for Ubuntu installieren
- Installeren von Docker EE für Red Hat Enterprise Linux

Sie müssen zur Docker-Gruppe hinzugefügt werden, damit ein Docker-Befehl ohne Rootberechtigungen ausgeführt werden kann.

Sie müssen die vollständig qualifizierte Domäne in Cognos Configuration anhand der folgenden Prozedur festlegen:

1. Klicken Sie im Fenster **Explorer** in IBM Cognos Configuration auf **Umgebung**.
2. Legen Sie unter **Dispatcher-URI für externe Anwendungen** den vollständig qualifizierten Domänennamen (FQDN) für den IBM Cognos Analytics-Server fest.
3. Legen Sie unter **Gateway-URI** den vollständig qualifizierten Domänennamen (FQDN) für den IBM Cognos Analytics-Server fest.
4. Klicken Sie auf **Datei > Speichern**.
5. Starten Sie den Cognos Analytics-Service erneut.

Informationen zu diesem Vorgang

Ein Beispiel für die Vorgehensweise zur Installation von Jupyter Notebook Server finden Sie in diesem Video.

Vorgehensweise

1. Laden Sie das IBM Cognos Analytics for Jupyter Notebook Server-Installationsprogramm und das Serverrepository von Passport Advantage herunter.

   Tipp: Im Downloaddokument zu Cognos Analytics 11.1.2 finden Sie heraus, welche Teilenummer Sie herunterladen müssen. Das Installationsprogramm und das Repository für den Jupyter-Server befinden sich nur in den eAssemblies für Linux.
2. Klicken Sie doppelt auf die Installationsdatei.
3. Folgen Sie den Anweisungen im Installationsassistenten, um die Dateien auf Ihren Computer zu kopieren und dort zu installieren.

   Tipp: Sie können die Installation über einer älteren Version von Jupyter Server durchführen.

   Der Ordner *jupyter-installationsposition*`/dist` enthält zwei Unterordner:

   - `dist/images`
   - `dist/scripts`

     Tipp: Der Ordner `dist/scripts/unix` enthält alle Scripts, die Sie ausführen müssen.

Script	Zweck
`build.sh`	Führen Sie diesen Befehl aus, um die Images neu zu erstellen.
`config.conf`	Bearbeiten Sie diese Konfigurationsdatei, um Jupyter-Parameter zu ändern.
`install.sh`	Führen Sie diesen Befehl aus, um die Docker-Container zu laden und zu starten.
`prune.sh`	Führen Sie diesen Befehl aus, um alte Docker-Images zu entfernen.
`start.sh`	Führen Sie diesen Befehl aus, um den Jupyter-Server zu starten.
`stop.sh`	Führen Sie diesen Befehl aus, um den Jupyter-Server zu stoppen.
`uninstall.sh`	Führen Sie diesen Befehl aus, um den Jupyter-Server zu deinstallieren.

4. Stellen Sie sicher, dass Sie für jedes Script über die Ausführungsberechtigungen verfügen:

   Geben Sie Folgendes ein: `chmod -R u+x dist/scripts/unix`
5. Wechseln Sie in das Verzeichnis `dist/scripts/unix`.
6. Geben Sie `./install.sh` ein.

   Das Installationsscript wird ausgeführt.

Ergebnisse

Alle Docker-Images von Jupyter Server werden aus dem Verzeichnis *`jupyter-installationsposition`*`/dist/images` geladen und die Docker-Container werden gestartet.

Nächste Schritte

Nach der Installation von IBM Cognos Analytics for Jupyter Notebook Server können folgende Tasks durchgeführt werden:

- Wenn Sie einige Standardeinstellungen ändern möchten, können Sie Jupyter Notebook Server konfigurieren.
- Der Administrator muss die Funktion 'Notebook' den entsprechenden Benutzern zuordnen. Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung*.
- Der Administrator muss IBM Cognos Analytics for Jupyter Notebook aktivieren. Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung*.

Deinstallieren von Jupyter Notebook Server

Um Jupyter Notebook Server zu deinstallieren, navigieren Sie in das Verzeichnis `dist/scripts/unix` und geben Sie dann `./uninstall.sh` ein.

Installation von Jupyter Notebook Server unter Microsoft Windows 10

11.1.5

Sie können IBM Cognos Analytics for Jupyter Notebook Server for Microsoft Windows 10 nun entweder auf demselben Computer wie Cognos Analytics oder auf einem anderen Computer installieren.

Jupyter Notebook Server unterstützt Linux- und Microsoft Windows 10-Plattformen und setzt voraus, dass Docker installiert ist.

Anmerkung: Docker CE (Community Edition), Docker EE (Enterprise Edition) und Docker Desktop (CE) werden zum gegenwärtigen Zeitpunkt unterstützt.

Wenn Sie das Installationsscript herunterladen und ausführen, laden und starten Sie Docker-Container. Mit diesen Containern können Cognos Analytics-Benutzer Jupyter Notebook erstellen und bearbeiten. Standardmäßig ist Cognos Analytics für Jupyter Server mit vielen der gängigsten Python-Pakete für Datascience und Analyse konfiguriert. In Cognos Analytics on Premises 11.1.2+ enthält Jupyter Server Pakete von Versionen von Anaconda und PixieDust.

Tipp: Sie können später in Ihrer vorhandenen Installation ein Upgrade der Python-Pakete durchführen.

Vorbereitende Schritte

Damit sichergestellt wird, dass Linux-Container auf einem Windows-Host ausgeführt werden können, muss die **Hyper-V-Plattform** aktiv sein.

Gehen Sie wie folgt vor, um dies zu verifizieren:

1. Öffnen Sie die **Systemsteuerung**.
2. Klicken Sie auf **Programme**.
3. Klicken Sie auf **Windows-Features aktivieren oder deaktivieren**.
4. Suchen Sie die Option **Hyper-V** und erweitern Sie sie.
5. Stellen Sie sicher, dass **Hyper-V-Plattform** ausgewählt ist

Installieren Sie Docker unter Windows, bevor Sie Jupyter Notebook Server installieren. Weitere Informationen erhalten Sie, wenn Sie die Prozeduren für Microsoft Windows 10 ausführen:

- Installation von Docker Desktop for Windows

Wichtig: Für den Jupyter-Server ist es erforderlich, dass Docker Linux-Container verwendet. Wenn Ihre Docker Desktop-Installation für die Verwendung von Windows-Containern konfiguriert wurde, führen Sie eine der folgenden Aufgaben aus:

- Klicken Sie mit der rechten Maustaste auf das Docker-Symbol in der rechten unteren Ecke des Fensters und wählen Sie dann die Option zum Wechseln zu Linux-Containern aus.
- Installieren Sie Docker Desktop erneut und stellen Sie sicher, dass Sie nicht die Option für die Verwendung von Windows-Containern anstelle von Linux-Containern auswählen.

Sie müssen zur Docker-Gruppe hinzugefügt werden, damit ein Docker-Befehl ohne Rootberechtigungen ausgeführt werden kann.

Sie müssen die vollständig qualifizierte Domäne in Cognos Configuration anhand der folgenden Prozedur festlegen:

1. Klicken Sie im Fenster **Explorer** in IBM Cognos Configuration auf **Umgebung**.
2. Legen Sie unter **Dispatcher-URI für externe Anwendungen** den vollständig qualifizierten Domänennamen (FQDN) für den IBM Cognos Analytics-Server fest.
3. Legen Sie unter **Gateway-URI** den vollständig qualifizierten Domänennamen (FQDN) für den IBM Cognos Analytics-Server fest.
4. Klicken Sie auf **Datei > Speichern**.
5. Starten Sie den Cognos Analytics-Service erneut.

Vorgehensweise

1. Laden Sie das IBM Cognos Analytics for Jupyter Notebook Server-Installationsprogramm und das Serverrepository von Passport Advantage herunter.

   Tipp: Im Downloaddokument zu Cognos Analytics 11.1.5 finden Sie heraus, welche Teilenummer Sie herunterladen müssen.
2. Klicken Sie doppelt auf die Installationsdatei.

3. Folgen Sie den Anweisungen im Installationsassistenten, um die Dateien auf Ihren Computer zu kopieren und dort zu installieren.

   Tipp: Sie können die Installation über einer älteren Version von Jupyter Server durchführen.

   Der Ordner *jupyter-installationsposition*/dist enthält zwei Unterordner:

   - dist/images
   - dist/scripts

     Tipp: Der Ordner dist/scripts/windows enthält alle Scripts und Konfigurationsdateien für Windows-Installationen.

Script	Zweck
build.bat	Führen Sie diesen Befehl aus, um die Images neu zu erstellen.
config.conf	Bearbeiten Sie diese Konfigurationsdatei, um Jupyter-Parameter zu ändern.
install.bat	Führen Sie diesen Befehl aus, um die Docker-Container zu laden und zu starten.
prune.bat	Führen Sie diesen Befehl aus, um alte Docker-Images zu entfernen.
startup.bat	Führen Sie diesen Befehl aus, um den Jupyter-Server zu starten.
stop.bat	Führen Sie diesen Befehl aus, um den Jupyter-Server zu stoppen.
uninstall.bat	Führen Sie diesen Befehl aus, um den Jupyter-Server zu deinstallieren.

4. Öffnen Sie ein Eingabeaufforderungsfenster mit Administratorrechten.
5. Navigieren Sie zum Verzeichnis dist/scripts/windows.
6. Geben Sie ./install.bat ein.

   Das Installationsscript wird ausgeführt.

Ergebnisse

Alle Docker-Images von Jupyter Server werden aus dem Verzeichnis *jupyter-installationsposition*/dist/images geladen und die Docker-Container werden gestartet.

Nächste Schritte

Nach der Installation von IBM Cognos Analytics for Jupyter Notebook Server können folgende Tasks durchgeführt werden:

- Wenn Sie einige Standardeinstellungen ändern möchten, können Sie Jupyter Notebook Server konfigurieren.
- Der Administrator muss die Funktion 'Notebook' den entsprechenden Benutzern zuordnen. Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung*.
- Der Administrator muss IBM Cognos Analytics for Jupyter Notebook aktivieren. Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung*.

Deinstallieren von Jupyter Notebook Server

Öffnen Sie zur Deinstallation von Jupyter Notebook Server ein Eingabeaufforderungsfenster mit Administratorrechten, navigieren Sie zum Verzeichnis `dist/scripts/windows` und geben Sie dann `./uninstall.bat` ein.

Installieren eines PiP-Pakets in einer Linux-Offlineumgebung

Installieren Sie Jupyter Notebook Server einschließlich des zusätzlichen Pip-Pakets ohne Internetzugang.

Informationen zu diesem Vorgang

Bei der Installation von Jupyter Notebook Server müssen Sie das PixieDust-Package `additional_pip_packages.txt` installieren. Zur Durchführung dieser Aufgabe ist eigentlich Internetzugriff erforderlich, der in einigen Fällen möglicherweise nicht verfügbar ist. Daher müssen Sie also das Package vor der Installation von Jupyter herunterladen.

Vorgehensweise

1. Suchen Sie online die Datei `tar.gz` für Ihr spezielles Package und laden Sie sie herunter.

   Die meisten PiP-Packages können über die PyPI-Website (Python Package Index) unter pypi.org (https://pypi.org) von der Quelle heruntergeladen werden.
2. Navigieren Sie zum Verzeichnis `/opt/ibm/cognos/jupyter/dist/scripts/` und erstellen Sie ein neues Verzeichnis namens `tmp`.
3. Stellen Sie sämtliche Packages vom Typ `tar.gz`, die Sie heruntergeladen haben, in das Verzeichnis `tmp`.
4. Öffnen Sie die Datei `/opt/ibm/cognos/jupyter/dist/scripts/Dockerfile_server_instance` zum Bearbeiten.
5. Ändern Sie die Datei auf die folgende Weise:
   a) Suchen Sie die folgende Zeile:

   ```
   COPY additional_pip_packages.txt /home/ca_user
   ```

   Fügen Sie unter der obigen Zeile die folgende neue Zeile hinzu:

   ```
   COPY tmp/ /tmp/
   ```

   Diese Zeile weist Docker an, Ihre Packages während des Builds in den Docker-Container zu platzieren.

   b) Setzen Sie den folgenden Abschnitt auf Kommentar:

   ```
   #COPY additional_conda_packages.txt .
   #RUN if [ -s additional_conda_packages.txt ]; then \
   # conda install --yes --file additional_conda_packages.txt; \
   # fi \
   #&& rm additional_conda_packages.txt
   ```
6. Speichern Sie die Datei `Dockerfile_server_instance` und achten Sie dabei darauf, dass sie ohne Dateierweiterung gespeichert wird.
7. Öffnen Sie die Datei `/opt/ibm/cognos/jupyter/dist/scripts/additional_pip_packages.txt` zum Bearbeiten.
8. Nehmen Sie die folgenden Änderungen an der Datei vor:
   a) Entfernen Sie die Zeile `pixiedust==1.1.17`
   b) Fügen Sie die Zeile `/tmp/<package-name>.tar.gz` neu hinzu. Stellen Sie sicher, dass der Pfad mit dem genauen Namen Ihrer komprimierten Datei vom Typ `tar.gz` übereinstimmt.
   c) Fügen Sie für jedes Paket, das auf diese Weise installiert werden soll, eine eigene Zeile neu hinzu.

9. Speichern Sie die Datei `additional_pip_packages.txt`.
10. Führen Sie das Script für die Installation unter Linux durch Absetzen des Befehls `/opt/ibm/cognos/jupyter/dist/scripts/unix/install.sh` aus.

Installieren eines PiP-Pakets in einer Windows-Offlineumgebung

Installieren Sie Jupyter Notebook Server einschließlich des zusätzlichen Pip-Pakets ohne Internetzugang.

Informationen zu diesem Vorgang

Bei der Installation von Jupyter Notebook Server müssen Sie das PixieDust-Package `additional_pip_packages.txt` installieren. Zur Durchführung dieser Aufgabe ist eigentlich Internetzugriff erforderlich, der in manchen Fällen möglicherweise nicht verfügbar ist. Daher müssen Sie also das Package vor der Installation von Jupyter herunterladen.

Vorgehensweise

1. Suchen Sie online die Datei `tar.gz` für Ihr spezielles Package und laden Sie sie herunter.

   Die meisten PiP-Packages können über die PyPI-Website (Python Package Index) unter pypi.org (https://pypi.org) von der Quelle heruntergeladen werden.
2. Navigieren Sie zum Verzeichnis `C:\Programme\ibm\cognos\jupyter\dist\scripts` und erstellen Sie ein neues Verzeichnis namens `tmp`.
3. Stellen Sie sämtliche Packages vom Typ `tar.gz`, die Sie heruntergeladen haben, in das Verzeichnis `tmp`.
4. Öffnen Sie die Datei `C:\Programme\ibm\cognos\jupyter\dist\scripts\Dockerfile_server_instance` zum Bearbeiten.
5. Nehmen Sie die folgenden Änderungen an der Datei vor:
   a) Suchen Sie die folgende Zeile:

   ```
   COPY additional_pip_packages.txt /home/ca_user
   ```

   Fügen Sie unter der obigen Zeile die folgende neue Zeile hinzu:

   ```
   COPY tmp/ /tmp/
   ```

   Diese Zeile weist Docker an, Ihre Packages während des Buildvorgangs in den Docker-Container zu stellen.

   b) Setzen Sie den folgenden Abschnitt auf Kommentar:

   ```
   #COPY additional_conda_packages.txt .
   #RUN if [ -s additional_conda_packages.txt ]; then \
   # conda install --yes --file additional_conda_packages.txt; \
   # fi \
   #&& rm additional_conda_packages.txt
   ```
6. Speichern Sie die Datei `Dockerfile_server_instance` und achten Sie dabei darauf, dass sie ohne Dateierweiterung gespeichert wird.
7. Öffnen Sie die Datei `C:\Programme\ibm\cognos\jupyter\dist\scripts\additional_pip_packages.txt` zum Bearbeiten.
8. Nehmen Sie die folgenden Änderungen an der Datei vor:
   a) Entfernen Sie die Zeile `pixiedust==1.1.17`
   b) Fügen Sie die Zeile `/tmp/<package-name>.tar.gz` neu hinzu. Stellen Sie sicher, dass der Pfad mit dem genauen Namen Ihrer komprimierten Datei vom Typ `tar.gz` übereinstimmt.
   c) Fügen Sie für jedes Paket, das auf diese Weise installiert werden soll, eine eigene Zeile neu hinzu.
9. Speichern Sie die Datei `additional_pip_packages.txt`.

10. Führen Sie das Script für die Installation unter Windows durch Absetzen des Befehls `C:\Program-me\ibm\cognos\jupyter\dist\scripts\windows\install.bat` aus.

Jupyter Notebook Server konfigurieren

Wenn Sie einige Standardeinstellungen in IBM Cognos Analytics for Jupyter Notebook Server ändern möchten, können Sie die Datei *Jupyter-Installationsposition*`/dist/scripts/unix/config.conf` für Linux oder die Datei *Jupyter-Installationsposition*`/dist/scripts/windows/config.conf` für Microsoft Windows 10 bearbeiten.

Geben Sie bei Bedarf Werte für die Parameter an, die in der folgenden Tabelle aufgeführt sind:

Parameter	**Beschreibung**
`CERTIFICATES_DIRECTORY_PATH`	Wenn Sie Jupyter Notebook Server mit SSL schützen, geben Sie den Pfad zu dem Verzeichnis ein, das Zertifikate für vertrauenswürdige SSL-Hosts enthält. **Tipp:** Es wird empfohlen, das Verzeichnis, in dem sich die Zertifikate befinden, *außerhalb* des Verzeichnisses *jupyter-installationsposition* zu positionieren. Aus diesem Grund müssen die Zertifikatsdateien nach nachfolgenden Installationen nicht verschoben werden und die Datei `config.conf` kann weiterhin auf die Zertifikate verweisen. Beispiel: `CERTIFICATES_DIRECTORY_PATH=//myjupyterserver.mycompany.com/certificates`
`PROXY_CERTIFICATE_FILE_PATH`	Wenn Sie SSL verwenden, geben Sie den Pfad im PEM-Format (Privacy Enhanced Mail) in die Zertifikatsdatei für Jupyter Server ein. Beispiel: `PROXY_CERTIFICATE_FILE_PATH=//myjupyterserver.mycompany.com/certificates/myjupyterserver.chained.pem`
`PROXY_KEY_FILE_PATH`	Wenn Sie SSL verwenden, geben Sie den Pfad im PEM-Format (Privacy Enhanced Mail) in die Datei mit privatem Schlüssel für das Zertifikat für Jupyter Server ein. Beispiel: `PROXY_KEY_FILE_PATH=//myjupyterserver.mycompany.com/certificates/myjupyterserver.my company.com.rsa.key`
`DOCKER_IMAGES_PATH=../../images`	Wenn sich die Position Ihrer Docker-Images ändert, aktualisieren Sie den Pfad auf die neue Position.

Parameter	Beschreibung
HOST_NAME=$(*hostname*)	Eine Bearbeitung des Hostnamenwerts sollte nicht notwendig sein. Er wird automatisch aufgelöst, wenn der Hostname korrekt festgelegt ist. Um dies zu überprüfen, geben Sie `hostname` in eine Befehlszeile ein. Der vollständig qualifizierte Name des Computers sollte zurückgegeben werden. Ist er nicht korrekt, können Sie den Wert HOST_NAME bearbeiten und den vollständig qualifizierten Namen hinzufügen. Geben Sie z. B. Folgendes ein: `HOST_NAME=myjupyterserver.mycompany.com`
HOST_PORT=8000	Die Portnummer des Jupyter Notebook-Hubs.
11.1.7 COGNOS_HOST	COGNOS_HOST ist ein optionaler Parameter, der den Jupyter-Server auf den Cognos Analytics-Host verweist. Standardmäßig verwendet der Jupyter-Server den Umgebungsparameter **Dispatcher-URI für externe Anwendungen** von Cognos Configuration. Falls erforderlich, kann er hier aber überschrieben werden. Gültige Beispiele: `https://cognos.domain.com:9300`, `http://9.23.132.233:9300` oder `http://another-cognos-host.com`. **Anmerkung:** `localhost` und `127.0.0.1` können nicht verwendet werden.
SERVER_LIMIT=0	Gibt die maximale Anzahl der Benutzer an, die gleichzeitig verbunden werden können. Wird dieser Wert auf 0 gesetzt (der Standardwert), wird keine Begrenzung erzwungen.
MEM_LIMIT=	Gibt den Speichergrenzwert für die Container jedes Benutzers an. Der Wert kann eine Ganzzahl (Byte) oder eine Zeichenfolge mit dem Präfix K, M, G oder T sein. Beispiele: MEM_LIMIT=150M MEM_LIMIT=2G Wenn kein Wert (der Standardwert) vorhanden ist, wird dem Benutzercontainer der Speicher zugeordnet, den er benötigt.
11.1.5 CULL_TIMEOUT	Gibt den Inaktivitätszeitraum für die einzelnen Container an, nach dessen Ablauf diese vom Bereinigungsservice entfernt werden (der Standardwert beträgt 3600 Sekunden).

Wichtig: Nachdem Sie Änderungen an der Datei `config.conf` vorgenommen haben, müssen Sie die folgenden Schritte ausführen:

1. Führen Sie das Script `dist/scripts/unix/build.sh` für Linux oder das Script `dist/scripts/windows/build.bat` für Windows aus, um die Änderungen anzuwenden.
2. Führen Sie das Script `dist/scripts/unix/startup.sh` für Linux oder das Script `dist/scripts/windows/startup.bat` für Windows aus, um die Änderungen anzuzeigen.

Konfigurieren des Cognos Analytics-Gateways für Jupyter Notebook Server

Wenn Sie das Cognos Analytics-Gateway installiert haben und Cognos Analytics for Jupyter Notebook Server integrieren möchten, müssen Sie die vorhandene Gateway-Konfiguration bearbeiten.

Informationen zu diesem Vorgang

Zwischen Jupyter Notebook Server und dem Browser-Client wird die WebSocket-Kommunikation verwendet.

Die Proxy-Schicht im Cognos Analytics-Service verwaltet die Zuteilung von `http://`- und `https://`-Datenverkehr an den Jupyter-Server. Sie kann jedoch keine WebSocket-Anforderungen verteilen. Daher müssen Notebook-WebSocket-Anforderungen die Cognos Analytics-Serviceschicht umgehen und direkt mit dem Jupyter-Service hinter dem Cognos Analytics-Service verbunden werden.

Wenn Cognos Analytics ein Gateway verwendet, können Sie das Umgehen von WebSocket-Datenverkehr konfigurieren, indem Sie der Proxy-Spezifikation eine Rewrite-Regel hinzufügen. Weitere Informationen finden Sie unter "Konfigurieren des Gateways" in der Veröffentlichung *IBM Cognos Analytics - Installation und Konfiguration* .

Vorgehensweise

1. Wenn Sie ein Apache-Gateway verwenden, führen Sie Schritt 4 im Abschnitt "Konfigurieren von Apache HTTP Server oder IBM HTTP Server bei Cognos Analytics" in der Veröffentlichung *IBM Cognos Analytics - Installation und Konfiguration* aus.
2. Wenn Sie ein IIS-Gateway verwenden, gehen Sie wie folgt vor:
   a) Installieren Sie die WebSocket-Protokollunterstützung in IIS. Weitere Informationen finden Sie im Abschnitt WebSocket <webSocket> (https://docs.microsoft.com/en-us/iis/configuration/system.webserver/web socket).
   b) Führen Sie Schritt **6 d** im Abschnitt "Konfigurieren von IIS in Cognos Analytics" aus.
3. Starten Sie den Cognos Analytics-Service erneut.

Jupyter Notebook Server schützen

Mithilfe von SSL-Zertifikaten können Sie Ihre Jupyter Notebook Server-Installation mit SSL-Verschlüsselung schützen.

Die SSL-Zertifikate müssen von einem vertrauenswürdigen Provider stammen, da die Secure Web Sockets-Verschlüsselung die Verwendung von "selbst signierten" Zertifikaten wie HTTPS-Anforderungen nicht zulässt.

Anmerkung: Wenn der Cognos Analytics-Server mit SSL geschützt ist, muss auch Jupyter Notebook Server mit SSL geschützt sein. Ebenso darf Jupyter Notebook Server **nicht** mit SSL geschützt sein, wenn der Cognos Analytics-Server **nicht** mit SSL geschützt ist.

Informationen zu diesem Vorgang

Ein Beispiel für das Schützen von Jupyter Notebook Server finden Sie in diesem Video.

Vorgehensweise

1. Aktualisieren Sie die Datei `config.conf` für die SSL-Verschlüsselung.

a) Legen Sie den Wert für CERTIFICATES_DIRECTORY_PATH auf den Pfad zu dem Verzeichnis fest, das die Berechtigungszertifikate für den Jupyter-Server enthält.

b) Legen Sie den Wert für PROXY_CERTIFICATE_FILE_PATH auf den Pfad zu dem Verzeichnis fest, das die Zertifikatsdatei für den Jupyter-Server enthält.

c) Legen Sie den Wert für PROXY_KEY_FILE_PATH auf den Pfad zu der Datei mit privatem Schlüssel für den Jupyter-Server fest.

Tipp: Weitere Informationen hierzu finden Sie in „Jupyter Notebook Server konfigurieren" auf Seite 47.

2. Stellen Sie sicher, dass der Administrator HTTPS und nicht HTTP angibt, wenn er IBM Cognos Analytics für Jupyter Notebook aktiviert. Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung*.
3. Registrieren Sie den Jupyter-Server beim Cognos Analytics-Server als vertrauenswürdiger Fremdanbieter.

   Unabhängig davon, ob der Cognos Analytics-Server für SSL eingerichtet ist, müssen Sie den Jupyter-Server beim Trust-Service-Store für Cognos Analytics registrieren. Cognos Analytics leitet eine Anforderung nicht an ein HTTPS-Ziel weiter, ohne zuerst (anhand des Zertifikats) zu prüfen, ob das Ziel vertrauenswürdig und authentisch ist.

   Dies beinhaltet das Importieren einer Kopie des Zertifikats für den gesicherten Jupyter-Server mithilfe des ThirdPartyCertificateTool-Dienstprogramms, das mit Cognos Analytics bereitgestellt wird, in den Trust-Service-Store für Cognos Analytics unter dem Verzeichnis *Installationsposition*/bin. Weitere Informationen finden Sie unter "ThirdPartyCertificateTool - Befehle und Beispiele" in in der Veröffentlichung *IBM Cognos Analytics - Installation und Konfiguration*.

   Wenn Sie z. B. ein Zertifikat importieren möchten, geben Sie Folgendes in eine Befehlszeile auf dem Computer ein, auf dem Cognos Analytics installiert ist:

   ThirdPartyCertificateTool -i -T -p NoPassWordSet -r *fully_qualified_pathname_of_jupyter_certificate_file_in_pem_format*
4. **Nur** wenn der Cognos Analytics-Server auch für SSL konfiguriert ist, registrieren Sie den Cognos Analytics-Server beim Jupyter-Server als vertrauenswürdiger Fremdanbieter.

   a) Erstellen Sie auf dem Computer, auf dem Jupyter-Server installiert ist, ein Verzeichnis, in dem die Zertifikate gespeichert werden sollen.

   b) Bearbeiten Sie die Datei config.conf und richten Sie den Parameter CERTIFICATES_DIRECTORY_PATH so ein, dass er auf das soeben erstellte Verzeichnis verweist.

   c) Kopieren Sie für jede Instanz von Cognos Analytics, die eine Verbindung zum Jupyter-Server herstellen wird, im PEM-Format (Privacy Enhanced Mail) für den Cognos Analytics-Server in das Zertifikatsverzeichnis, das Sie in Schritt „4.b" auf Seite 50 konfiguriert haben.

   Wichtig: Auch wenn die Zertifikate das PEM-Format haben müssen, müssen sie über .crt-Dateierweiterungen verfügen.

   d) Erstellen Sie das Image erneut:

   Führen Sie unter Linux *Jupyter-Installationsposition*/dist/scripts/unix/build.sh aus.

   Führen Sie unter Windows *Jupyter-Installationsposition*/dist/scripts/windows/build.bat aus.

   e) Starten Sie den Server erneut:

   Führen Sie unter Linux *Jupyter-Installationsposition*/dist/scripts/unix/start.sh aus.

   Führen Sie unter Windows *Jupyter-Installationsposition*/dist/scripts/windows/startup.bat aus.

Ergebnisse

Jupyter Notebook Server ist mit SSL-Verschlüsselung geschützt.

Upgrade für IBM Cognos Analytics for Jupyter Notebook Server

Sie können ein Upgrade für IBM Cognos Analytics for Jupyter Notebook Server auf eine neuere Version durchführen. Alternativ können Sie die Python-Pakete in Ihrer vorhandenen Installation von IBM Cognos Analytics for Jupyter Notebook Server aktualisieren.

Wichtig: Wenn der IBM Cognos Analytics for Jupyter Notebook-Server und die zugehörigen Bibliotheken von Benutzern angepasst werden, wird nur eine "Best-Effort-Unterstützung" bereitgestellt.

Upgrade der Installation für Linux

Sie können eine neuere Version von IBM Cognos Analytics for Jupyter Notebook Server installieren, ohne dass die aktuelle Version manuell deinstalliert werden muss.

Anmerkung: Diese Aufgabe umfasst die Angabe einer **anderen Position** als Installationsverzeichnis.

Informationen zu diesem Vorgang

Ein Beispiel für ein Upgrade Ihrer Jupyter Server-Installation finden Sie in diesem Video.

Vorgehensweise

1. Führen Sie in „Installation von Jupyter Notebook Server unter Linux” auf Seite 40 die Schritte „1” auf Seite 41 bis „4” auf Seite 42 aus und geben Sie bei entsprechender Aufforderung eine andere Installationsposition an.
2. Wenn Sie ein Upgrade für Cognos Analytics Version 11.1.6 oder eine neuere Version durchführen, kopieren Sie die Dateien `additional_pip_packages.txt` und `additional_conda_packages.txt` im Verzeichnis *`aktuelle_position_der_jupyter-installation`*`/dist/scripts/` und fügen Sie sie in den entsprechenden Ordner an der neuen Speicherposition *`neue_position_der_jupyter-installation`*`/dist/scripts/` ein.
3. Wenn Sie ein Upgrade für Cognos Analytics Version 11.1.5 oder eine Vorgängerversion durchführen, kopieren Sie den Inhalt der Datei `additional_packages.txt` im Verzeichnis *`aktuelle_position_der_jupyter-installation`*`/dist/scripts/` und fügen Sie sie je nach Bedarf in eine oder beide der folgenden Dateien ein:
   - *`neue_position_der_jupyter-installation`*`/dist/scripts/additional_pip_packages.txt`
   - *`neue_position_der_jupyter-installation`*`/dist/scripts/additional_conda_packages.txt`
4. Kopieren Sie die Datei *`aktuelle_position_der_jupyter-installation`*`/dist/scripts/unix/config.conf` und fügen Sie sie in den entsprechenden Ordner an der neuen Position ein: *`neue_position_der_jupyter-installation`*`/dist/scripts/unix/`.
5. Wechseln Sie in das Verzeichnis *`neue_position_der_jupyter-installation`*`dist/scripts/unix`.
6. Geben Sie `./install.sh` ein.

Ergebnisse

Ihre aktuelle Installation wird deinstalliert. Anschließend werden alle Docker-Images von Jupyter Server aus dem Verzeichnis *`neue Jupyter-Installationsposition`*`/dist/images` geladen und die Docker-Container gestartet.

Upgrade der Installation für Microsoft Windows

Sie können eine neuere Version von IBM Cognos Analytics for Jupyter Notebook Server installieren, ohne dass die aktuelle Version manuell deinstalliert werden muss.

Anmerkung: Diese Aufgabe umfasst die Angabe einer **anderen Position** als Installationsverzeichnis.

Informationen zu diesem Vorgang

Ein Beispiel für ein Upgrade Ihrer Jupyter Server-Installation finden Sie in diesem Video.

Vorgehensweise

1. Führen Sie die Schritte 1 bis 4 in Installation von Jupyter Notebook Server unter Microsoft Windows 10 aus und geben Sie eine andere Installationsposition an, wenn Sie dazu aufgefordert werden.
2. Wenn Sie ein Upgrade für Cognos Analytics Version 11.1.6 oder eine neuere Version durchführen, kopieren Sie die Dateien `additional_pip_packages.txt` und `additional_conda_packages.txt` im Verzeichnis *`aktuelle_position_der_jupyter-installation`*`/dist/scripts/` und fügen Sie sie in den entsprechenden Ordner an der neuen Speicherposition *`neue_position_der_jupyter-installation`*`/dist/scripts/` ein.
3. Wenn Sie ein Upgrade für Cognos Analytics Version 11.1.5 oder eine Vorgängerversion durchführen, kopieren Sie den Inhalt der Datei `additional_packages.txt` im Verzeichnis *`aktuelle_position_der_jupyter-installation`*`/dist/scripts/` und fügen Sie sie je nach Bedarf in eine oder beide der folgenden Dateien ein:
   - *`neue_position_der_jupyter-installation`*`/dist/scripts/additional_pip_packages.txt`
   - *`neue_position_der_jupyter-installation`*`/dist/scripts/additional_conda_packages.txt`
4. Kopieren Sie die Datei *`aktuelle Jupyter-Installationsposition`*`/dist/scripts/windows/config.conf` und fügen Sie sie in den entsprechenden Ordner an der neuen Position ein: *`neue Jupyter-Installationsposition`*`/dist/scripts/windows/`.
5. Öffnen Sie ein Eingabeaufforderungsfenster mit Administratorrechten.
6. Navigieren Sie zum Verzeichnis *`neue Jupyter-Installationsposition`*`dist/scripts/windows`.
7. Geben Sie `./install.bat` ein.

Ergebnisse

Ihre aktuelle Installation wird deinstalliert. Anschließend werden alle Docker-Images von Jupyter Server aus dem Verzeichnis *`neue Jupyter-Installationsposition`*`/dist/images` geladen und die Docker-Container gestartet.

Upgrades für Python-Pakete und R-Pakete

Sie können weitere Python-Pakete oder R-Pakete hinzufügen. Sie können außerdem die Versionen vorhandener Python-Pakete in Ihrer IBM Cognos Analytics for Jupyter Notebook Server-Installation aktualisieren.

Um diese Aufgabe zu erfüllen, bearbeiten Sie die Dateien `additional_pip_packages.txt` und `additional_conda_packages.txt`.

Anmerkung: Die Dateien `additional_pip_packages.txt` und `additional_conda_packages.txt` folgen dem Standarddateiformat `requirements.txt`, das in Python verwendet wird, wie im PyPA-Referenzhandbuch (https://pip.pypa.io/en/stable/reference/pip_install/#requirements-file-format) beschrieben.

Vorbereitende Schritte

Entscheiden Sie, ob Sie ein Upgrade durchführen müssen. Überprüfen Sie, welche Versionen von Python-Paketen in Ihrer aktuellen Installation enthalten sind.

Tipp: Um die Inhalte der in der Notebook-Umgebung verfügbaren Module anzuzeigen, geben Sie Folgendes in eine Notebook-Zelle ein:

```
`!pip list --isolated`
```

Für die meisten Python-Pakete können Sie auch zur Laufzeit mit dem Befehl 'pip' ein Modul für das jeweilige Notebook laden. Geben Sie z. B. Folgendes in eine Notebook-Zelle ein:

```
!pip install --user prettyplotlib`
```

Informationen zu diesem Vorgang

Ein Beispiel für die Vorgehensweise zum Upgrade von Python-Paketen finden Sie in diesem Video.

Vorgehensweise

1. Bearbeiten Sie die Datei *Jupyter-Installationsposition*`/dist/scripts/additional_pip_packages.txt`.

   Tipp: Sie können Python-Pakete hinzufügen, indem Sie sie in der Datei `additional_pip_packages.text` angeben.
2. Stoppen Sie den Server:

   Führen Sie für Linux *Jupyter-Installationsposition*`/dist/scripts/unix/stop.sh` aus.

   Führen Sie für Windows *Jupyter-Installationsposition*`/dist/scripts/windows/stop.bat` aus.
3. Erstellen Sie das Image erneut:

   Führen Sie für Linux *Jupyter-Installationsposition*`/dist/scripts/unix/build.sh` aus.

   Führen Sie für Windows *Jupyter-Installationsposition*`/dist/scripts/windows/build.bat` aus.
4. Starten Sie den Server erneut:

   Führen Sie für Linux *Jupyter-Installationsposition*`/dist/scripts/unix/start.sh` aus.

   Führen Sie für Windows *Jupyter-Installationsposition*`/dist/scripts/windows/startup.bat` aus.
5. Bearbeiten Sie die Datei *Jupyter-Installationsposition*`/dist/scripts/additional_conda_packages.txt` und wiederholen Sie die Schritte 2 bis 4.

   Tipp: Sie können sowohl Python-Pakete als auch R-Pakete hinzufügen, indem Sie sie in der Datei `additional_conda_packages.text` angeben.

Hinzufügen zusätzlicher Ubuntu-Betriebssystempackages

In 11.1.5 können Sie Betriebssystempackages zu Jupyter Notebook Server hinzufügen.

Bearbeiten Sie hierzu die Datei `Installationsverzeichnis>/dist/scripts/additional_os_packages.txt`.

Anmerkung: Jeder Packagename muss in einer neuen Zeile stehen.

Prozedur

1. Suchen Sie die Datei `Installationsverzeichnis>/dist/scripts/additional_os_packages.txt`.
2. Fügen Sie den Namen des gewünschten Pakets in einer neuen Zeile hinzu.

3. Speichern Sie die Datei.
4. Führen Sie für Linux das Script 'install.sh' bzw. für Microsoft Windows das Script 'install.bat' für den Server aus.

Fehlerbehebung für IBM Cognos Analytics for Jupyter Notebook Server

Um Probleme mit Jupyter Notebook Server zu beheben, können Sie diesen Docker-Befehl verwenden: `Docker-Protokolle container_id`

JupyterHub kann hilfreiche Informationen geben, die Ihnen bei der Diagnose eines Problems helfen. Geben Sie für IBM Cognos Analytics for Jupyter Notebook Server Folgendes ein:

```
docker logs ca_jupyter_hub
```

Weitere Informationen finden Sie unter Fehlerbehebung (https://jupyterhub.readthedocs.io/en/latest/troubleshooting.html) auf der JupyterHub-Website.

Fehlernachricht aufgrund von fehlendem Speicherplatz bei der Installation von Jupyter Server

Die offizielle Docker-Dokumentation enthält Informationen zum Freigeben von Speicherplatz.

Anmerkung:

Docker speichert den gesamten Inhalt (Container, Images und Datenträger) standardmäßig im Verzeichnis '/var/lib/docker'.

Die Standardspeicherposition kann geändert werden, indem der Schlüssel 'data-root' zur Datei 'daemon.json' hinzugefügt wird.

Weitere Informationen zur Docker-Dämonkonfigurationsdatei sind in den folgenden Ressourcen verfügbar:

https://docs.docker.com/engine/reference/commandline/dockerd/#daemon-configuration-file

Kapitel 7. Verteilungsoptionen

Legen Sie vor der Implementierung von IBM Cognos Analytics fest, wie die Lösung in der verwendeten Umgebung installiert werden soll. Sie können alle Serverkomponenten auf einem Computer installieren oder sie über ein Netz verteilen. Die jeweils optimale Verteilungsmethode hängt von den Berichtsanforderungen, den Ressourcen sowie den Vorgaben ab. Die Konfigurationsanforderungen richten sich danach, ob Sie alle Komponenten auf einem oder auf mehreren Computern installieren.

Cognos Analytics ist kompatibel mit anderen Cognos-Produkten. Wenn in Ihrer Umgebung andere Cognos-Produkte eingesetzt werden, müssen Sie zuvor überlegen, wie Cognos Analytics in diese Umgebung eingepasst werden kann.

Cognos Analytics kann nicht an derselben Position wie andere Cognos-Produkte, z. B. Cognos Framework Manager, Cognos Transformer, Cognos PowerPlay usw., installiert werden.

Cognos Analytics-Komponenten

IBM Cognos Analytics ist eine webbasierte Business-Intelligence-Lösung mit integrierten Funktionen für die Berichterstellung, das Dashboarding, die Analyse, das Ereignismanagement und weiteren Funktionen. Cognos Analytics enthält Server- und Modellierungskomponenten.

Cognos Analytics kann mithilfe von Ressourcen, die sich in Ihrer Umgebung befinden, ohne großen Aufwand in Ihre bestehende Infrastruktur integriert werden. Einige der vorhandenen Ressourcen sind erforderlich, z. B. eine Datenbank für den Content Store. Andere Ressourcen sind optional, z. B. ein Sicherheitsprovider für die Authentifizierung.

Tipp: Wenn Cognos Analytics über die Option **Easy Install** installiert wird, müssen Sie keine Content-Store-Datenbank und keinen Sicherheitsprovider installieren. Das Produkt ist vorkonfiguriert und bereit zur Verwendung.

IBM Cognos Analytics führt WebSphere Application Server Liberty Profile als Anwendungsserver aus.

Serverkomponenten

Die Serverkomponenten für IBM Cognos Analytics sind auf drei Ebenen aufgeteilt: Datenebene, Anwendungsebene und optionale Gateway-Ebene.

Die Serverkomponenten stellen die Benutzerschnittstellen für Berichterstellung, Dashboarding, Analyse, Ereignismanagement usw. sowie die Funktionalität für das Routing und die Verarbeitung von Anforderungen zur Verfügung.

Im Installationsprogramm können Sie auswählen, welche der folgenden Serverkomponenten installiert werden sollen:

- „Inhaltsebene” auf Seite 56
- „Anwendungsebene: Komponenten” auf Seite 56
- „Gatewayebene: Webkommunikation” auf Seite 57

  Tipp: Das optionale Gateway ist nur für Kerberos erforderlich.

Als optionale Serverkomponente können Sie auch Cognos Analytics-Beispiele installieren. Die Beispiele veranschaulichen anhand von Daten eines fiktiven Unternehmens, der Beispielfirma für Outdoor-Ausrüstung, Produktfunktionen und bewährte Verfahren im technischen und geschäftlichen Bereich. Mithilfe dieser Beispiele können Sie Berichtsdesignverfahren testen und gemeinsam verwenden sowie Fehler beheben. Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics - Beispiele*.

Inhaltsebene

Content Manager ist der IBM Cognos Analytics-Service, der den Speicher der Anwendungsdaten, einschließlich Sicherheit, Konfigurationsdaten, Modellen, Berichtsspezifikationen und Berichtsausgaben, verwaltet.

Content Manager wird zum Publizieren von Packages, zum Abrufen und Speichern von Berichtsspezifikationen, zum Verwalten von Zeitplaninformationen und zum Verwalten des Cognos-Namespace benötigt.

Content Manager speichert Informationen in einer Content Store-Datenbank.

Anwendungsebene: Komponenten

Die IBM Cognos Analytics-Anwendungsebene enthält einen oder mehrere Cognos Analytics-Server. Die Server führen Anforderungen (z. B. Berichte, Analysen und Abfragen) aus, die vom Gateway weitergeleitet werden und geben die Schnittstellen wieder.

Konfigurieren und Verwalten des Produkts - IBM Cognos Configuration

IBM Cognos Configuration wird zum Konfigurieren von Cognos Analytics sowie zum Starten und Stoppen der zugehörigen Services verwendet.

Publizieren, Verwalten und Anzeigen von Inhalt - Cognos Analytics-Portal

Cognos Analytics-Portal stellt einen einheitlichen Zugriffspunkt für die Unternehmensdaten bereit, die über die zugehörigen Produkte verfügbar sind. Außerdem bietet es einen einheitlichen Einstiegspunkt, um Daten abzufragen, zu analysieren und zu organisieren und Berichte, Scorecards und Ereignisse zu erstellen. Benutzer können alle webbasierten Cognos Analytics-Anwendungen über das Portal ausführen. Andere Anwendungen und Webadressen zu anderen Anwendungen können in das Portal integriert werden.

Professionelle Berichterstellung

Reporting ermöglicht Berichtserstellern die Erstellung, Bearbeitung und Verteilung einer breiten Auswahl professioneller Berichte.

Dashboarding

Cognos Analytics stellt Dashboards bereit, mit denen Sie Erkenntnisse und Analysen kommunizieren können. Sie können eine Ansicht zusammenstellen, die Visualisierungen wie Grafiken, Diagramme, Kurven, Tabellen, Karten oder sonstige visuelle Darstellungen von Daten enthält.

Ein Dashboard ist ein Ansichtstyp, mit dem Sie Ereignisse und Aktivitäten auf einen Blick überwachen können. Es stellt wichtige Erkenntnisse und Analysen für Ihre Daten auf einer oder mehreren Seiten bzw. in einer oder mehreren Anzeigen bereit.

Zentrale Administration - Verwaltungs- und Administrationskonsole

Cognos Analytics enthält die Funktion **Verwalten**, mit der Sie alltäglich die allgemeinen Administrationsaufgaben durchführen können. Über eine Option im Menü **Verwalten** wird die **Administrationskonsole** geöffnet. Dies ist eine zentrale Verwaltungsschnittstelle, die die administrativen Aufgaben für IBM Cognos Analytics enthält. Sie bietet einfachen Zugriff auf die gesamte Verwaltung der IBM Cognos-Umgebung. Der Zugriff auf die jeweiligen Verwaltungsfunktionen ist von den Berechtigungen der einzelnen Benutzer abhängig.

Durchführen von Ad-hoc-Abfragen und Self-Service-Berichterstellung - Query Studio

Mit Query Studio können Benutzer mit geringer oder sogar ohne Schulung schnell Berichte entwerfen, erstellen und speichern, um Berichtsanforderungen zu erfüllen, die von den in Reporting erstellten professionellen Standardberichten nicht abgedeckt werden.

Überwachen von Daten auf außergewöhnliche Bedingungen - Event Studio

In Event Studio können Sie Agenten erstellen, mit denen Sie Ihre Daten überwachen und Aufgaben ausführen, wenn Geschäftsereignisse oder Ausnahmebedingungen in den Daten auftreten, auf die reagiert werden muss. Beim Auftreten eines Ereignisses werden Benutzer darüber informiert und aufgefordert, bestimmte Aktionen auszuführen. Agenten können Details im Portal publizieren, Alerts per E-Mail übermitteln, Berichte basierend auf Ereignissen ausführen und verteilen sowie den Status von Ereignissen überwachen. So kann z. B. das Anfordern von Unterstützung von einem Hauptkunden oder die Stornierung einer umfangreichen Bestellung ein Ereignis auslösen und veranlassen, dass an die betreffenden Mitarbeiter eine E-Mail gesendet wird.

Hilfe bei Entscheidungsfindung - IBM Cognos Workspace

Sie können entsprechend Ihren Informationsanforderungen komplexe interaktive Arbeitsbereiche unter Verwendung von IBM Cognos-Inhalten und externen Datenquellen wie z. B. TM1 Websheets und CubeViews erstellen. Außerdem können Sie für Arbeitsbereiche und Berichte Favoriten anzeigen und öffnen, den Inhalt ändern und Ihre Ergebnisse per E-Mail senden. Darüber hinaus können Sie auch Kommentare und Aktivitäten für die gemeinsame Entscheidungsfindung verwenden.

Ferner kann zur gemeinsamen Entscheidungsfindung auch Social Software wie z. B. IBM Connections verwendet werden.

Microsoft Office-Kompatibilität - IBM Cognos for Microsoft Office

IBM Cognos for Microsoft Office ermöglicht Microsoft Office-Benutzern, auf Daten und Visualisierungen von IBM Cognos-Berichten in Microsoft Office-Anwendungen (z. B. Excel, PowerPoint und Word) zuzugreifen.

Cognos for Microsoft Office-Komponenten sind in Cognos Analytics enthalten und müssen separat installiert werden.

Gatewayebene: Webkommunikation

Gateways sind häufig CGI-Programme, sie können jedoch auch anderen Standards wie Internet Server Application Program Interface (ISAPI) oder Apache Modules (apache_mod) folgen. IBM Cognos Analytics verwendet nur CGI, ISAPI oder Apache Modules für Kerberos. Andernfalls müssen Sie kein Gateway konfigurieren.

In IBM Cognos Analytics stellt die Anwendungsebene die Funktionen eines Gateways bereit.

Modellierungskomponenten

Modellierungskomponenten strukturieren Daten in Datenquellen so, dass sie für den Benutzer auf sinnvolle Weise abgebildet werden. Modellierungskomponenten enthalten folgende Tools:

IBM Cognos Analytics-Webmodellierung

IBM® Cognos® Analytics enthält ein komfortables Modellierungstool ohne lokalen Speicherbedarf, das Sie dazu verwenden können, Datenmodule aus verschiedenen Datenquellen ohne großen Zeitaufwand zu erstellen. Sie können Datenquellen, wie beispielsweise Datenserver, hochgeladene Dateien und bereits zuvor gespeicherte Datenmodule, zum Erstellen von Datenmodulen verwenden. Die Cognos Analytics-Datenmodellierung verwendet Intent-driven Modeling zur Generierung eines Moduls anhand der von Ihnen definierten Bedingungen. Details zu allen verfügbaren Features finden Sie in der Veröffentlichung *IBM Cognos Analytics - Datenmodellierung*.

Die Cognos Analytics-Datenmodellierung ersetzt nicht die komplexeren Modellierungsfunktionen von IBM Cognos Framework Manager oder IBM Cognos Cube Designer. Diese Tools sind in Cognos Analytics weiterhin verfügbar.

Erstellen einer Geschäftsansicht Ihrer Daten - Framework Manager

IBM Cognos Framework Manager ist ein Modellierungstool, mit dem Sie unternehmensbezogene Metadaten erstellen und verwalten und für die Berichterstellung und Analyse in IBM Cognos Analytics verwenden können. Metadaten werden für die Verwendung durch Berichtstools als Package publiziert und stellen eine einzelne, integrierte Geschäftsansicht einer beliebigen Anzahl von heterogenen Datenquellen bereit.

Framework Manager muss an einer anderen Position als Cognos Analytics installiert werden.

ROLAP-Modellierung - Cube Designer

IBM® Cognos® Cube Designer ist das mit IBM Cognos Dynamic Cubes bereitgestellte Modellierungstool. Mit diesem Tool können Sie dynamische Cubes erstellen und zur Verwendung in IBM Cognos Analytics publizieren.

Als ersten Schritt importieren Sie Metadaten aus einer relationalen Datenbank. Modellieren Sie dynamische Cubes anhand der Metadaten und speichern Sie die Cube-Definitionen in einem Projekt. Nach dem Publizieren der Cubes werden diese als Datenquellen in Content Manager aufgeführt und die zugehörigen Packages stehen Berichtserstellern zur Verfügung.

Cube Designer muss an einer anderen Position als Cognos Analytics installiert werden.

Mehrdimensionale Modellierung - IBM Cognos Transformer

IBM Cognos Transformer ist das Modellierungstool in IBM Cognos Analytics, mit dem PowerCubes zur Verwendung in IBM Cognos Analytics erstellt werden. Gesicherte IBM Cognos Analytics PowerCubes sind nicht mit IBM Cognos Series 7 kompatibel.

Transformer muss an einer anderen Position als Cognos Analytics installiert werden.

Tipp: Informationen zur Installation und Konfiguration von Transformer-Versionen, die älter als Version 8.4 sind, finden Sie in der Dokumentation, die im Lieferumfang von Transformer enthalten ist.

Landkarten importieren und verwalten (nur traditionelle Map Manager-Landkarten)

IBM Cognos Map Manager ist ein Windows-basiertes Dienstprogramm, mit dem Administratoren und Modellierer Landkarten importieren und Beschriftungen für Landkarten in Reporting aktualisieren können. Für Landkarteneinträge wie Länder- oder Regions- und Städtenamen können Administratoren und Modellierer alternative Namen definieren, um auf der Landkarte angezeigten Text in mehreren Sprachen zur Verfügung zu stellen.

Map Manager muss an einer anderen Position als Cognos Analytics installiert werden.

Weitere Informationen finden Sie im *IBM Cognos Map Manager Installation and User Guide*.

Erforderliche Datenbankkomponenten

Zusätzlich zu den bereitgestellten Tools erfordert IBM Cognos Analytics noch die folgenden Komponenten, die mithilfe anderer Ressourcen erstellt werden.

Content Store

Der Content Store ist eine relationale Datenbank und enthält Daten, die für den Betrieb von Cognos Analytics erforderlich sind. Dazu zählen z. B. Berichtsspezifikationen, publizierte Modelle und Packages, in denen diese enthalten sind, sowie Verbindungsinformationen für Datenquellen, Informationen über externe Namespaces und den Cognos-Namespace selbst sowie Informationen über Zeitpläne und Zielgruppenverteilungen für Berichte.

Richten Sie beim Konfigurieren der Cognos Analytics-Umgebung den Content Store so ein, dass er eine unterstützte Datenbank verwendet, die im Hinblick auf Leistung und Stabilität gesichert und optimiert werden kann. Weitere Informationen finden Sie im Abschnitt über die Bereitstellung des gesamten Content Store im Handbuch *IBM Cognos AnalyticsVerwaltung und Sicherheit*.

Designmodelle und Protokolldateien werden nicht im Content Store gespeichert.

Der IBM Cognos-Service, der den Content Store verwendet, wird als Content Manager bezeichnet.

Datenquellen

Bei Datenquellen (so genannten Abfragedatenbanken) handelt es sich um relationale Datenbanken, Dimensions- oder OLAP-Cubes, Dateien oder andere physische Data-Stores, auf die über Cognos Analytics zugegriffen werden kann. Komponenten auf Anwendungsebene greifen über Datenquellenverbindungen auf Datenquellen zu.

Verteilen von Komponenten

Bei der Installation der IBM Cognos Analytics-Serverkomponenten geben Sie die jeweilige Position für die Komponenten der Anwendungsebene, der Datenebene (Content Manager) und der Ebene des optionalen Gateways an.

Sie können die folgenden Installationsszenarios verwenden:

- Installieren aller Komponenten auf einem Computer:

  Diese Option wird normalerweise für abteilungsspezifische Bereitstellungen, als Demonstrationssystem oder in einer Machbarkeitsprüfungsumgebung verwendet.
- Installieren der Komponenten der Anwendungsebene und Installieren von Content Manager auf separaten Computern.

  Wählen Sie diese Option, um die Leistung, Verfügbarkeit, Kapazität oder die Sicherheit basierend auf den Verarbeitungseigenschaften Ihres Unternehmens zu optimieren.
- Installieren des optionalen Gateways auf einem eigenständigen Computer.

  Bei dieser Option befinden sich das Gateway und der Web-Server auf einem Computer und die übrigen Cognos-Komponenten auf anderen Computern. Sie können diese Option wählen, wenn Sie bereits über Web-Server zur Verarbeitung der Anforderungen von Cognos Analytics-Komponenten verfügen.
- Konsolidieren mehrerer Server durch Installation auf System z

  IBM Cognos Analytics wird für Linux on System z unterstützt. Diese Art der Installation ist geeignet, wenn Sie eine Installation in Ihrer Umgebung einrichten oder an Ihre IT- und Infrastrukturanforderungen anpassen möchten.

Nach der Installation der Serverkomponenten müssen Sie diese entsprechend konfigurieren, dass sie miteinander kommunizieren können.

Zusätzlich zur Installation der Komponenten der Datenebene (Content Manager), der Anwendungsebene und der optionalen Gateway-Ebene können Sie Cognos Framework Manager, das Metadatenmodellierungstool, und Cognos Transformer, das Modellierungstool für die Erstellung von PowerCubes, installieren. Unabhängig von dem angewendeten IBM Cognos-Installationsszenario müssen Sie die Modellierungskomponenten an separaten Positionen installieren.

Komponenten der Anwendungsebene und Content Manager auf separaten Computern

Lasten bei Komponenten der Anwendungsebene verteilen, auf Daten zugreifen, Abfragen durchführen, Jobs planen und Berichte ausgeben. Content Manager speichert alle Berichtsspezifikationen, Ergebnisse, Packages, Ordner und Jobs im Content Store.

Sie können die Komponenten der Anwendungsebene und Content Manager auf demselben Computer oder auf verschiedenen Computern installieren. Durch die Installation auf mehreren Computern können Sie die Leistung, Verfügbarkeit und Kapazität steigern.

Mehrere Content Manager

Sie können eine beliebige Anzahl an Content Manager-Instanzen installieren, obwohl immer nur eine Instanz aktiv sein kann. Die anderen Installationen fungieren jeweils als Standby-Content Manager. Eine dieser Installationen wird nur dann aktiv, wenn ein Fehler auftritt, der sich auf den aktiven Content Manager-Computer auswirkt. Aus Gründen des Ausfallschutzes ist es ratsam, Content Manager auf mindestens zwei Computern zu installieren.

Installieren von mehreren Content Manager-Instanzen

Content Manager speichert Daten, die für den Betrieb von IBM Cognos Analytics erforderlich sind. Dazu zählen z. B. Berichtsspezifikationen, publizierte Modelle und die Packages, die diese verwenden, sowie Verbindungsinformationen für Datenquellen, Informationen über den externen Namespace und den Cognos-Namespace selbst sowie Informationen über Zeitpläne und Zielgruppenverteilungen für Berichte. Beim Content Store handelt es sich um ein relationales Datenbankverwaltungssystem (RDBMS). Pro IBM Cognos-Installation steht nur ein Content Store zur Verfügung.

Möglicherweise möchten Sie Content Manager getrennt von den Komponenten der Anwendungsebene installieren. Beispielsweise möchten Sie vielleicht, dass sich Content Manager auf Ihrer Datenebene anstatt auf Anwendungsebene befindet.

Wenn ein aktiver Content Manager ausfällt, gehen die nicht gespeicherten Sitzungsdaten verloren. Sobald der neue aktive Content Manager übernimmt, wird der Benutzer aufgefordert, sich anzumelden.

Im folgenden Diagramm übergibt das Gateway die Abfrage an den Dispatcher (nicht abgebildet), der sie wiederum an den standardmäßig aktiven Content Manager-Computer übergibt. Wenn der standardmäßig aktive Content Manager-Computer ausfällt, wird der Content Manager-Standy-Computer aktiviert und die Anforderung wird umgeleitet.

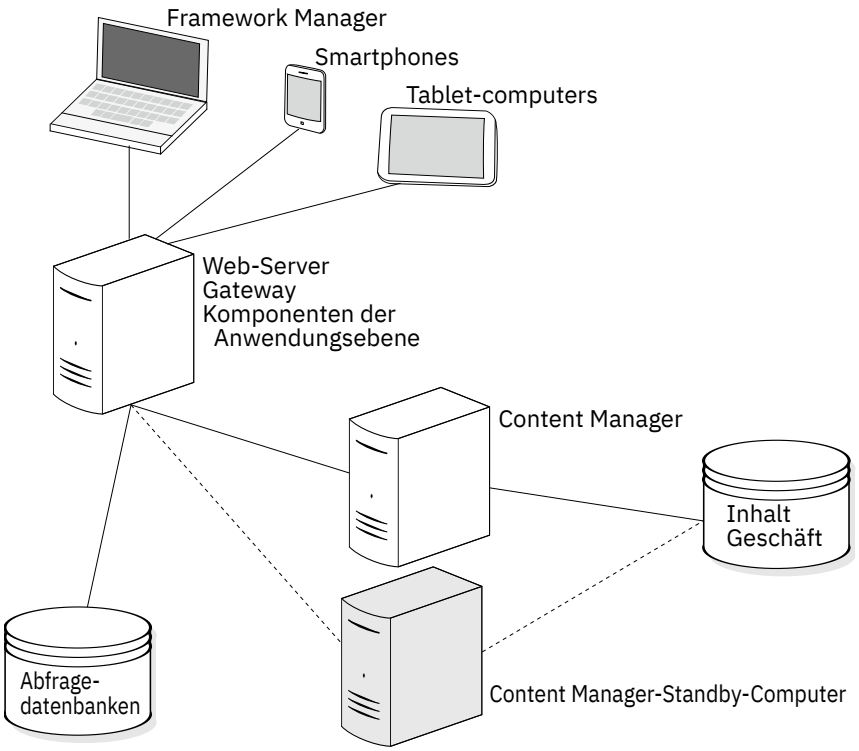


Abbildung 1. Installation mit einem aktiven Content Manager und einem Content Manager im Standby-Modus

Konfigurationsanforderungen

Auf jedem Computer, auf dem Content Manager installiert ist, müssen Sie folgende Schritte ausführen:

- Angeben der Verbindungsinformationen für die Verbindung zum Content Store
- Angeben der Dispatcher-URIs
- Angeben aller Content Manager-URIs
- Angeben des Dispatcher-URIs für externe Anwendungen
- Einrichten einer Verbindung zu einem E-Mail-Server (wenn Sie Berichte oder Benachrichtigungen per E-Mail versenden möchten)

Mehrere Computer mit Komponenten der Anwendungsebene

Um in einer Umgebung mit einer großen Anzahl an zu verarbeitenden Reporting-Anforderungen die Skalierbarkeit zu verbessern, können Sie die Komponenten der Anwendungsebene auf mehreren Computern installieren, die allein zur Verarbeitung eingehender Anforderungen dienen. Indem Sie die Komponenten der Anwendungsebene auf mehreren Computern installieren, verteilen Sie die Last zwischen den Computern. Außerdem bieten mehrere Computer bessere Zugriffsmöglichkeiten, einen höheren Durchsatz sowie bessere Unterstützung bei Computerausfällen als ein einzelner Computer.

Konfigurationsanforderungen

Wenn Sie eine oder mehrere Komponenten der Anwendungsebene auf einem separaten Computer installieren, führen Sie folgende Schritte aus, um sicherzustellen, dass sie mit anderen IBM Cognos Analytics-Komponenten kommunizieren können:

- Angeben aller Content Manager-URIs
- Angeben der Dispatcher-URIs
- Angeben des Dispatcher-URIs für externe Anwendungen

Konsolidieren von Servern für Linux auf System z

Linux auf System z ist eine native Implementierung des Betriebssystems Linux. Zu den Hosting-Optionen gehört die Ausführung von Linux auf einer oder mehreren logischen Partitionen (LPAR).

Integrated Facility for Linux (IFL)

IFLs sind dedizierte System z-Prozessoren für die Ausführung von Linux-Arbeitslasten. Diese Ausführung kann je nach Ihren Anforderungen nativ oder unter einer Virtualisierungssoftware erfolgen. IFLs ermöglichen die Konsolidierung und zentrale Verwaltung von Linux-Ressourcen auf System z.

LPAR-Modus (logische Partition)

Linux kann in LPARs ausgeführt werden und mit anderen Linux-Partitionen über TCP/IP-Verbindungen kommunizieren.

Die horizontale Skalierbarkeit ist in einer großen Linux-Umgebung durch die Anzahl der erstellbaren LPARs begrenzt. Die Ausführung von Linux in LPARs ist möglicherweise die beste Alternative, wenn Sie nur einige wenige Linux-Images ausführen und diese Images sehr viel Prozessorleistung oder dedizierten Speicher benötigen werden. Dadurch wird sichergestellt, dass den Images keine schwach ausgelasteten Ressourcen zugeordnet werden.

Installation für optionale Modellierungskomponenten

Sie installieren die Modellierungstools, wie Framework Manager und Transformer, auf Microsoft Windows-Computern.

Um Packages zu publizieren und damit für die Benutzer verfügbar zu machen, müssen Sie die optionalen Modellierungstools für die Verwendung eines Dispatchers (direkt oder über ein Gateway) konfigurieren. Wenn das Portal gesichert ist, müssen Sie über Berechtigungen zum Erstellen von Datenquellen und Publizieren von Packages im Portal verfügen.

Hinweise zu Firewalls

Wenn sich das Modellierungstool außerhalb einer Netzfirewall befindet, durch die die Komponenten der Anwendungsebene geschützt sind, können bei der Kommunikation mit dem Dispatcher Probleme auftreten. Aus Sicherheitsgründen wird mit der IBM Cognos Analytics-Standardkonfiguration verhindert, dass der Dispatcher Anforderungen von Modellierungstools außerhalb der Firewall entgegennimmt.

Ein Modellierungstool, das sich außerhalb einer Netzfirewall befindet (z. B. Framework Manager), kann keine Anforderungen über die Netzfirewall hinweg an den Dispatcher auf dem IBM Cognos Analytics-Anwendungsserver senden. Um Probleme bei der Kommunikation über eine Netzfirewall zu vermeiden, installieren Sie das Modellierungstool auf derselben Architekturebene wie die Komponenten der Anwendungsebene. Das folgende Diagramm zeigt den Framework Manager-Computer innerhalb der Netzfirewall bei der erfolgreichen Kommunikation mit dem Dispatcher auf dem IBM Cognos Analytics-Anwendungsserver.

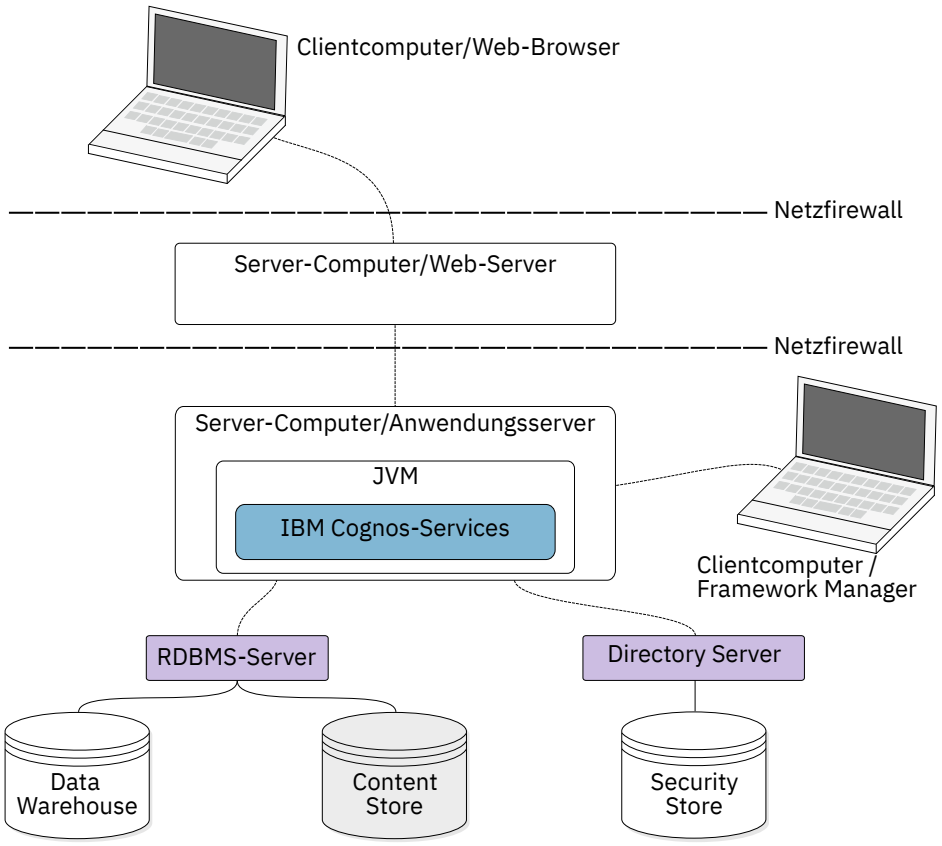


Abbildung 2. Client-Computer außerhalb der Firewall

Die Alternative besteht darin, ein weiteres, für die Kommunikation mit dem Modellierungstool dediziertes Gateway zu installieren, wie im Folgenden dargestellt. Anschließend können Sie das Modellierungstool und dessen Gateway so konfigurieren, dass der Dispatcher Anforderungen vom Modellierungstool akzeptiert.

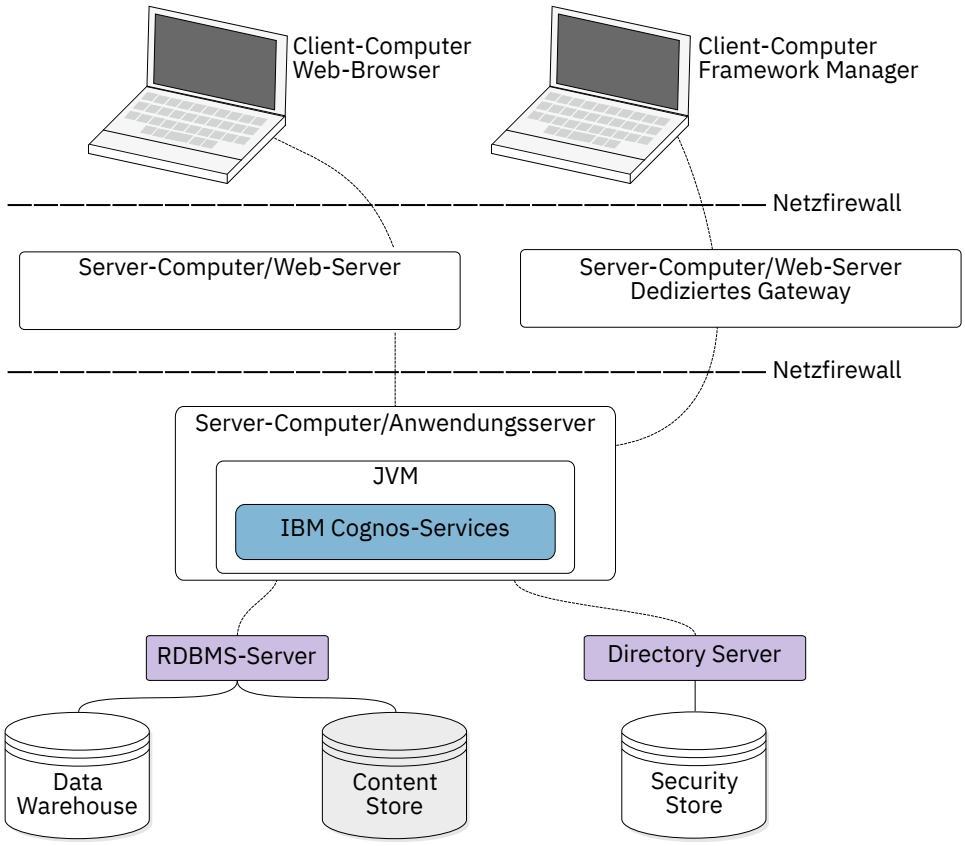


Abbildung 3. Client-Computer außerhalb der Firewall

Verteilen von Framework Manager-Komponenten

Framework Manager kommuniziert mit den Komponenten der Anwendungsebene, die auf einem oder mehreren Anwendungsservern installiert werden können. Um Packages publizieren zu können, müssen Sie Framework Manager für die Kommunikation mit dem Dispatcher konfigurieren, entweder über ein dediziertes Gateway oder direkt.

Konfigurationsanforderungen

Konfigurieren Sie auf dem Computer, auf dem Framework Manager installiert ist, die folgenden Umgebungseigenschaften:

- **Gateway-URI**
- **Dispatcher-URI für externe Anwendungen**

Wenn das Modellierungstool ein dediziertes Gateway verwendet, statt direkt mit dem Dispatcher zu kommunizieren, müssen Sie auch die Eigenschaft **Dispatcher-URIs für die Gateway** auf dem dedizierten Gateway-Computer konfigurieren.

Verteilen von Transformer-Komponenten

Transformer kann sowohl auf einem Computer installiert werden, auf dem sich andere IBM Cognos Analytics-Komponenten befinden, als auch auf einem Computer, auf dem sich keine der IBM Cognos Analytics-Komponenten befinden. Bei einer getrennten Installation können Sie Transformer als eigenständiges Produkt verwenden oder so konfigurieren, dass es mit anderen IBM Cognos Analytics-Komponenten kommuniziert.

Transformer besteht aus den folgenden Komponenten. Abhängig von der Umgebung sind entweder eine oder beide Komponenten vorhanden.

- Transformer unter Windows

Hierbei handelt es sich um das Modellierungstool für Microsoft Windows zum Entwerfen von PowerCubes, die in IBM Cognos Analytics verwendet werden. Es kann auch zum Erstellen und Publizieren von PowerCubes verwendet werden.

- Transformer unter UNIX oder Linux

  Hierbei handelt es sich um ein Befehlszeilendienstprogramm zum Erstellen von PowerCubes unter UNIX und Linux. Zuerst erstellen Sie die Modelle mithilfe von Transformer Windows- oder MDL-Scripts und erstellen dann anhand dieser Modelle die PowerCubes.

  Sie installieren die Komponenten zum Erstellen von Transformer PowerCubes für Linux auf System z.

Unterstützte Funktionen

Wenn Sie Transformer als eigenständiges Produkt verwenden, können Sie in IBM Cognos Analytics externe Datenquellen verwenden, aber Sie können keine gesicherten Sichten mit dimensionaler Filterung erstellen. Wenn Sie Transformer mit anderen IBM Cognos Analytics-Komponenten verwenden, stehen Ihnen die folgenden IBM Cognos Analytics-Funktionen zur Verfügung:

- IBM Cognos Analytics-Authentifizierungsprovider
- IBM Cognos Analytics-Datenquellen, wie z. B. publizierte Packages, Query Studio-Berichte und Reporting-Berichte

  Sie können keine Flatfiles als Datenquellen verwenden.
- das Portal zum Publizieren der PowerCube-Datenquelle und des PowerCube-Packages
- PowerCube-Erstellung

Überlegungen zu rollenbasierten Servern

Unter Umständen ist es wünschenswert, dedizierte Transformer-Server einzurichten, um eine optimale Leistung bei der Cube-Erstellung und Verfügbarkeit für die IBM Cognos Analytics-Benutzer zu erzielen. Berücksichtigen Sie in diesem Szenario die folgenden Anforderungen:

- Die Datenbank-Client-Software wird auf jedem Computer installiert, auf dem Transformer zum Erstellen von PowerCubes oder Testen von Datenquellen verwendet wird.
- Richten Sie für die Datenquellenverbindung entsprechende Umgebungsvariablen für UNIX- und Linux-Server ein.
- IBM Cognos Analytics-Server müssen auf die Position zugreifen können, an der PowerCubes gespeichert werden, sodass der Berichtsserver auf die PowerCubes zugreifen kann.

Die Erstellung und Aktualisierung von PowerCubes in der Produktion kann per Script erfolgen und über Fernzugriff ausgeführt werden, wenn ausreichende Benutzerrechte eingerichtet sind. Weitere Informationen zur Erstellung und Aktualisierung von PowerCubes in der Produktion finden Sie im *Transformer Benutzerhandbuch*.

Unternehmensanalysten oder Spezialisten

Sie verfügen möglicherweise über spezialisierte Geschäfts- oder erfahrene Benutzer, die PowerCubes erstellen möchten, die anhand einer Kombination aus Unternehmens- und persönlichen Datenquellen modelliert werden. Diese Benutzer möchten möglicherweise eigene Analysen der Daten für Ihre Geschäftssparte oder eine kleine Benutzergruppe durchführen. Sie können solchen Benutzern ermöglichen, selbstständig in der IT- und Sicherheitsinfrastruktur des Unternehmens zu arbeiten, indem Sie folgende Anforderungen erfüllen:

- Die Datenbank-Client-Software ist auf den Transformer-Computern installiert (bzw. steht Modellierern dort für die Installation zur Verfügung), die zum Zugriff auf IBM Cognos Analytics-Datenquellen oder IBM Cognos Series 7 IQD-Datenquellen verwendet werden.

- Modellierer müssen Berechtigungen zum Erstellen von Datenquellen in IBM Cognos Administration besitzen.

  Die Modellierer müssen nicht direkt auf IBM Cognos Administration zugreifen können. Sie können Datenquellen mit Transformer oder Befehlszeilen-Tools erstellen und aktualisieren. Sie können für Modellierer einen gesicherten Ordner in dem Portal zur Verfügung stellen, in dem PowerCube-Packages publiziert werden.
- Die Modellierer müssen auf eine Position zugreifen können, an der der PowerCube nach der Erstellung gespeichert werden kann.

  Der IBM Cognos-Service muss auf diese Position zugreifen können; hierbei kann es sich durchaus auch um ein gesichertes gemeinsam genutztes Verzeichnis in einem LAN handeln.
- Um PowerCubes auf einem spezifischen Transformer-Server zu erstellen, muss der Modellierer über FTP-Berechtigungen für die Übertragung von Modellen und Ausführungsberechtigungen für die Erstellung von Cubes auf dem Server verfügen.

  Der Modellierer kann Modelle übertragen und die Cube-Erstellung mithilfe von Scripts ausführen. Der Modellierer kann auch automatische Methoden verwenden, um PowerCubes zu erstellen. Weitere Informationen finden Sie im Handbuch *Verwaltung und Sicherheit*.

Konfigurationsanforderungen

Um PowerCube-Packages publizieren zu können, müssen Sie Transformer für die Kommunikation mit dem Dispatcher konfigurieren, entweder über ein dediziertes Gateway oder direkt. Wenn IBM Cognos Connection gesichert ist, müssen Sie über Berechtigungen zum Erstellen von Datenquellen und Publizieren von Packages in Portal verfügen.

Konfigurieren Sie auf dem Computer, auf dem Transformer installiert ist, die folgenden Umgebungseigenschaften:

- **Gateway-URI**
- **Dispatcher-URI für externe Anwendungen**

Wenn das Modellierungstool ein dediziertes Gateway verwendet, statt direkt mit dem Dispatcher zu kommunizieren, müssen Sie auch die Eigenschaft **Dispatcher-URIs für die Gateway** auf dem dedizierten Gateway-Computer konfigurieren.

IBM Cognos Analytics in Kombination mit anderen IBM Cognos-Produkten

Sie können IBM Cognos Analytics in einer Umgebung installieren, in der auch andere IBM Cognos-Produkte eingesetzt werden.

Der Installationsassistent für IBM Cognos Analytics erkennt kompatible Verzeichnisse und zeigt eine Warnung an, wenn Konflikte auftreten. Nachdem IBM Cognos Analytics installiert wurde, können Sie in IBM Cognos Analytics auf Objekte zugreifen, die mit einem anderen IBM Cognos-Produkt erstellt wurden. Die Zugriffsanforderungen sind von der Art und Weise der Ausführung abhängig, die Sie für die beiden Produkte ausgewählt haben.

Doppelte Services bei Verwendung mehrerer Produkte

Viele IBM Cognos Produkte verwenden ähnliche Services, z. B. den Berichtsservice und den Präsentationsservice. Wenn Sie mehrere Produkte verwenden, z. B. IBM Cognos Analytics mit IBM Cognos PowerPlay, müssen Sie einige der doppelten Services inaktivieren, damit die Produkte fehlerfrei arbeiten.

Nehmen Sie z. B. an, dass auf Ihrem System IBM Cognos Analytics und IBM Cognos PowerPlay installiert sind. Beide Produkte verfügen über einen Berichtsservice und einen Präsentationsservice. Wenn auf beide Produkte über dasselbe Gateway zugegriffen wird, können Berichte, die über die IBM Cognos Analytics-Services ausgeführt werden müssen, an die IBM Cognos PowerPlay-Services weitergeleitet werden. Dies kann dazu führen, dass in Ihren Berichten ein Fehler ausgegeben wird.

IBM Cognos-Produkte, die in Kombination mit IBM Cognos Analytics verwendet werden können

Bestimmte IBM Cognos-Produkte stellen Funktionen zur Verfügung, die in IBM Cognos Analytics nicht verfügbar sind. Sie können diese Produkte weiterhin in derselben Umgebung wie IBM Cognos Analytics verwenden. Mit einigen Produkten können Sie auf die verschiedenen Typen von Cubes oder Berichten im IBM Cognos Analytics-Portal zugreifen. Mit anderen Produkten können Sie auf einzigartige Funktionen im IBM Cognos Analytics-Portal zugreifen.

Cognos Planning - Analyst

Zum Zugriff auf publizierte Plandaten in IBM Cognos Analytics können Sie den Assistenten zum Generieren von Framework Manager-Modellen verwenden. Dazu ist IBM Cognos Planning - Analyst 7.3 MR1 oder eine höhere Version erforderlich.

Wenn Sie dieses Produkt mit dem IBM Cognos Analytics-Server verwenden möchten, müssen Sie sicherstellen, dass beide Produkte dieselbe Version aufweisen.

Weitere Informationen finden Sie im *IBM Cognos Analyst - Benutzerhandbuch*.

Cognos Planning - Contributor

Sie können in IBM Cognos Analytics auf nicht publizierte (Echtzeit-)Contributor-Cubes zugreifen, indem Sie im Rahmen einer benutzerdefinierten Installation die Komponente IBM Cognos Analytics - Contributor Data Server installieren, die Bestandteil von IBM Cognos Planning - Contributor 7.3 MR1 und höheren Releases ist. Zum Zugriff auf publizierte Plandaten in IBM Cognos Analytics können Sie die Administrationserweiterung zum Generieren von Framework Manager-Modellen in Contributor verwenden. Dazu ist IBM Cognos Planning - Contributor 7.3 MR1 oder höher erforderlich.

Wenn Sie dieses Produkt mit dem IBM Cognos Analytics-Server verwenden möchten, müssen Sie sicherstellen, dass beide Produkte dieselbe Version aufweisen. IBM Cognos Planning darf nicht in demselben Pfad wie die 64-Bit-Version von IBM Cognos Analytics installiert werden.

Weitere Informationen finden Sie im *IBM Cognos Contributor Administration Guide*.

Cognos Controller

Sie können auf IBM Cognos Analytics zugreifen, um Standardberichte für IBM Cognos Controller zu erstellen, indem Sie auf ein vordefiniertes Framework Manager-Modell zurückgreifen, das bei der Installation von IBM Cognos Controller erstellt wird. Sie können auch in Framework Manager auf die publizierten Daten und Strukturen von Controller zugreifen, um benutzerdefinierte Analyseberichte zu erstellen.

Cognos Transformer

IBM Cognos PowerCubes und Transformer-Modelle, die mit Transformer 7.3 oder höher generiert wurden, können direkt in IBM Cognos Analytics verwendet werden. Die Cubes und Modelle sind aufwärtskompatibel und erfordern keine Migrations- oder Aktualisierungsprogramme. Für IBM Cognos PowerCubes können in IBM Cognos Analytics Berichte und Analysen ausgeführt werden.

Wenn Sie die neuen Integrationsfunktionen von Transformer mit IBM Cognos Analytics verwenden möchten, können Sie Transformer-Modelle von IBM Cognos Series 7.x auf IBM Cognos Analytics Transformer 8.4 oder höher aktualisieren. Auf diese Weise können Sie IBM Cognos Analytics-Datenquellen (z. B. publizierte Packages) verwenden, in Query Studio oder Reporting verfasste Berichte auflisten, mit der Sicherheitsfunktion von IBM Cognos Analytics eine Authentifizierung durchführen und direkt im Portal publizieren.

Bevor Sie das Modell laden, muss der IBM Cognos Series 7-Namespace in IBM Cognos Analytics konfiguriert werden. Hierbei muss die Namens-ID, die zum Konfigurieren des Namespace in IBM Cognos Analytics verwendet wird, mit dem in IBM Cognos Series 7 verwendeten Namen übereinstimmen.

Weitere Informationen zum Aktualisieren von gesicherten IBM Cognos Series 7-PowerCubes finden Sie im *IBM Cognos Analytics Transformer Benutzerhandbuch*.

Damit IBM Cognos Series 7-PowerCubes in IBM Cognos Analytics verwendet werden, müssen Sie die Cubes für die Verwendung in IBM Cognos Analytics mit dem Dienstprogramm "pcoptimizer" optimieren. Dieses Dienstprogramm wird mit IBM Cognos Analytics bereitgestellt. Andernfalls dauert das Öffnen der mit Vorgängerversionen von Transformer erstellten PowerCubes in den IBM Cognos Analytics Web-Studios zu lange. Das Dienstprogramm für die Optimierung ist für ältere PowerCubes geeignet, die vor Transformer 8.4 erstellt wurden, und erfordert keinen Zugriff auf das Modell oder die Datenquelle. Für Cubes, die in Transformer 8.4 oder einer höheren Version erstellt wurden, muss dieses Befehlszeilendienstprogramm nicht ausgeführt werden. Weitere Informationen zur Optimierung von PowerCubes finden Sie im *Transformer Benutzerhandbuch*.

Sie können PowerCubes mit Transformer 8.4, Framework Manager oder direkt im IBM Cognos Analytics-Portal publizieren. Einzelne PowerCube-Datenquellen und -Packages können Sie im Portal interaktiv mit Transformer oder über die Befehlszeile publizieren. Sie können sie mithilfe von Stapelscripts nach der Erstellung eines PowerCubes auch im Hintergrund publizieren. Ein Benutzer mit den Berechtigungen zum Erstellen von Datenquellen und Packages im Portal kann auch PowerCubes im Portal publizieren. Die MDC-Datei muss sich an einer gesicherten Position befinden, auf die der IBM Cognos Analytics-Dispatcher und der Berichtsserverprozess zugreifen können. Packages, die mehrere PowerCubes aus verschiedenen PowerCube-Definitionen oder mit anderen Datenquellen kombinierte PowerCubes verwenden, müssen mit Framework Manager publiziert werden.

Wenn Sie einen IBM Cognos Series 7-PowerCube als Datenquelle verwenden, konvertiert IBM Cognos Analytics die Cube-Daten aus der Codierung, die auf dem PowerCube-Erstellungssystem verwendet wurde. Für eine erfolgreiche Konvertierung müssen IBM Cognos Series 7-PowerCubes mit derselben Ländereinstellung wie die Daten im PowerCube erstellt werden.

Cognos Lifecycle Manager

Lifecycle Manager ist eine Windows-basierte Anwendung für das Audit von Upgrades von Cognos 8 und höher auf neuere Versionen von IBM Cognos Analytics. Sie bietet eine Überprüfungsfunktion, mit der Berichtsergebnisse aus zwei unterschiedlichen IBM Cognos Analytics-Releases geprüft, ausgeführt und miteinander verglichen werden können. Dadurch können Aktualisierungs- und Kompatibilitätsprobleme zwischen Releases leicht erkannt werden. Durch das Design der Benutzeroberfläche und die Status-Reporting-Funktionalität werden bewährte Verfahren und die Unterstützung für Projektplanungs- und Status-Reporting-Aktualisierungen in einer Anwendung vereint.

Weitere Informationen finden Sie im *IBM Cognos Lifecycle Manager User Guide*.

Planning Analytics

IBM Planning Analytics integriert Geschäftsplanung, Leistungsmessung und Betriebsdaten und ermöglicht es so Unternehmen, die Effektivität und die Interaktion mit den Kunden unabhängig von der Geografie oder Struktur zu optimieren. Planning Analytics bietet unmittelbare Einsicht in Daten, Verantwortlichkeit innerhalb eines bereichsübergreifenden Prozesses und eine konsistente Ansicht der Informationen, so dass Führungskräfte betriebliche Schwankungen schnell stabilisieren und neue neue Chancen nutzen können.

Weitere Informationen finden Sie in der Dokumentation zu *IBM Planning Analytics*.

Kapitel 8. Upgrade für Cognos Analytics

Wenn Sie ein Upgrade für IBM Cognos Analytics durchführen, müssen Sie den Content Store sichern, Ihre Daten aktualisieren, die Auswirkungen des Upgrades auf andere Komponenten in einer verteilten Umgebung kennen, sicherstellen, dass Dateien, die beibehalten werden müssen, nicht überschrieben werden, und möglicherweise andere Upgradeaufgaben ausführen.

Die Upgradeinformationen in diesem Dokument gelten für alle unterstützten Versionen von Cognos Analytics. Bei versionsspezifischen Informationen ist die Versionsnummer im Thementitel enthalten.

Upgrade für die aktuelle Version von Cognos Analytics 11

Sie können ein Upgrade für Ihre Version von IBM Cognos Analytics durchführen, indem Sie eine Installation auf der Basis einer vorhandenen Version vornehmen.

Hierbei handelt es sich um die Standardmethode für Upgrades und damit um die einfachste und komfortabelste Upgradeprozedur. Für alle Komponenten wird ein Upgrade auf eine neuere Version durchgeführt, wobei dieselben Konfigurationsdetails, Ports, Motive und Erweiterungen verwendet werden wie bei der vorherigen Installation.

Die neue, verbesserte Upgradeprozedur nutzt das Continuous Delivery-Modell von Cognos Analytics und stellt neue Features schnell und unkompliziert bereit.

Eine detaillierte Beschreibung der Schritte und ein Video finden Sie hier: http://www.ibm.com/support/docview.wss?uid=swg21994915.

Datenaktualisierungstasks für Cognos Analytics Version 11.1

Zur Unterstützung einer optimierten Benutzererfahrung in Dashboards, Explorationen und anderen Komponenten und zur Verbesserung der Abfrageleistung für hochgeladene Dateien und Datasets müssen die Daten der Version 11.0.x von IBM Cognos Analytics Version 11.0.x aktualisiert werden.

Der Upgradeprozess umfasst die folgenden zwei Aufgaben: Abrufen einiger tieferer Datenmerkmale von Datenservern, Packages, hochgeladenen Dateien und Datasets sowie Aktualisieren des Parquet-Dateiformats in hochgeladenen Dateien und Datasets.

Tiefere Datenmerkmale von Datenservern, Packages, hochgeladenen Dateien und Datasets abrufen

Die tieferen Datenmerkmale unterstützen die Produktfunktionen hinter der optimierten Benutzererfahrung in Dashboards, Explorationen und anderen Komponenten. Diese Merkmale werden anhand der Stichproben von Daten aus den zugrundeliegenden Quellen erfasst.

Cognos Analytics 11.1 erfasst die tieferen Datenmerkmale aus folgenden Gründen:

- Um die Standardspalteneigenschaften auf intelligente Weise festzulegen, z. B. **Verwendung** und **Aggregat**.
- Um Empfehlungen für Visualisierungen in Dashboards, Storys und Explorationen bereitzustellen.
- Um die Untergruppe der Felder zu ermitteln, die sich am besten dafür eignen, im Beziehungsdiagramm in **Erkunden** angezeigt zu werden.
- Damit der **Assistent** die Benutzerabsicht besser erkennen kann.
- Um weitere Formen der automatisierten Unterstützung anzugeben.

Um die tieferen Datenmerkmale abzurufen, müssen Sie die Quellen von Cognos Analytics 11.0.x mit den folgenden Methoden neu hochladen:

- Für Datenserververbindungen müssen Sie die Schemametadaten erneut laden.

Verwenden Sie die Option **Ladeoptionen**. Stellen Sie sicher, dass die folgenden Kontrollkästchen ausgewählt sind: **Primär- und Fremdschlüssel abrufen**, **Beispieldaten abrufen** und **Statistikdaten abrufen** (Version 11.1.4 und ältere Versionen).

Weitere Informationen finden Sie im Abschnitt über das Vorabladen von Metadaten aus einer Datenserververbindung im *IBM Cognos Analytics-Handbuch für Verwaltung*.

- Für Packages verwenden Sie die Aktion **Package aufbereiten**.

  Verwenden Sie die Option für automatische Aufbereitung und stellen Sie sicher, dass auf der Registerkarte **Ladeoptionen** die Kontrollkästchen **Beispieldaten abrufen** und **Statistikdaten abrufen** (Version 11.1.4 und ältere Versionen) ausgewählt sind.

  Weitere Informationen finden Sie im Abschnitt über das Aufbereiten von Packages im *IBM Cognos Analytics-Handbuch für Verwaltung*.

- Für hochgeladene Dateien und Datasets führen Sie entweder das Dienstprogramm `ParquetUpgrade` mit der Option **m** aus oder aktualisieren die einzelnen Dateien und Datasets manuell.

  Das Dienstprogramm `ParquetUpgrade` mit der Option **m** ruft die tieferen Datenmerkmale aus allen hochgeladenen Dateien und Datasets im Content Store ab. Wenn Sie dieses Dienstprogramm ausführen, aktualisieren Sie das Parquet-Format in den betreffenden Dateien und Datasets gleichzeitig. Weitere Informationen finden Sie im Abschnitt „Dienstprogramm 'ParquetMigrate' ausführen ” auf Seite 70.

  Für einzelne hochgeladene Dateien verwenden Sie die Optionen **Datei anhängen** und **Datei ersetzen**. Für einzelne Datasets verwenden Sie die Option **Aktualisieren**.

Parquet-Format in hochgeladenen Dateien und Datasets aktualisieren

Das Parquet-Dateiformat, das zum Speichern der hochgeladenen Dateien und Datasets verwendet wird, hat sich mit Cognos Analytics Version 11.1 geändert. Das neue Parquet-Format ermöglicht eine schnellere Abfrageverarbeitung für hochgeladene Dateien und Datasets.

Sie können dieses Upgrade auf die folgenden Arten implementieren:

- Verwenden Sie das Dienstprogramm `ParquetUpgrade`, um das Parquet-Format in allen hochgeladenen Dateien und Datasets im Content Store zu aktualisieren.

  Führen Sie dieses Dienstprogramm aus, bevor Benutzer mit der Ausführung der Berichte, Dashboards oder Explorationen beginnen. Dadurch wird sichergestellt, dass alle Workloads sofort von den Leistungssteigerungen durch das neue Format profitieren. Weitere Informationen finden Sie im Abschnitt „Dienstprogramm 'ParquetMigrate' ausführen ” auf Seite 70.

- Aktualisieren Sie die Daten manuell in den einzelnen hochgeladenen Dateien und Datasets.

  Für hochgeladene Dateien verwenden Sie die Optionen **Datei anhängen** und **Datei ersetzen**. Für Datasets verwenden Sie die Option **Aktualisieren**.

- Es müssen keinerlei Upgrades durchgeführt werden.

  Wenn eine Abfrage nicht-konvertierte Daten verwendet, leitet der Abfrageservice intern das Upgrade ein und es entsteht eine einmalige Leistungseinbuße bei der Ausführung der Dashboards, Berichte, Berichte oder Explorationen in Cognos Analytics 11.1. In nachfolgenden Abfragen werden dann die aktualisierten Daten verwendet.

Das neue Parquet-Format wird automatisch verwendet, wenn neue Dateien hochgeladen werden, neue Datasets erstellt werden und wenn Bereitstellungsarchive, die hochgeladene Dateien und Datasets enthalten, importiert werden.

Dienstprogramm 'ParquetMigrate' ausführen

Mit dem Dienstprogramm `ParquetMigrate` können Sie das neue Parquet-Format auf von IBM Cognos Analytics 11.0.x hochgeladene Dateien und Datasets anwenden. Bei Verwendung mit der Option **m** ruft dieses Dienstprogramm auch die tieferen Dateneigenschaften aus hochgeladenen Dateien und Datasets ab.

Das Parquet-Format, das zum Speichern von Daten in hochgeladenen Dateien und Datasets verwendet wird, wurde von Version Cognos Analytics 11.0.x zu Version 11.1 geändert. Führen Sie erst den Befehl `ParquetUpgrade` aus, bevor Benutzer mit der Ausführung von Dashboards und Berichten beginnen. Dadurch wird sichergestellt, dass alle Workloads sofort von den Leistungssteigerungen durch das neue Format profitieren. Wenn eine Abfrage nicht aktualisierte Daten verwendet, leitet der Abfrageservice intern das Upgrade ein und es entsteht eine einmalige Leistungseinbuße beim Ausführen der Dashboards, Storys, Berichte oder Explorationen in Cognos Analytics 11.1. In nachfolgenden Abfragen werden dann die aktualisierten Daten verwendet.

Der Befehl `ParquetMigrate` unterstützt die folgenden Parameter:

-h *URL*

Die URL zu einem aktiven Cognos Analytics-Server. Wenn Sie die URL nicht angeben, wird die URL verwendet, die in Cognos Configuration auf dem Computer konfiguriert ist, von dem aus der Befehl ausgeführt wird.

-n *Namespace*

Der Namespace zur Authentifizierung bei der Verbindung mit dem Cognos Analytics-Server.

-u *benutzername*

Der Benutzername zur Authentifizierung bei der Verbindung mit dem Cognos Analytics-Server.

-p *kennwort*

Das Kennwort zur Authentifizierung beim Cognos Analytics-Server.

-d

Zeigt Informationen zu den hochgeladenen Dateien und Datasets im Content Store an. Es werden keine Objekte aktualisiert.

-m

Ruft die tieferen Datenmerkmale in Cognos Analytics ab. Weitere Informationen finden Sie in „Datenaktualisierungstasks für Cognos Analytics Version 11.1" auf Seite 69.

Vorgehensweise

1. Öffnen Sie das Befehlszeilendienstprogramm und navigieren Sie zum Verzeichnis *position_von_cognos_analytics*\bin64.
2. Geben Sie den Befehl `ParquetMigrate` mit der folgenden Syntax an.

   Verwenden Sie die folgende Syntax, um Informationen zu hochgeladenen Dateien oder Datasets anzuzeigen:

   ```
   ParquetMigrate -d -n namespace -u benutzername -p kennwort
   ```

   Oder

   ```
   ParquetMigrate -d -h http://cognos_analytics_host:9300 -n namespace -u user_name -p password
   ```

   Verwenden Sie die folgende Syntax, um ein Upgrade für Dateien oder Datasets durchzuführen:

   ```
   ParquetMigrate -d -n namespace -u benutzername -p kennwort
   ```

   Zum Aktualisieren von Dateien und Datasets und gleichzeitigen Abrufen der tieferen Datenmerkmale verwenden Sie folgende Syntax:

   ```
   ParquetMigrate -m -d -n namespace -u benutzername -p kennwort
   ```

3. Führen Sie den Befehl aus.

Ergebnisse

Wenn der Befehl abgeschlossen ist, wird die Anzahl der aktualisierten Objekte angezeigt. Der Wert Null gibt an, dass keine Objekte gefunden wurden, die eine Aktualisierung erforderten.

Beim Cognos Analytics-Upgrade beibehaltene Dateien und Ordner

Sie können eine neue Version von IBM Cognos Analytics auf der Basis Ihrer aktuellen Produktversion installieren, ohne dass dabei die Konfigurationseinstellungen der Vorgängerversion überschrieben werden.

Dateien, die bei einem Upgrade beibehalten werden sollen, sind in der Datei *Installationsposition*\configuration\preserve\.ca_base_preserve.txt aufgeführt. Diese Datei nicht bearbeiten. Bearbeiten Sie stattdessen die Datei *Installationsposition*\configuration\preserve\preserve.txt, wenn Sie bei einem Upgrade bestimmte Dateien oder Verzeichnisse entfernen oder beibehalten möchten. Anweisungen zur Verwendung von preserve.txt sind in der Datei selbst enthalten.

Tipp: Von Kunden innerhalb der Cognos Analytics-Dateistruktur erstellte Hard- und Softlinks werden nicht unterstützt.

Standardmäßig werden die folgenden Ordner und Dateien bei einem Upgrade für Cognos Analytics beibehalten:

Ordner

Installationsposition\deployment

Installationsposition\data\cmstorage

Installationsposition\data\search

Installationsposition\drivers

Installationsposition\ldapschema

Installationsposition\informix

Installationsposition\configuration\certs

Installationsposition\configuration\csk

Installationsposition\configuration\data

Installationsposition\configuration\caSerial

Installationsposition\webapps\p2pd\WEB-INF\AAA\lib

Installationsposition\iso-swid

Installationsposition\apacheds\instances\cognos

Installationsposition\war\AuditExt

Konfigurationsdateien

Installationsposition\configuration\cogconfig.prefs

Installationsposition\configuration\cogconfig_reg.txt

Installationsposition\configuration\coglocale.xml

Installationsposition\configuration\cogstartup.xml

Installationsposition\configuration\dispatcher.properties

Installationsposition\configuration\install_gatewayurl.xml

Installationsposition\configuration\installData.properties

Installationsposition\configuration\ipfclientconfig.xml

Installationsposition\configuration\configuration\caSerial

Installationsposition\configuration\xqe.diagnosticlogging.xml

Installationsposition\configuration\c11AuditExtension.keystore

Installationsposition\configuration\local-server.xml

Sonstige Dateien

Installationsposition\webapps\p2pd\WEB-INF\web.xml

Installationsposition\wlp\usr\servers\cognosserver\bootstrap.properties

Installationsposition\wlp\usr\servers\cognosserver\jvm.options

Installationsposition\wlp\usr\servers\cognosserver\server.xml

Installationsposition\wlp\usr\servers\dataset-service\bootstrap.properties

Installationsposition\wlp\usr\servers\dataset-service\jvm.options

Installationsposition\wlp\usr\servers\dataset-service\server.xml

Installationsposition\cgi-bin\web.config

Installationsposition\wlpdropins\AuditExt.war

Web-Content-Dateien

Installationsposition\webcontent\web.config

Installationsposition\webcontent\bi\web.config

TM1-Dateien

Installationsposition\templates\ps\portal\variables_TM1.xml

Installationsposition\templates\ps\portal\variables_plan.xml

Installationsposition\templates\ps\portal\icon_active_application.gif

Installationsposition\webcontent\planning.html

Installationsposition\webcontent\tm1\web\tm1web.html

Installationsposition\webcontent\PMHub.html

Installationsposition\templates\ps\system.xml

Installationsposition\templates\ps\portal\system.xml

PowerPlay-Dateien

Installationsposition\webcontent\skins\series7\ppwb

Installationsposition\webcontent\skins\presentation\ppwb

Installationsposition\webcontent\skins\modern\ppwb

Installationsposition\webcontent\skins\corporate\ppwb

Installationsposition\webcontent\skins\contemporary\ppwb

Installationsposition\webcontent\skins\classic\ppwb

Installationsposition\webcontent\skins\business\ppwb

Installationsposition\webcontent\bi\skins\series7\ppwb

Installationsposition\webcontent\bi\skins\presentation\ppwb

Installationsposition\webcontent\bi\skins\modern\ppwb

Installationsposition\webcontent\bi\skins\corporate\ppwb

Installationsposition\webcontent\bi\skins\contemporary\ppwb

Installationsposition\webcontent\bi\skins\classic\ppwb

Installationsposition\webcontent\bi\skins\business\ppwb

Installationsposition\webcontent\bi\ppwb

Installationsposition\webcontent\ps\powerplaystudio

Installationsposition\webcontent\fragments\ppesAdmin

Installationsposition\webcontent\ppwb

Installationsposition\webapps\p2pd\WEB-INF\fragments\applications\cogadmin\pages\ppesAdminPage.xml

Installationsposition\webapps\p2pd\WEB-INF\fragments\applications\cogadmin\fragments\ppesAdmin.xml

Installationsposition\msgsdk\ppesAdminStrings_en.xml

Installationsposition\msgsdk\ppesAdminStrings_ldkspec.xml

Installationsposition\eclipse\plugins\org.eclipse.equinox.cm_1.0.400.v20120522-1841.jar

Installationsposition\eclipse\plugins\org.eclipse.equinox.ds_1.4.1.v20120926-201320.jar

Installationsposition\eclipse\plugins\org.eclipse.equinox.event_1.2.200.v20120522-2049.jar

Installationsposition\eclipse\plugins\org.eclipse.equinox.util_1.0.400.v20120917-192807.jar

Installationsposition\eclipse\plugins\org.eclipse.osgi.services_3.3.100.v20120522-1822.jar

Installationsposition\eclipse\plugins\org.eclipse.osgi.util_3.2.300.v20120913-144807.jar

LCM-Dateien

Installationsposition\wlp\usr\servers\lcm\server.xml

Installationsposition\project

Installationsposition\benchmarks

Installationsposition\configuration

Diese Dateien und Ordner müssen Sie nur in den folgenden Fällen manuell migrieren:

- Wenn die neue Version in einem neuen Verzeichnis installiert wird.
- Wenn die aktuelle Version deinstalliert und dann die neue Version installiert wird.

  Beim Deinstallieren der aktuellen Version wird das Verzeichnis *Installationsposition* vollständig gelöscht.

Standardaktualisierungsprozess

Die Erweiterungen in neuen Versionen von IBM Cognos Analytics können sich auf viele Bereiche der Business Intelligence-Umgebung auswirken. Daher ist es am sinnvollsten, das Upgrade stufenweise auszuführen. Damit das Upgrade erfolgreich ausgeführt werden kann, betrachten Sie es als eigenständiges IT-Projekt und stellen Sie dafür ausreichend Zeit und geeignete Ressourcen für Planung und Ausführung bereit.

Sie müssen Ihr Upgrade so planen, dass Sie für jede Phase des Vorgangs wissen, was auf Sie zukommt. In der Planungsphase können Sie die Dokumentation zur Aktualisierung konsultieren, um sich über das erwartungsgemäße Verhalten, neue Funktionen, die Kompatibilität der Versionen und notwendige Maßnahmen zur Vorbereitung der Produktionsumgebung zu informieren. Nachdem Sie diesbezüglich Klarheit erlangt haben, können Sie sich am Standort über die BI-Infrastruktur, Anwendungen, Berichte und benutzerdefinierte Konfigurationseinstellungen informieren. Abschließend können Sie die Aktualisierung an einer Teilmenge der Daten testen und dann Berichte und Daten auf der Grundlage der Testergebnisse optimieren, bevor Sie die Aktualisierung in vollem Umfang durchführen.

Führen Sie beim Planen des Upgrades die folgenden Aufgaben aus:

- Alle benötigten Daten zusammenstellen, z. B. die erforderlichen Eingaben und die erwarteten Ausgaben für jede Phase
- Die Anwendungen in der Berichtsumgebung bewerten und ähnliche Berichte gruppieren
- Die neue Software in einer Testumgebung installieren und alle benötigten Inhalte in der Testumgebung bereitstellen
- Die aktualisierten Anwendungen aufrufen und testen, ob die Berichte erwartungsgemäß ausgeführt werden

Mithilfe von Lifecycle Manager können Sie Berichte aus verschiedenen IBM Cognos Analytics-Versionen vergleichen. Weitere Informationen finden Sie in der Dokumentation zu Lifecycle Manager.

Bereitstellung und Test werden normalerweise als iterativer Prozess durchgeführt. Achten Sie auf alle Abweichungen zwischen Quellen- und Zielumgebung. Nachdem Sie sich davon überzeugt haben, dass die bereitgestellten Anwendungen Ihren Geschäftsanforderungen entsprechen, wechseln Sie in die Produktionsumgebung.

Das folgende Diagramm zeigt einen allgemeinen Upgrade-Workflow und die einzelnen Phasen im Upgradeprozess. Der Prozess umfasst die folgenden Phasen:

- Erstellen eines Upgradeplans, der die folgenden Aktivitäten umfasst:
  - Lesen von Ressourcen, z. B. der Dokumentation, auf der Website Upgrade Central (www.ibm.com/support/docview.wss?uid=swg22011664) und Befolgen dieser Upgrade-Schritte: http://www.ibm.com/support/docview.wss?uid=swg21994915
  - Überprüfen der unterstützten Umgebungen in Hinsicht auf Kompatibilität mit Ihrer übrigen Software in denIBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235). Diese Seite sollten Sie auch vor einer Aktualisierung Ihres Betriebssystems lesen.
  - Bewerten des vorhandenen Systems, um festzulegen, welche Komponenten in Ihre neue Produktversion verschoben werden sollen.
  - Erstellen eines detaillierten Plans zur Implementierung Ihrer Upgradestrategie.
- Erstellen eines Entwicklungs- oder Testsystems mit der neuen Produktversion.
- Anwendung der aus dem Entwicklungs- oder Testsystem gewonnenen Informationen bei der Erstellung des Qualitätssicherungs- oder Produktionssystems.

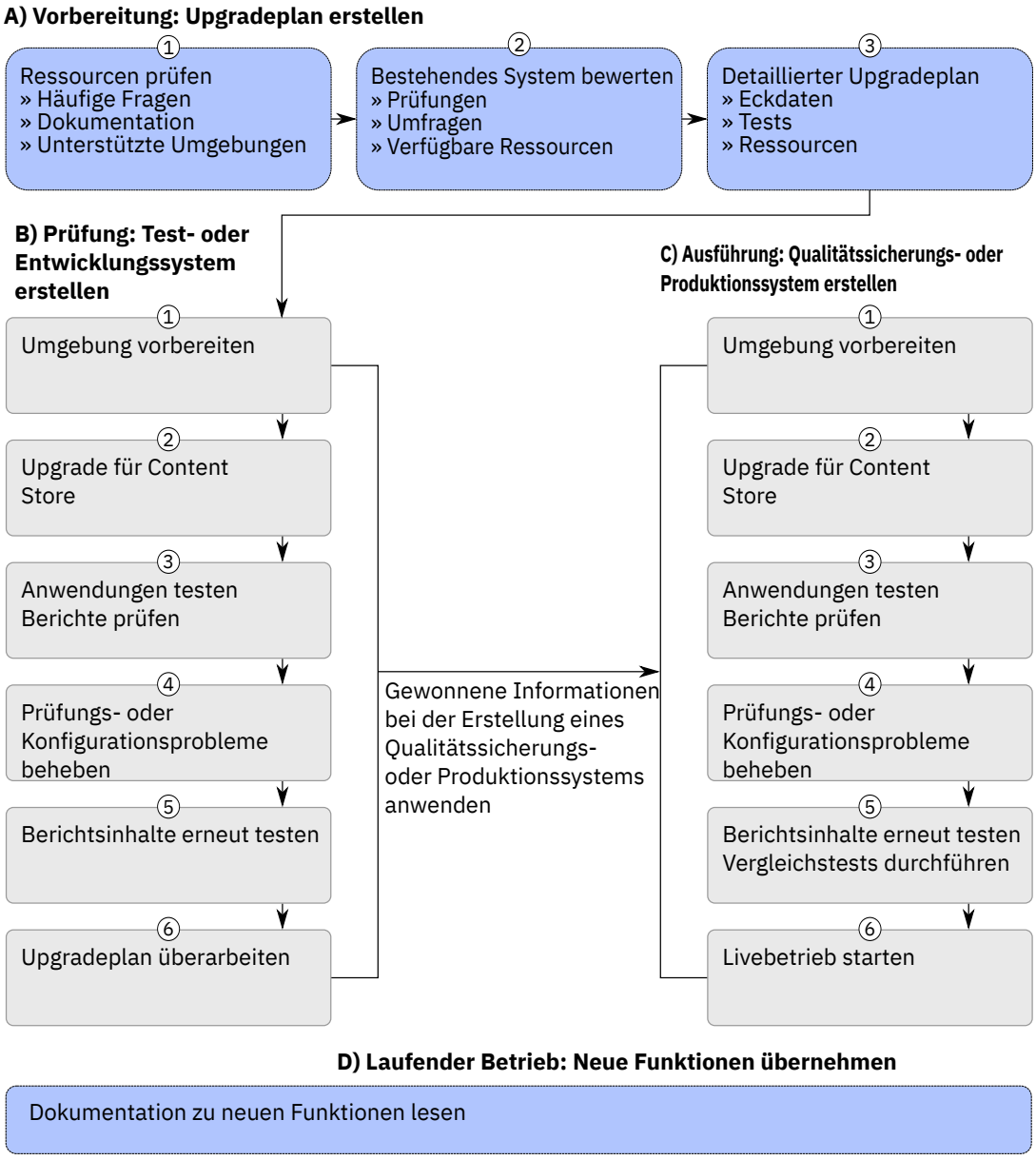


Abbildung 4. Upgradeprozess

Lesen der Dokumentation

Es werden Dokumentationsmaterialien zur Verfügung gestellt, die Sie bei der erfolgreichen Aktualisierung unterstützen.

Die gesamte Dokumentation ist online im IBM Cognos Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSEP7J_11.1.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html) verfügbar.

Bewerten von Anwendungen in Ihrer Umgebung vor einer Aktualisierung

Die Vorbereitung einer Aktualisierung stellt eine günstige Gelegenheit dar, um Ihre aktuellen Anwendungen zu überprüfen und die Quellenumgebung zu bereinigen.

Es könnten sich zum Beispiel viele Anwendungen in Ihrer Umgebung befinden. In der Regel werden einige dieser Anwendungen nie verwendet oder erfüllen nicht mehr Ihre Anforderungen.

Die Bewertung Ihrer Anwendungen ist hilfreich, da Sie dadurch die Anzahl der Anwendungen reduzieren können, die Sie bei einer Aktualisierung berücksichtigen müssen.

Führen Sie ein Audit Ihrer vorhandenen Anwendungen mit Aktionen wie zum Beispiel den folgenden durch:

- Führen Sie eine Umfrage durch, um die aktuelle Produktionsumgebung zu bewerten und ermitteln Sie Bereiche, denen Sie sich im Rahmen einer Aktualisierung gesondert widmen müssen. Die Umfrage erfasst Informationen zur Infrastruktur sowie zu Anwendungen, Benutzern und Konfigurationseinstellungen.
- Bewerten Sie die in Ihrer Umgebung verwendete Software und erstellen Sie eine Liste der Software, z. B. Betriebssysteme, Web-Server, Sicherheitsprovider und Datenbanken.

  Eine aktuelle Liste der Umgebungen, die von den IBM Cognos Analytics Produkten unterstützt werden, einschließlich Informationen zu Betriebssystemen, Patches, Browsern, Webservern, Verzeichnisservern, Datenbankservern und Anwendungsservern, finden Sie auf der Seite IBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235).
- Führen Sie eine detaillierte Bewertung Ihrer Anwendungen durch. Nutzung, Alter, Größe und Komplexität Ihrer Anwendungen sind wichtige Faktoren, die beim Vorbereiten der Aktualisierung berücksichtigt werden müssen. Die Zeit, die Sie zum Durchführen der Aktualisierung benötigen, hängt unter anderem von der Anzahl und der Größe der Anwendungen ab, die aktualisiert werden sollen.
- Erstellen Sie eine Liste mit folgenden Informationen zu Ihrer Konfiguration:
  - Konfigurationseinstellungen, die Sie in IBM Cognos Configuration aktiviert haben.

    Wenn Sie die neue Version des Produkts an einer anderen Position als die vorhandene Version installieren, können Sie die Einstellungen zwischen den beiden Versionen vergleichen. Zum Ausführen der beiden Versionen müssen Sie sicherstellen, dass Sie eindeutige Portnummern, Web-Server-Aliasse und eindeutige Content Store-Datenbanken verwenden.
  - Änderungen an anderen Konfigurationsdateien.

    Sie müssen die Änderungen an anderen Konfigurationsdateien während der Aktualisierung manuell ausführen. Wenn Sie andere Konfigurationsdateien geändert haben, müssen Sie prüfen, welche Änderungen in die aktualisierte Umgebung übernommen werden sollen. Davon können `.xml`-, `.txt`- und `.css`-Dateien in den Verzeichnissen `configuration`, `templates`, `webapps` und `webcontent` betroffen sein.

    Anmerkung: Falls Sie `.ini`-Dateien geändert haben, wenden Sie sich an die Kundenunterstützung, um zu klären, ob die Änderungen in der neuen Version der Software unterstützt werden.
- Sichern Sie Ihre Content Store-Datenbank.

Nach Abschluss des Audits können Sie einen Aktualisierungsplan erstellen.

Hinweise zum Upgrade des Betriebssystems

Vor einem Upgrade des Betriebssystems auf Computern, auf denen IBM Cognos Analytics installiert ist, sollten Sie die folgenden Hinweise lesen:

- Lesen Sie IBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235), um sicherzustellen, dass die installierte IBM Cognos Analytics-Version die neue Betriebssystemversion unterstützt.
- Stellen Sie sicher, dass die von IBM Cognos Analytics verwendete Drittanbieter-Software von der neuen Betriebssystemversion unterstützt wird. Drittanbieter-Software sind Komponenten wie Datenbank und Datenbanktreiber, Anwendungsserver, Web-Server und Browser.
- Stellen Sie fest, ob die SDK-Anwendungen von IBM Cognos Analytics neu kompiliert werden müssen.
- Stellen Sie fest, ob Sie Web-Bereitstellungen wie Webarchive (WAR-Dateien) und Unternehmensarchive (EAR-Dateien) neu erstellen müssen.

Installieren und Konfigurieren einer neuen Produktversion

Installieren Sie die neue Version des Produkts an einer neuen Position. Die Position kann sich auf demselben Computer befinden wie die vorhandene Produktversion oder auf einem anderen Computer.

Durch die Installation an einer neuen Position können Sie Ihre vorhandene Version des Produkts beibehalten und diese zusätzlich zu der neuen Produktversion ausführen. Dadurch können Sie Ihre neue Version ohne Auswirkungen auf die vorhandene Version testen. Sie können die Konfigurationseinstellungen zwischen den Versionen vergleichen sowie die Darstellung und die Funktionalität der Berichte in beiden Umgebungen, um die Gleichwertigkeit sicherzustellen.

Ausführen mehrerer Versionen oder Instanzen von IBM Cognos Analytics auf demselben Computer

Damit mehrere Versionen oder Instanzen von IBM Cognos Analytics auf demselben Computer ausgeführt werden können, müssen Sie die Konfiguration so ändern, dass sichergestellt wird, dass die Versionen keine Portnummern oder anderen Ressourcen gemeinsam nutzen.

Erforderliche Änderungen an der Konfiguration zum Ausführen mehrerer Versionen auf demselben Computer

Zum Ausführen mehrerer Versionen von IBM Cognos Analytics auf demselben Computer müssen Sie sicherstellen, dass zwischen den einzelnen Installationen unterschieden werden kann. Die Versionen oder Instanzen müssen in unterschiedlichen Verzeichnissen installiert werden. Die Konfigurationseinstellungen für die einzelnen Versionen müssen sich bezüglich der folgenden Konfigurationseigenschaften unterscheiden.

Port- und URI-Einstellungen

Wenn Sie den Standardanwendungsserver verwenden, müssen Sie andere Portnummern als Port 9300 verwenden, um Portkonflikte zu vermeiden. Da IBM Cognos Analytics einen Portnummernbereich reserviert, müssen Sie sicherstellen, dass zwischen den Portnummern ein Abstand von mindestens 100 besteht. Beispiel: Sie verwenden die Standardportnummer 9300 für eine Instanz von IBM Cognos Analytics. Für eine zweite Installation auf demselben Computer müssen Sie mindestens Portnummer 9400 verwenden. Verwenden Sie nicht für beide Installationen dieselbe Portnummer.

Ändern Sie die folgenden Ports:

- Dispatcher-URIs für das Gateway
- Externer Dispatcher-URI
- Interner Dispatcher-URI
- Dispatcher-URI für externe Anwendungen
- Content Manager-URIs
- Portnummer des lokalen Protokollservers

Wenn Sie das Produkt auf einem Anwendungsserver installieren, bei dem es sich nicht um den mit IBM Cognos Analytics bereitgestellten Anwendungsserver handelt, stellen Sie sicher, dass Sie die neue Version in einem neuen Anwendungsserverprofil oder in einer anderen Instanz als die vorhandene Version installieren.

Content Store

Verwenden Sie für jede Installation einen anderen Content Store oder ein anderes Schema. Nach einem Upgrade kann der Inhalt nicht zurückgesetzt werden. Als Content Store für die neuere Version von IBM Cognos Analytics können Sie eine wiederhergestellte Kopie Ihres vorhandenen Content Store verwenden. Mit der neueren Version des Produkts wird für den Content Store beim Starten der Services ein Upgrade durchgeführt.

Optionale virtuelle Verzeichnisse des Web-Servers

Um statischen Inhalt für IBM Cognos Analytics anzuzeigen, müssen die virtuellen Verzeichnisse für den Web-Server für jede Version anders sein. Der Gateway-URI in Cognos Configuration muss so aktualisiert werden, dass er die Namen der virtuellen Verzeichnisse widerspiegelt.

Beispiel: Das virtuelle Standardverzeichnis lautet `http://Servername/ibmcognos`. Sind zwei Gateways auf demselben Computer installiert, müssen Sie das virtuelle Verzeichnis `ibmcognos` für eines der Gateways ändern.

Anwendungspools (Microsoft IIS-Web-Server)
Bei der Arbeit mit `cognosisap.dll` muss jedes Gateway einen separaten Anwendungspool verwenden.

Benutzerkonto, das den Service startet (optional)
Das Ändern des Benutzerkontos kann bei der Fehlerbehebung hilfreich sein. Beispielsweise ist es möglich, Fehler bei Java-Prozessen nach Eigentümer zu beheben.

Gleiche Konfigurationseinstellungen für mehrere Versionen auf demselben Server

Mehrere Instanzen oder Versionen von IBM Cognos Analytics, die auf demselben Computer ausgeführt werden, verwenden die gleichen Ressourcen (beispielsweise Speicher, Netz und Plattenspeicher).

Mehrere Versionen von IBM Cognos können dieselbe Authentifizierungsquelle für beide Versionen verwenden. Sie können identische Eigenschaften für den Namespace konfigurieren.

Angepasste Konfigurationsdateien

Wenn Sie eine Konfigurationsdatei manuell bearbeitet haben, müssen Sie die Änderungen erneut anwenden. Erfassen Sie alle Anpassungen, um sicherzustellen, dass sie nach dem Upgrade erneut angewendet werden können. Sichern Sie außerdem diese Dateien, damit bei Bedarf die ursprüngliche Version wiederhergestellt werden kann.

Der Präsentationsservice von IBM Cognos Analytics unterstützt das automatische Upgrade einiger Dateien mit der Bezeichnung `system.xml`. Wenn Sie zahlreiche Anpassungsänderungen an Dateien `system.xml` vorgenommen haben und die Funktion für das automatische Upgrade verwenden, müssen Sie die Änderungen nach dem Upgrade nicht erneut manuell anwenden. Durch das Ersetzen der Dateien `system.xml` durch die Dateien der früheren Version des Produkts können diese Dateien mit der neuen Version des Produkts aktualisiert werden. Das automatische Upgrade erfolgt, wenn Sie den IBM Cognos-Service starten.

Die Dateien mit der Bezeichnung `system.xml`, für die das automatische Upgrade unterstützt wird, befinden sich in den folgenden Verzeichnissen:

- *installationsposition*`/templates/ps`
- *installationsposition*`/templates/ps/portal`
- *installationsposition*`/templates/ps/qs`

Konfigurieren einer zweiten Instanz von IBM Cognos Analytics auf einem Computer

Sollen mehrere Instanzen von IBM Cognos Analytics auf einem Computer vorhanden sein, müssen Sie jede Instanz mit eindeutigen Werten für Ports, das virtuelle Web-Server-Verzeichnis und die Content Store-Datenbank konfigurieren.

Vorbereitende Schritte

Für die neue Produktversion ist ein neuer Content Store erforderlich. Bei einem Upgrade des gesamten Content Store müssen Sie einen Content Store von einer Sicherungskopie des vorhandenen Content Store erstellen. Wenn Sie Ihren Inhalt mithilfe von Bereitstellungsarchiven verschieben, können Sie eine leere Content Store-Datenbank erstellen.

Stellen Sie sicher, dass die neue Content Store-Datenbank vorhanden ist, bevor Sie die neue Version des Produkts konfigurieren.

Wichtig: Wenn Sie eine Verbindung zu einer Sicherungskopie Ihres Content Store herstellen, werden Sie beim ersten Starten der IBM Cognos-Services dazu aufgefordert, Ihre Berichte zu aktualisieren. Das Aktu-

alisieren Ihrer Berichte kann lange Zeit in Anspruch nehmen; daher sollten die Berichte erst aktualisiert werden, wenn die neue Version ausgeführt wird. Sie können Ihre Berichte zu einem späteren Zeitpunkt mithilfe von IBM Cognos Administration aktualisieren.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration für die neue Instanz von IBM Cognos Analytics.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Stellen Sie sicher, dass es bei den Portnummern für die folgenden Einstellungen keinen Konflikt mit der anderen Instanz oder Version von IBM Cognos Analytics gibt:
   - **Dispatcher-URIs für das Gateway**
   - **Externer Dispatcher-URI**
   - **Interner Dispatcher-URI**
   - **Dispatcher-URI für externe Anwendungen**
   - **Content Manager-URIs**
4. Stellen Sie sicher, dass der **Gateway-URI** ein anderes virtuelles Verzeichnis oder einen anderen Aliasnamen verwendet als Ihre andere Instanz bzw. Version von IBM Cognos Analytics.
5. Klicken Sie auf **Protokollierung** und stellen Sie sicher, dass die **Portnummer des lokalen Protokollservers** eindeutig ist.
6. Wenn Sie die Portalservices verwenden, aktualisieren Sie die Position der Datei `applications.xml`:
   - Klicken Sie im Fenster **Explorer** auf **Umgebung** > **Portalservices**.
   - Stellen Sie im Fenster **Eigenschaften** sicher, dass die Portnummer für **Pfad von 'applications.xml'** mit der Portnummer für die anderen URI-Eigenschaften übereinstimmt.
7. Stellen Sie im Fenster **Explorer** unter **Datenzugriff** > **Content Manager** sicher, dass Sie nicht denselben Content Store verwenden, der für Ihre andere Instanz oder Version von IBM Cognos Analytics verwendet wird.
8. Speichern Sie die Konfiguration und starten Sie IBM Cognos Analytics.

Verschieben des Inhalts in die neue Produktversion

Für das Verschieben des Inhalts stehen zwei Methoden zur Auswahl. Sie können entweder den gesamten Content Store oder den Inhalt durch Erstellen von Bereitstellungsarchiven verschieben.

Verschieben des gesamten Content Store

Bei dieser Methode müssen Sie eine Sicherung des vorhandenen Content Store erstellen und dann die Sicherung in einem neuen Content Store wiederherstellen. Anschließend verbinden Sie Ihre neue Produktversion mit dem wiederhergestellten Content Store und das Produkt aktualisiert den Content Store auf die neue Version.

Bei dieser Methode bleiben alle Sicherheits- und Benutzervorgaben bestehen, es ist jedoch eine neue Content Store-Datenbank erforderlich.

Stellen Sie beim Konfigurieren des Sicherheitsfunktionen sicher, dass Sie die eindeutige ID auf denselben Wert einstellen wie in dem Release, von dem Sie das Upgrade vornehmen. Andernfalls gehen die Sicherheitseinstellungen verloren.

Nehmen Sie eine Konsistenzprüfung für Ihren Content Store vor, bevor Sie das Upgrade ausführen, um sicherzustellen, dass keine Inkonsistenzen vorliegen. Weitere Informationen finden Sie im Abschnitt "Erstellen einer Verwaltungsaufgabe für den Content Store" in der Veröffentlichung *IBM Cognos Business Intelligence - Verwaltung und Sicherheit*.

Wichtig: Wenn Sie diese Methode verwenden, werden Sie beim ersten Starten der IBM Cognos-Services aufgefordert, Ihre Berichte zu aktualisieren. Das Aktualisieren Ihrer Berichte kann lange Zeit in Anspruch nehmen; daher sollten die Berichte erst aktualisiert werden, wenn die neue Version ausgeführt wird.

Wählen Sie die Option zum Aktualisieren Ihrer Berichtsspezifikationen auch nicht aus, wenn SDK-Anwendungen (SDK = Software Development Kit) vorhanden sind, die Berichtsspezifikationen erstellen, ändern oder speichern. Sie können Ihre Berichte zu einem späteren Zeitpunkt mithilfe von IBM Cognos Administration aktualisieren.

Des Weiteren müssen Sie sicherstellen, dass Sie die Registrierung aller Dispatcher von der Vorgängerversion des Produkts aufheben. Dazu können Sie IBM Cognos Administration verwenden, nachdem Sie die Services gestartet haben.

Verschieben des Inhalts durch Erstellen von Bereitstellungsarchiven

Sie können Inhalte verschieben, indem Sie Bereitstellungsarchive erstellen.

Mit dieser Methode können Sie bestimmte Inhalte verschieben, dies kann jedoch für einen großen Content Store zeitaufwändig sein.

Wenn Sie die Anbieter von Content Store-Datenbanken wechseln, müssen Sie Bereitstellungen einrichten, um Ihre Inhalte zu verschieben. Wechseln Sie z. B. mit Ihrem Content Store von Microsoft SQL Server zu IBM Db2, benötigen Sie hierfür Bereitstellungsarchive.

Aspekte beider Verfahren

Es ist nicht erforderlich, während eines Upgrades die vorhandenen NC-Tabellen zu migrieren, da das System diese resynchronisiert. Da die Warteschlangentabellen leer sein müssen, empfiehlt es sich, bei einem Upgrade die vorhandenen NC-Tabellen nicht zu verwenden.

NC-Tabellen müssen vollständig leer sein, bevor das Upgrade ausgeführt wird.Führen Sie die entsprechende Datei `NC_DROP_`*`Datenbanktyp`*`.sql` vor dem Upgrade aus.

Stellen Sie im Rahmen des Aktualisierungsprozesses sicher, dass alle Anwendungen problemlos in der neuen Version ausgeführt werden können. Manchmal können Änderungen zu unerwarteten Ergebnissen führen. Daher ist es wichtig, Ihre Anwendungen mit der neuen Produktversion zu testen, bevor Sie die Anwendungen in Ihre neue Produktionsumgebung verschieben.

Upgrade des Content Store

IBM Cognos Analytics führt beim ersten Starten der Services ein Upgrade der Content Store-Datenbank auf die neue Produktversion aus.

Der Prozess zum Durchführen eines Upgrades des Content Store auf die neue Produktversion umfasst die folgenden Schritte:

1. Erstellen einer Sicherung der Content Store-Datenbank.
2. Erstellen einer Datenbank mithilfe der Sicherung.
3. Verbinden der neuen Produktversion mit dem Content Store, den Sie mithilfe der Sicherung in IBM Cognos Configuration erstellt haben.
4. Starten der Services.

   Der Content Store wird während des Startvorgangs aktualisiert.

   Tipp: Beim manuellen Starten von Services muss gegebenenfalls der Service **ApacheDS - cognos** vor dem Service **IBM Cognos** gestartet werden.

Bei diesem Prozess können Sie die alte und die neue Version des Produkts gleichzeitig verwenden, wobei jede Version über ihren eigenen Content Store verfügt.

Sie können später Ihre Berichte mithilfe von IBM Cognos Administration aktualisieren. Wählen Sie die Option zum Aktualisieren Ihrer Berichtsspezifikationen auch nicht aus, wenn SDK-Anwendungen (SDK = Software Development Kit) vorhanden sind, die Berichtsspezifikationen erstellen, ändern oder speichern.

Wenn Sie die neue Produktversion mit dem Content Store verbinden, den Sie mithilfe der Sicherung erstellt haben, wird die Content Store-Datenbank aktualisiert und kann nicht mehr mit der älteren Produktversion verwendet werden.

Entfernen der Registrierung von Dispatchern der Vorgängerversion aus dem Content Store

Wenn Sie eine Sicherung Ihres vorhandenen Content Store mit einer neuen Produktversion verwenden, müssen Sie die Registrierung der Dispatcher Ihrer früheren Version entfernen.

Vorgehensweise

1. Öffnen Sie IBM Cognos Administration über **Verwalten** > **Administrationskonsole**.
2. Klicken Sie auf **Konfiguration** und anschließend auf **Dispatcher und Services**.
3. Klicken Sie auf **Mehr**, um die Dispatcher Ihrer Vorgängerversion anzuzeigen.
4. Klicken Sie auf **Entfernen aus der Registrierung** und anschließend auf **OK**.

   Die Informationen zum Dispatcher werden aus dem Content Store entfernt.

Verschieben des Inhalts mit einem Bereitstellungsarchiv

Sie können Bereitstellungsarchive verwenden, um bestimmte Inhalte aus Ihrem Content Store zu verschieben. Bei Bereitstellungsarchiven handelt es sich um komprimierte Dateien, die Sie in Ihre neue Version des Produkts importieren können.

Wichtig: Wenn Sie Ihren Inhalt durch Wiederherstellung Ihres vorhandenen Content Store verschoben haben, müssen Sie Ihren Inhalt nicht mithilfe von Bereitstellungsarchiven verschieben.

Das Verschieben des Inhalts mithilfe von Bereitstellungsarchiven umfasst die folgenden Schritte:

1. Erstellen des Archivs.
2. Kopieren des Archivs in die neue Version des Produkts.
3. Importieren des Inhalts.

Erstellen eines Bereitstellungsarchivs

Führen Sie zum Erstellen eines Bereitstellungsarchivs die folgende Aufgabe aus.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration** auf der Registerkarte **Konfiguration** auf **Inhaltsadministration**.
2. Klicken Sie in der Symbolleiste auf das Symbol **Neuer Export**  .
3. Geben Sie den **Namen** für das Archiv ein.
4. Wählen Sie den Inhalt aus, der im Archiv enthalten sein soll.
   - Wenn Sie bestimmte Ordner und Verzeichnisinhalte exportieren möchten, klicken Sie auf **Wählen Sie öffentliche Ordner und Verzeichnisinhalte aus**.
   - Wenn Sie den gesamten Content Store exportieren möchten, klicken Sie auf **Gesamten Content Store wählen**. Wenn Sie den gesamten Content Store auswählen, können Sie auch **Benutzerkontoinformationen einschließen** auswählen.
5. Klicken Sie auf **Weiter**.
6. Wenn Sie auf **Gesamten Content Store wählen** geklickt haben, geben Sie ein Kennwort ein, das zum Importieren des Inhalts verwendet werden soll, und klicken Sie anschließend auf **OK**.
7. Wenn Sie auf **Wählen Sie öffentliche Ordner und Verzeichnisinhalte aus** geklickt haben, gehen Sie folgendermaßen vor:
   a) Klicken Sie im Fenster **Wählen Sie den Inhalt der öffentlichen Ordner aus** auf **Hinzufügen**.
   b) Wählen Sie im Fenster **Einträge auswählen** im Feld **Verfügbare Einträge** die Packages und Ordner aus, die Sie exportieren möchten.

Sie können die Hierarchie der öffentlichen Ordner durchsuchen und die gewünschten Packages und Ordner auswählen. Klicken Sie auf das Symbol **Hinzufügen**  , um die ausgewählten Elemente in das Feld **Ausgewählte Einträge** zu verschieben, und klicken Sie auf **OK**.

c) Führen Sie für jedes zu exportierende Package und jeden zu exportierenden Ordner folgende Aktionen aus und klicken Sie auf **Weiter**:

- Wenn Sie in der Zielumgebung Änderungen am Package oder Ordner vornehmen möchten, klicken Sie auf das Symbol **Bearbeiten**  , nehmen Sie die Änderungen vor und klicken Sie auf **OK**.
- Um den Zugriff auf das Package oder den Ordner und die zugehörigen Einträge zu beschränken, aktivieren Sie das Kontrollkästchen in der Spalte **Nach dem Importieren deaktivieren**. Dies ist hilfreich, wenn Sie die Berichte testen möchten, bevor Sie sie im Zielsystem bereitstellen.
- Wählen Sie unter **Optionen** aus, ob Sie die ausgegebenen Berichtsversionen, den Ausführungsverlauf und die Zeitpläne einschließen möchten und wie mit den Einträgen bei Versionskonflikten zu verfahren ist.

d) Wählen Sie im Fenster **Verzeichnisinhalt auswählen** die gewünschten Optionen aus und klicken Sie auf **Weiter**.

e) Wählen Sie im Fenster **Legen Sie die allgemeinen Optionen fest** die gewünschten Optionen aus und klicken Sie auf **Weiter**.

f) Wählen Sie im Fenster **Geben Sie ein Bereitstellungsarchiv an** ein vorhandenes Bereitstellungsarchiv aus der Liste aus oder erstellen Sie ein Bereitstellungsarchiv.

Wenn Sie einen neuen Namen für das Bereitstellungsarchiv eingeben, sollten Sie in diesem Namen keine Leerzeichen verwenden. Wenn der Name der neuen Bereitstellungsspezifikation mit dem Namen eines vorhandenen Bereitstellungsarchivs übereinstimmt, wird das vorhandene Bereitstellungsarchiv überschrieben.

8. Prüfen Sie die Zusammenfassung und klicken Sie auf **Weiter**.
9. Wählen Sie unter **Aktionen** den Eintrag **Speichern und einmal ausführen** aus.
10. Wählen Sie im Fenster **Mit Optionen ausführen** den Eintrag **Jetzt** aus und klicken Sie auf **Ausführen**.

Ergebnisse

Ein Bereitstellungsarchiv wird im Verzeichnis `deployment` erstellt, in dem Sie IBM Cognos Analytics installiert haben.

Kopieren des Bereitstellungsarchivs in neue Version

Sie müssen die Bereitstellungsarchive manuell von der Instanz, in der sie erstellt wurden, in Ihre neue Instanz kopieren.

Vorgehensweise

Kopieren Sie die von Ihnen erstellten Bereitstellungsarchive aus dem Verzeichnis *Installationsposition_alter_Version*/deployment in das Verzeichnis *Installationsposition_neuer_Version*/deployment.

Anmerkung: Das Verzeichnis `deployment` kann in IBM Cognos Configuration konfiguriert werden. Standardmäßig wird das Verzeichnis *Installationsposition*/deployment verwendet. Wenn Sie eine andere Position verwenden, stellen Sie sicher, dass Sie die Bereitstellungsarchive in das entsprechende Verzeichnis kopieren.

Einbeziehen von Konfigurationsobjekten beim Import eines Bereitstellungsarchivs des gesamten Content Store

Sie können Konfigurationsobjekte beim Importieren eines gesamten Content Store mit einschließen. Zum Beispiel möchten Sie möglicherweise die Konfiguration importieren, weil Sie über eine Reihe von erweiterten Einstellungen für Ihre Services verfügen, die Sie aus dem Quellensystem übernehmen möchten.

Standardmäßig werden Konfigurationsobjekte ausgeschlossen, wenn Sie einen gesamten Content Store importieren, obwohl sie in den Export eingeschlossen sind. Zu den Konfigurationsobjekten gehören Dispatcher und Konfigurationsordner, die zum Gruppieren der Dispatcher verwendet werden.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration** auf der Registerkarte **Konfiguration** auf **Dispatcher und Services**.
2. Klicken Sie auf den gewünschten Dispatcher.
3. Klicken Sie neben **ContentManagerService** auf das Symbol **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen**.
5. Klicken Sie in der Spalte **Wert** auf **Bearbeiten**.
6. Aktivieren Sie das Kontrollkästchen **Die vom übergeordneten Eintrag erhaltenen Einstellungen überschreiben**.
7. Geben Sie in der Spalte **Parameter** den folgenden Text in Großbuchstaben ein:

   `CM.DEPLOYMENTINCLUDECONFIGURATION`
8. Geben Sie in der Spalte **Wert** die Angabe `true` ein.
9. Klicken Sie zum Fertigstellen auf **OK**.

Importieren eines Bereitstellungsarchivs

Zum Importieren der Einträge erstellen Sie eine Bereitstellungsspezifikation.

Beim Import treffen Sie eine Auswahl aus den exportierten Einträgen. Sie können entweder die beim Export festgelegten Standardoptionen verwenden oder diese ändern. Nur Optionen, die beim Export in das Bereitstellungsarchiv aufgenommen wurden, stehen beim Import zur Auswahl.

Wenn Sie eine teilweise Bereitstellung von bestimmten öffentlichen Ordnern und Verzeichnisinhalten ausführen, wird im Importassistenten angezeigt, ob im Zielsystem Packages und Ordner vorhanden sind und zu welchem Zeitpunkt sie zum letzten Mal bearbeitet wurden. Sie können diese Informationen zum Lösen von Versionskonflikten einsetzen. Bei einer erneuten Bereitstellung wird im Assistenten zusätzlich angezeigt, ob die Packages und Ordner bereits Bestandteil der ursprünglichen Bereitstellung waren.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie das Bereitstellungsarchiv in das Verzeichnis *installationsposition*`/deployment` für Ihre neue Produktversion kopiert haben.

Vorgehensweise

1. Klicken Sie für Ihre neue Produktversion in **IBM Cognos Administration** auf der Registerkarte **Konfiguration** auf **Inhaltsadministration**.
2. Klicken Sie auf der Symbolleiste auf das Symbol für neuen Import. 
3. Klicken Sie im Feld **Bereitstellungsarchiv** auf das Bereitstellungsarchiv, das Sie importieren möchten, und klicken Sie auf **Weiter**.
4. Wenn Ihr Bereitstellungsarchiv den gesamten Content Store umfasst, geben Sie das beim Export eingegebene Kennwort ein und klicken Sie auf **OK**.

5. Geben Sie einen Namen für den Import ein, wählen Sie einen Ordner zum Speichern aus und klicken Sie anschließend auf **Weiter**.
6. Wählen Sie die Inhalte aus, die beim Import eingeschlossen werden sollen, wählen Sie die Optionen aus und klicken Sie auf **Weiter**.

   Tipp: Klicken Sie auf das Bearbeitungssymbol  neben dem Package, wenn Sie die Zielposition für den importierten Inhalt ändern wollen.
7. Wählen Sie im Fenster **Legen Sie die allgemeinen Optionen fest** die gewünschten Optionen aus und klicken Sie auf **Weiter**.
8. Prüfen Sie die Zusammenfassung und klicken Sie auf **Weiter**.
9. Wählen Sie unter **Aktionen** die Option **Speichern und einmal ausführen** aus und klicken Sie auf **Fertigstellen**.
10. Führen Sie im Fenster **Mit Optionen ausführen** folgende Aktion aus:
    a) Wählen Sie **Alle Berichtsspezifikationen auf die neueste Version aktualisieren** aus, wenn die Berichtsspezifikationen während des Imports aktualisiert werden sollen. Diese Aufgabe können Sie auch nach dem Importieren des Inhalts ausführen.
    b) Klicken Sie auf **Ausführen**.

Vergleichen von Berichten zwischen Produktversionen mithilfe von Lifecycle Manager

Mit dem von Lifecycle Manager können Sie Ihre aktualisierten Inhalte durch Vergleichen der Berichte in Ihrer alten Umgebung mit den Berichten in der neuen Produktversion prüfen.

Weitere Informationen finden Sie in der Dokumentation zum IBM Cognos Lifecycle Manager.

Aktualisieren der Berichtsspezifikationen

Die Berichtsspezifikationen werden in jeder neuen Version von IBM Cognos Analytics geändert. Sie müssen alle in den Vorgängerversionen des Produkts erstellten Berichtsspezifikationen aktualisieren.

Bei einer Aktualisierung von einer Sicherung Ihres vorhandenen Content Store sollten Sie die Berichtsspezifikationen nach dem Starten der Services aktualisieren.

Wenn Sie Inhalte mithilfe von Bereitstellungsarchiven in eine neue Version verschieben, können Sie auswählen, dass die Importspezifikationen während des Imports aktualisiert werden.

Wenn Sie Ihre Inhalte mithilfe von Bereitstellungsarchiven verschoben haben, haben Sie möglicherweise die Option zum Aktualisieren der Berichtsspezifikationen ausgewählt. Wurden die Berichtsspezifikationen während des Imports aktualisiert, ist keine erneute Aktualisierung erforderlich.

Vorbereitende Schritte

Wichtig: Führen Sie kein Upgrade für Ihre Berichtsspezifikationen durch, wenn Sie Software Development Kit-Anwendungen haben, die Berichtsspezifikationen erstellen, ändern oder speichern. Sie müssen Ihre Software Development Kit-Anwendungen zum ersten Mal aktualisieren, um das IBM Cognos -Berichtsspezifikationen-Schema zu erfüllen. Andernfalls können Ihre Software Development Kit-Anwendungen möglicherweise nicht auf die aktualisierten Berichtsspezifikationen zugreifen. Informationen zum Aktualisieren von Berichtsspezifikationen finden Sie im *IBM Cognos Software Development Kit Developer Guide*.

Vorgehensweise

1. Öffnen Sie **IBM Cognos Administration**.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
3. Klicken Sie in der Symbolleiste auf den Pfeil auf der neuen Schaltfläche für die Inhaltsverwaltung  und klicken Sie dann auf **Neues Berichtsupgrade** .

4. Geben Sie einen Namen für die Upgrade-Task und, wenn Sie möchten, eine Beschreibung und einen Anzeigentipp ein. Klicken Sie auf **Weiter**.
5. Wählen Sie die Pakete und Positionen für die Berichtsspezifikation aus, für die ein Upgrade durchgeführt werden soll. Klicken Sie auf **Weiter**.

   Wenn Sie ein Upgrade für Berichtsspezifikationen nach Paket durchführen, werden alle Berichte im Content-Store, die auf dem Modell im Paket basieren, aktualisiert. Wenn Sie die Berichtsspezifikationen nach Ordner aktualisieren, werden alle Berichte in dem Ordner aktualisiert.
6. Wählen Sie eine der folgenden Optionen aus:
   - **Speichern und einmal ausführen** öffnet die Seite 'Ausführen mit Optionen'.
   - **Speichern und planen** öffnet das Planungswerkzeug.
   - Mit **Nur speichern** können Sie das Upgrade speichern, so dass Sie es zu einem späteren Zeitpunkt ausführen können.

Kapitel 9. Konfigurieren von Serverkomponenten

Sie können alle IBM Cognos Analytics-Komponenten auf einem Computer oder für eine verteilte Installation auf mehreren Servern installieren oder Sie können eine vorhandene Einzelinstallation auf einem Computer auf andere Server erweitern, um so die Leistung zu verbessern.

Die folgenden Optionen sind bei der Installation von IBM Cognos Analytics mithilfe des Installationsassistenten verfügbar.

- Verwenden Sie die Option **Easy Install**, um IBM Cognos Analytics ohne großen Zeitaufwand betriebsbereit zu machen, ohne dass zusätzliche Konfigurationsschritte oder die Installation unterstützender Software erforderlich sind.

  Wichtig: Die Funktion **Easy Install** ist nur für Windows OS verfügbar. Wenn Sie für Installationen des Typs **Easy Install** ein Upgrade durchführen (d. h. eine Installation auf der Basis einer vorhandenen Installation durchführen), beenden Sie zuerst manuell alle Services, einschließlich Informix- und ApacheDS-Services.

  Diese Installationsoption umfasst die folgenden Komponenten einschließlich der vollständigen Konfiguration:

  – Vollversion der IBM Cognos Analytics-Software mit allen neuen Funktionen.
  – Informix 12.10, zur Verwendung als Content Store-Datenbank installiert und konfiguriert.
  – Apache Directory Server zur Erstellung und Verwaltung von Benutzern.
- Verwenden Sie die Option **Benutzerdefiniert**, um bei der Auswahl der IBM Cognos Analytics-Komponenten, die installiert werden sollen, die volle Flexibilität zu nutzen. Möchten Sie IBM Cognos Analytics anpassen oder in die Software anderer Anbieter integrieren? Dann ist dies die geeignete Option.

Wenn Sie zwei oder mehr Komponenten auf demselben Computer installieren möchten, sollten Sie diese im selben Installationsverzeichnis installieren, um Konflikte hinsichtlich der Ports und anderer Standardeinstellungen zu vermeiden.

Bei einer verteilten Installation werden die Serverkomponenten in folgenden Ebenen erfasst:

- Inhaltsrepository (Content Manager)
- Anwendungsservices
- Gatewayebene

Sie können die einzelnen Komponenten auf verschiedenen oder auf demselben Computer installieren. Das Gateway muss auf einem Computer installiert werden, der auch einen Web-Server ausführt.

Reihenfolge beim Stoppen von Services

Bein Stoppen von Services in einer verteilten Umgebung muss die Reihenfolge beachtet werden. Stoppen Sie zuerst den IBM Cognos-Service für Komponenten der Anwendungsebene, danach den Standby-Content Manager und anschließend den aktiven Content Manager.

Außerdem müssen Sie die folgenden Komponenten stoppen:

- Anwendungen, die mit dem IBM Cognos-Service verbunden sind, z. B. Framework Manager, Cognos Transformer oder IBM Cognos Administration.
- Alle Software Development Kit-Anwendungen, die ausgeführt werden.

Aktualisierung der Installation

Informationen zum Aktualisieren eines Vorgängerrelease von IBM Cognos-Produkten finden Sie in Kapitel 8, „Upgrade für Cognos Analytics”, auf Seite 69.

Wenn Sie eine frühere Version von IBM Cognos Analytics aktualisieren, müssen alle verteilten Komponenten dieselbe Version von IBM Cognos Analytics aufweisen. Wenn Sie IBM Cognos Analytics auf zusätzlichen oder alternativen Hosts installieren, müssen Sie die positionsspezifischen Eigenschaften in IBM Cognos Configuration entsprechend aktualisieren.

64-Bit-Installationen

Das IBM Cognos Analytics-Gateway stellt 32-Bit-Bibliotheken bereit, unabhängig davon, ob die Installation auf einem 64-Bit-Server oder auf einem 32-Bit-Server durchgeführt wird. Auf einigen Web-Servern, z. B. auf dem Apache-Web-Server, kann eine 32-Bit-Bibliothek auf einem 64-Bit-Server nicht geladen werden. Installieren Sie in diesem Fall die 32-Bit-Version des IBM Cognos-Gateways auf einem 32-Bit-Web-Server.

Die Berichtsserverkomponente, die in die Komponenten der Anwendungsebene integriert ist, wird sowohl in der 32- als auch in der 64-Bit-Version bereitgestellt. Die Auswahl der von Ihnen verwendeten Version wird nach der Installation mithilfe von IBM Cognos Configuration vorgenommen. Standardmäßig wird für die Berichtsserverkomponente die Verwendung des 32-Bit-Modus festgelegt, auch auch einem 64-Bit-Computer. Mit dem 32-Bit-Modus können Sie alle Berichte ausführen, wohingegen Sie mit dem 64-Bit-Modus lediglich Berichte ausführen können, die für den dynamischen Abfragemodus erstellt wurden.

Wenn Sie für IBM Cognos Analytics ein Upgrade in einer Umgebung durchführen, die ältere Versionen anderer IBM Cognos Analytics-Produkte enthält (z. B. IBM Cognos Business Intelligence Controller Version 8.x, IBM Cognos Analytics Planning Version 8.x oder IBM Cognos Business Intelligence Analysis *for Microsoft Excel* Version 8.x), installieren Sie die neue Version von IBM Cognos Analytics getrennt von dem anderen IBM Cognos Analytics-Produkt und konfigurieren Sie die neue Version von IBM Cognos Analytics so, dass sie unabhängig vom älteren Produkt ausgeführt wird. Nachdem Sie für das andere Produkt ein Upgrade auf eine mit IBM Cognos Analytics kompatible Version durchgeführt haben, können Sie die zwei Produkte so konfigurieren, dass sie zusammenarbeiten.

Windows-Installationen

Bei Microsoft Windows-Installationen müssen Sie sicherstellen, dass Sie für den Windows-Computer, auf dem Sie die Installation durchführen, über Administratorberechtigungen verfügen. Vergewissern Sie sich auch, dass die Systemvariable TEMP des Computers auf das Verzeichnis verweist, in dem temporäre Dateien gespeichert werden sollen. Während der Installation werden Dateien vom Datenträger vorübergehend in dieses Verzeichnis kopiert.

UNIX-Installationen

Bei UNIX-Installationen können Sie Serverkomponenten mithilfe einer grafischen Benutzeroberfläche oder durch Ausführen einer Hintergrund-Installation installieren. Für die Installation im Grafikmodus muss die an Ihren UNIX-Computer angeschlossene Konsole eine Java-basierte grafische Benutzeroberfläche unterstützen.

Beachten Sie darüber hinaus, dass IBM Cognos Analytics 755-Berechtigungen verwendet. Dies betrifft nur die Installationsverzeichnisse. und hat keine Auswirkungen auf die Dateiberechtigungen innerhalb der Verzeichnisse.

Druckeranforderungen

Um sicherzustellen, dass Berichte unter Windows ordnungsgemäß ausgedruckt werden, müssen Sie aufgrund der Anforderungen von Adobe Reader mindestens einen Drucker auf dem Betriebssystem konfigurieren, auf dem die Komponenten der Anwendungsebene (Application Tier Components) installiert sind. Alle Berichte werden unabhängig vom Druckformat, das Sie auswählen, zum Ausdrucken als temporäre PDF-Dateien an Adobe Reader gesendet.

Deinstallation

Anweisungen zur Deinstallation finden Sie in Kapitel 16, „Deinstallieren von IBM Cognos Analytics”, auf Seite 313.

Installationsreihenfolge für Serverkomponenten

Bei einer verteilten Installation ist die Reihenfolge wichtig, in der die Komponenten konfiguriert werden. Vor der Konfiguration anderer Serverkomponenten müssen die Services an mindestens einer Position, an der Sie Content Manager installiert haben, konfiguriert und gestartet werden.

Die Gateway-Komponente muss zuletzt konfiguriert werden, damit die kryptografischen Schlüssel gemeinsam genutzt werden können und eine sichere Kommunikation zwischen den drei Komponenten stattfinden kann. Der für die Eigenschaft **Externe Dispatcher-URI** auf dem Gateway-Computer angegebene Server muss die letzte Serverkomponente sein, die Sie starten.

Die folgende Abbildung zeigt die Installationsreihenfolge für verteilte Komponenten. Nach der Planung und Vorbereitung Ihrer Umgebung installieren und konfigurieren Sie zunächst die Content Manager-Komponenten, dann die Komponenten der Anwendungsebene und dann die Gateways. Nach Installation der Serverkomponenten installieren und konfigurieren Sie Framework Manager.

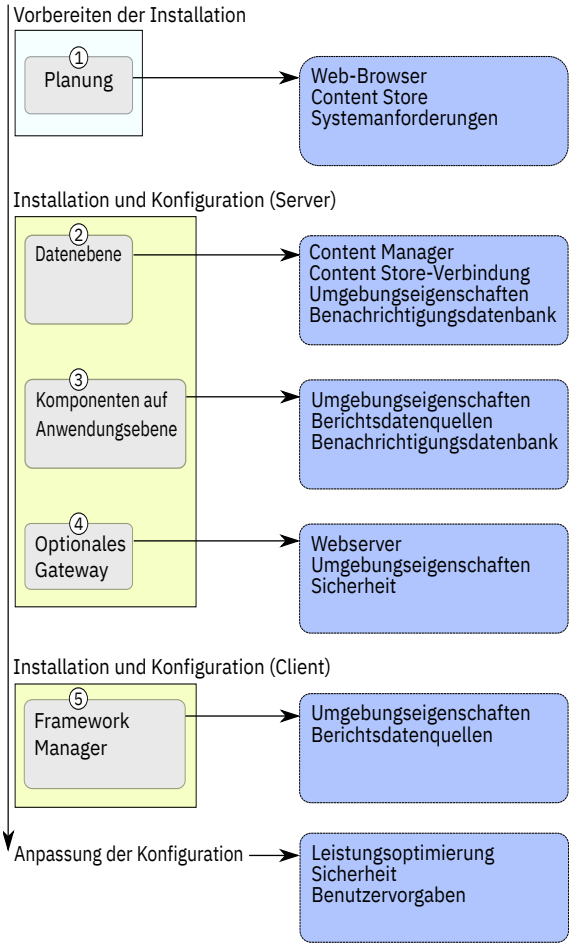


Abbildung 5. Ablauf beim Prozess für die verteilte Installation

Empfehlung - Installation und Konfiguration der Basisinstallation für verteilte Installationen

Bei einer verteilten Installation gibt es viele verschiedene Installations- und Konfigurationsoptionen, mit denen Sie IBM Cognos Analytics an die Infrastruktur Ihres Unternehmens anpassen können.

Führen Sie zuerst eine Basisinstallation durch, zu der die Installation jeweils einer oder mehrerer Instanzen der erforderlichen Serverkomponenten gehört: Komponenten auf Datenebene (Content Manager), Komponenten der Anwendungsebene und Komponenten auf Gateway-Ebene. Führen Sie zunächst nur die erforderlichen Konfigurationsaufgaben aus (wie die Konfiguration der verteilten Komponenten für die Kommunikation untereinander), um ein Funktionieren der verteilten Umgebung zu ermöglichen, und passen Sie dann erst die Einstellungen an.

Später können Sie optionale Komponenten hinzufügen und Ihre Konfigurationseinstellungen an Ihre speziellen Business Intelligence-Anforderungen anpassen.

Die Reihenfolge, in der Sie die Computer konfigurieren, ist wichtig. Sie müssen zunächst auf mindestens einem Computer, auf dem Sie Content Manager installiert haben, die Services konfigurieren und starten, bevor Sie andere Serverkomponenten oder Framework Manager konfigurieren. Weitere Informationen finden Sie in „Installationsreihenfolge für Serverkomponenten" auf Seite 89.

Der einfachste und schnellste Weg zur Ausführung von IBM Cognos Analytics in Ihrer Umgebung besteht darin, das Funktionieren einer Basisinstallation in Ihrer Umgebung sicherzustellen.

Installationsmodi

Für eine vollständige Installation müssen Sie die Komponenten auf Ihrem Server installieren und sie dann für die Ausführung in Ihrer Umgebung konfigurieren.

Interaktiver Modus

Normalerweise führen Sie die Installations- und Konfigurationsprogramme für IBM Cognos im interaktiven Modus aus. Der Installationsassistent fordert Sie zur Eingabe von Informationen auf und das Konfigurationstool ermöglicht Ihnen die Änderung der Standardeinstellungen. Der Installationsassistent ist `ca_srv_<platform>_<build>.exe` (Windows) oder `ca_srv_<platform>_<build>.bin` (UNIX, Linux).

Hintergrundmodus

Sie können die Installation von Komponenten automatisieren, indem Sie Antwortdateien verwenden und das Installationsprogramm im Hintergrundmodus ausführen.

Sofern die installierten Komponenten identisch sind, können Sie die Konfiguration von Komponenten automatisieren, indem Sie die Konfigurationseinstellungen per Export von einem Computer auf andere übertragen. Führen Sie IBM Cognos Configuration beim ersten Mal im interaktiven Modus aus.

Die andere Möglichkeit besteht darin, die Datei cogstartup.xml zu bearbeiten (d. h. die Einstellungen Ihrer Umgebung anzupassen) und dann das Konfigurationstool im Hintergrundmodus auszuführen.

Interaktiver Modus auf UNIX-Systemen

Außer bei einer Installation im Hintergrundmodus installieren Sie die Software von einer Arbeitsstation mit X Window-System, einem X-Terminal oder einem PC oder sonstigen System mit installierter X-Server-Software.

Für die Installation im interaktiven Modus muss die an Ihren Computer angeschlossene Konsole eine Java-basierte grafische Benutzeroberfläche unterstützen.

Installieren von Serverkomponenten unter UNIX oder Linux

Wählen Sie mithilfe des Installationsassistenten die zu installierenden Serverkomponenten sowie den Pfad auf Ihrem Computer aus, in dem sie installiert werden sollen.

Vorbereitende Schritte

Rufen Sie die Webseite IBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235) auf um zu überprüfen, ob die erforderlichen Patches auf Ihrem Computer installiert sind.

Vorgehensweise

1. Stellen Sie die Umgebungsvariable JAVA_HOME so ein, dass Sie auf die Installationsposition Ihrer Java Runtime Environment (JRE), zum Beispiel `/Verzeichnis/java/Java_Version/jre` verweist.

   Damit IBM Cognos Analytics unter Linux ausgeführt werden kann, ist eine JVM erforderlich, wie z. B. die von IBM zur Verfügung gestellte JVM.
2. Wechseln Sie an die Speicherposition, an der die Installationsdateien heruntergeladen und extrahiert wurden.

   Tipp: Verwenden Sie neue Versionen von Dateikomprimierungssoftware zum Extrahieren der Dateien. Mit älteren Versionen solcher Software können die Dateien möglicherweise nicht extrahiert werden.
3. Wechseln Sie zum Starten des Installationsassistenten in das Betriebssystemverzeichnis und geben Sie den folgenden Befehl ein:

   ```
   ./ca_srv_<platform>_<build>.bin
   ```

   Dabei ist *<build>* die Buildnummer und *<platform>* ist win (Windows), i386 (Linux i386), ppcle (Linux pl E), ppc (Linux Power PC), s390x (Linux z), aix (AIX) oder zos (z/OS).

   Tipp: Bei Verwendung des Befehls `./ca_srv_<platform>_<build>.bin` mit XWindows werden japanische Zeichen in Nachrichten und Protokolldateien möglicherweise fehlerhaft angezeigt. Bei der Installation der japanischen Version unter UNIX oder Linux legen Sie zuerst die Umgebungsvariablen fest und starten dann den Installationsassistenten.

   Wenn Sie nicht mit XWindows arbeiten, führen Sie eine unbeaufsichtigte Installation durch. Weitere Informationen finden Sie im Installationshandbuch.
4. Folgen Sie den Anweisungen im Installationsassistenten, um die Dateien auf Ihren Computer zu kopieren.

   Verwenden Sie als Installationsposition ein Verzeichnis, dessen Pfadname ausschließlich ASCII-Zeichen enthält. Einige UNIX- und Linux-Web-Server unterstützen in Verzeichnisnamen nur ASCII-Zeichen.
5. Auf der Seite **Fertigstellen** des Installationsassistenten können Sie auf **Ansicht** klicken, um auf die Protokolldateien zuzugreifen. Sie sollten IBM Cognos Analytics nicht sofort konfigurieren, da Sie zunächst andere Aufgaben ausführen müssen, um sicherzustellen, dass Ihre Umgebung ordnungsgemäß eingerichtet ist.

Nächste Schritte

Sie können IBM Cognos Analytics mithilfe von IBM Cognos Configuration konfigurieren. Geben Sie den Befehl `cogconfig.sh` im Verzeichnis `install_location/bin64`, um Cognos Configuration zu starten.

Installieren von Serverkomponenten unter Windows

Wählen Sie mithilfe des Installationsassistenten die zu installierenden Serverkomponenten sowie den Pfad auf Ihrem Computer aus, in dem sie installiert werden sollen.

Bei Windows-Computern ist die Standardinstallationsposition das Verzeichnis **Programme**. Wenn Sie die Installation an dieser Position durchführen, müssen Sie sicherstellen, dass Sie IBM Cognos Configuration

als Administrator ausführen. Alternativ können Sie das Produkt außerhalb des Verzeichnisses **Programme** installieren, z. B. im Verzeichnis `C:\IBM\cognos\analytics`.

Für die Installation sind mindestens 5 GB Speicherplatz im temporären Verzeichnis erforderlich. Das temporäre Verzeichnis wird mit der Umgebungsvariablen TMP festgelegt.

Vorgehensweise

1. Wechseln Sie zu der Position, an der die Installationsdateien heruntergeladen und extrahiert wurden, und klicken Sie doppelt auf die Datei `ca_srv_<platform>_<build>.exe`.

   Tipp: Verwenden Sie neue Versionen von Dateikomprimierungssoftware zum Extrahieren der Dateien. Mit älteren Versionen solcher Software können die Dateien möglicherweise nicht extrahiert werden.
2. Wählen Sie die für die Installation zu verwendende Sprache aus.

   Die von Ihnen ausgewählte Sprache bestimmt die Sprache der Benutzeroberfläche. Es werden alle unterstützten Sprachen installiert. Die Sprache der Benutzeroberfläche kann nach der Installation in eine der installierten Sprachen geändert werden.
3. Folgen Sie den Anweisungen im Installationsassistenten, um die Dateien auf Ihren Computer zu kopieren.

   Sie können eine der folgenden Installationsoptionen auswählen:

   - Verwenden Sie die Option **Easy Install**, um Komponenten auf einem einzelnen Computer zu installieren, eine Instanz der Informix-Datenbank für den Content Store zu installieren und das System zu konfigurieren.

     Wichtig: Wenn Sie für Installationen des Typs **Easy Install** ein Upgrade durchführen (d. h. eine Installation auf der Basis einer vorhandenen Installation durchführen), beenden Sie zuerst manuell alle Services, einschließlich Informix- und ApacheDS-Services.
   - Verwenden Sie die Option **Angepasst** für eine verteilte Installation, um Komponenten auf mehreren Servern zu installieren.

   Installieren Sie die IBM Cognos Analytics-Komponenten in einem Verzeichnis, dessen Pfadname ausschließlich aus ASCII-Zeichen besteht. Einige Windows-Web-Server unterstützen in Verzeichnisnamen nur ASCII-Zeichen.

Installieren und Konfigurieren von Content Manager für das Inhaltsrepository

Sie können mehrere Instanzen von Content Manager installieren, um über einen Ausfallschutz zu verfügen, und Sie können Content Manager an einer anderen Position installieren als die übrigen Komponenten, um die Leistung zu verbessern.

Die Content Manager-Computer müssen die Position des Content Store, die Position der anderen Content Manager-Komponenten und die Datenbank kennen, die für die Benachrichtigung verwendet wird.

Bei einer verteilten Installation muss mindestens ein Computer, auf dem Content Manager installiert wird, konfiguriert und ausgeführt werden sowie zugänglich sein, bevor andere Computer in der IBM Cognos-Umgebung konfiguriert werden können. Dadurch wird sichergestellt, dass der Zertifizierungsstellenservice, der zusammen mit Content Manager installiert wird, zum Ausstellen von Zertifikaten für andere Computer verfügbar ist.

Ihre Installation enthält möglicherweise mehrere Content Manager, jeweils einen auf einem anderen Computer. Dabei ist ein Content Manager-Computer aktiv, während sich der oder die anderen Content Manager-Computer im Standby-Modus befinden.

Berechtigungen

Sie können die Installation sowohl mit als auch ohne Root-Berechtigung durchführen.

Außerdem berücksichtigt IBM Cognos Analytics die Dateimodus-Erstellungsmaske (umask) des Benutzerkontos, unter dem das Installationsprogramm ausgeführt wird. Dies betrifft nur die Installationsverzeichnisse. und hat keine Auswirkungen auf die Dateiberechtigungen innerhalb der Verzeichnisse. Während der Laufzeit generierte Dateien, wie zum Beispiel Protokolle, berücksichtigen die Maske jedoch. Verwenden Sie nach Möglichkeit umask 022 für das Installationsverzeichnis.

Regeln für die Konfiguration

In einer Installation mit mehreren Content Manager-Komponenten oder mit einer Position für Content Manager muss mindestens eine Content Manager-Instanz konfiguriert sein, ausgeführt werden und erreichbar sein, bevor Sie andere Komponenten in Ihrer Umgebung konfigurieren. Dadurch wird sichergestellt, dass der Zertifizierungsstellenservice, der zusammen mit Content Manager installiert wird, zum Ausstellen von Zertifikaten für andere IBM Cognos-Computer verfügbar ist.

Weitere Informationen über die Installationsreihenfolge bei verteilten Komponenten finden Sie in „Installationsreihenfolge für Serverkomponenten" auf Seite 89.

Regeln für aktiven Content Manager

Wenn Sie mehrere Content Manager-Komponenten installieren, wird der Content Manager-Computer, den Sie als Erstes starten, die standardmäßig aktive Content Manager-Instanz. Mithilfe von IBM Cognos Administration können Sie auch einen anderen Content Manager-Computer als standardmäßig aktiven Content Manager-Computer festlegen.

Die Content Manager-Standby-Computer dienen dem Ausfallschutz. Wenn der aktive Content Manager-Computer aufgrund eines Software- oder Hardwareausfalls nicht zur Verfügung steht, wird einer der im Standby-Modus laufenden Content Manager-Computer aktiv und die Anforderungen werden an diesen gerichtet.

Wenn der aktive Content Manager ausfällt, gehen die nicht gespeicherten Sitzungsdaten verloren. Sobald ein anderer Content Manager aktiviert wird, werden die Benutzer aufgefordert, sich anzumelden.

Weitere Informationen zur Aktivierung eines Content Manager-Service finden Sie im Handbuch *Verwaltung und Sicherheit*. Informationen über aktive und Standby-Instanzen von Content Manager finden Sie in „Aktive und Standby-Instanzen von Content Manager" auf Seite 93.

Bei Installationen mit mehreren Content Manager-Instanzen wird empfohlen, IBM Cognos Analytics für die Verwendung kompilierter Gateways anstelle des Standard-CGI-Gateways zu konfigurieren. Verwenden Sie beispielsweise das Apache-Modul für den Apache-Server oder für IBM HTTP Server oder verwenden Sie ISAPI für IIS. Andernfalls kann nach einem Ausfallschutz die Leistung beeinträchtigt sein.

Aktualisierung

Wenn Sie eine Aktualisierung von ReportNet oder einer früheren Version von IBM Cognos Business Intelligence durchführen, können Sie die vorhandenen Konfigurationsdaten verwenden. Einige Funktionen in IBM Cognos Analytics sind jedoch neu und müssen daher eventuell konfiguriert werden.

PowerCubes

Wenn Sie planen, IBM Cognos Transformer zu installieren und PowerCubes zu verwenden, die durch einen IBM Cognos Series 7-Namespace gesichert sind, müssen Sie Content Manager auf einem Computer installieren, der IBM Cognos Series 7 unterstützt.

Aktive und Standby-Instanzen von Content Manager

Sie können eine beliebige Anzahl an Content Manager-Instanzen installieren, obwohl immer nur eine Instanz aktiv sein kann. Die anderen Installationen fungieren jeweils als Standby-Content Manager.

Die Standby-Instanzen von Content Manager dienen dem Ausfallschutz. Wenn die aktive Content Manager-Instanz aufgrund eines Software- oder Hardwareausfalls nicht zur Verfügung steht, wird eine der

im Standby-Modus laufenden Content Manager-Instanzen aktiv und die Anforderungen werden an diese Instanz geleitet.

Wenn der aktive Content Manager ausfällt, gehen die nicht gespeicherten Sitzungsdaten verloren. Sobald ein anderer Content Manager aktiviert wird, werden die Benutzer aufgefordert, sich anzumelden.

Standardmäßig wird der erste mit IBM Cognos Analytics installierte Content Manager als aktiver Content Manager verwendet. Ein IBM Cognos Analytics-Serveradministrator kann die standardmäßige und die aktive Content Manager-Instanz jederzeit ändern. Beim Start von IBM Cognos Analytics sperrt der standardmäßige Content Manager den Zugriff aller übrigen Content Manager-Installationen auf den Content Store. Diese übrigen Content Manager-Instanzen wechseln in den Standby-Modus.

Dieser Ausfallschutzmechanismus funktioniert, weil die Dispatcher und der aktive Content Manager regelmäßig miteinander kommunizieren. Wenn ein Dispatcher diesen Content Manager nicht mehr erreichen kann, sendet der Dispatcher ein Signal an einen Standby-Content Manager, der daraufhin in den aktiven Modus wechselt. Die anderen Content Manager-Instanzen verbleiben zum weiteren Ausfallschutz im Standby-Modus. Die Standby-Instanzen von Content Manager rufen von der aktiven Content Manager-Instanz die kryptografischen Einstellungen wie den Common Symmetric Key (notwendig für die Verschlüsselung und Entschlüsselung von Daten) ab.

Wenn Sie mehrere Content Manager installieren, **müssen** Sie die Systemzeiten der Content Manager-Computer synchronisieren, damit die Ausfallschutzfunktion (Failover) zwischen den Content Managern erfolgreich ausgeführt werden kann.

Installieren von Content Manager unter UNIX oder Linux

Gehen Sie folgendermaßen vor, um Content Manager unter UNIX oder Linux zu installieren.

Vorbereitende Schritte

Rufen Sie die Webseite IBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235) auf um zu überprüfen, ob die erforderlichen Patches auf Ihrem Computer installiert sind.

Vorgehensweise

1. Stellen Sie die Umgebungsvariable JAVA_HOME so ein, dass Sie auf die Installationsposition Ihrer Java Runtime Environment (JRE), zum Beispiel `/Verzeichnis/java/Java_Version/jre` verweist.

   Damit IBM Cognos Analytics unter Linux ausgeführt werden kann, ist eine JVM erforderlich, wie z. B. die von IBM zur Verfügung gestellte JVM.
2. Wechseln Sie an die Speicherposition, an der die Installationsdateien heruntergeladen und extrahiert wurden.

   Tipp: Verwenden Sie neue Versionen von Dateikomprimierungssoftware zum Extrahieren der Dateien. Mit älteren Versionen solcher Software können die Dateien möglicherweise nicht extrahiert werden.
3. Wechseln Sie zum Starten des Installationsassistenten in das Betriebssystemverzeichnis und geben Sie Folgendes ein: `./ca_srv_<platform>_<build>.bin`

   Tipp: Bei Verwendung des Befehls `ca_srv_<platform>_<build>.bin` mit XWindows werden japanische Zeichen in Nachrichten und Protokolldateien möglicherweise fehlerhaft angezeigt. Bei der Installation der japanischen Version unter UNIX oder Linux legen Sie zuerst die Umgebungsvariablen fest und starten dann den Installationsassistenten.

   Wenn Sie nicht mit XWindows arbeiten, führen Sie eine unbeaufsichtigte Installation durch. Weitere Informationen finden Sie im Abschnitt Kapitel 5, „Unbeaufsichtigte Installation, Deinstallation und Konfiguration", auf Seite 31.
4. Folgen Sie den Anweisungen im Installationsassistenten, um die Dateien auf Ihren Computer zu kopieren und eine Basiskonfiguration zu implementieren.

   - Beachten Sie beim Auswählen des Verzeichnisses Folgendes:

Installieren Sie Content Manager in einem Verzeichnis, dessen Pfadname ausschließlich aus ASCII-Zeichen besteht. Einige UNIX- und Linux-Web-Server unterstützen in Verzeichnisnamen nur ASCII-Zeichen.

Wenn Sie IBM Cognos Analytics auf einem Computer installieren, auf dem bereits eine frühere Version von IBM Cognos Analytics installiert ist, und Sie die frühere Version weiterhin ausführen möchten, müssen Sie die neue Version in einem anderen Verzeichnis installieren.

- Löschen Sie bei der Auswahl der Komponenten alle Komponenten mit Ausnahme des **Inhaltsrepositorys**.

5. Klicken Sie auf **Fertigstellen**.

Nächste Schritte

Sie sollten IBM Cognos Analytics nicht sofort konfigurieren, da Sie zunächst andere Aufgaben ausführen müssen, um sicherzustellen, dass Ihre Umgebung ordnungsgemäß eingerichtet ist.

Sie können IBM Cognos Analytics später mithilfe von IBM Cognos Configuration konfigurieren, indem Sie `cogconfig.sh` im Verzeichnis *`Installationsposition`*`/bin64` eingeben.

Installieren von Content Manager unter Windows

Gehen Sie folgendermaßen vor, um Content Manager unter Microsoft Windows zu installieren.

Bei Windows-Computern ist die Standardinstallationsposition das Verzeichnis **Programme**. Wenn Sie die Installation an dieser Position durchführen, müssen Sie sicherstellen, dass Sie IBM Cognos Configuration als Administrator ausführen. Alternativ können Sie das Produkt außerhalb des Verzeichnisses **Programme** installieren, z. B. im Verzeichnis `C:\IBM\cognos\analytics`.

Für die Installation sind mindestens 5 GB Speicherplatz im temporären Verzeichnis erforderlich. Das temporäre Verzeichnis wird mit der Umgebungsvariablen TMP festgelegt.

Vorbereitende Schritte

Rufen Sie die Webseite IBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235) auf um zu überprüfen, ob die erforderlichen Patches auf Ihrem Computer installiert sind.

Vorgehensweise

1. Wechseln Sie zu der Position, an der die Installationsdateien heruntergeladen und extrahiert wurden, und klicken Sie doppelt auf die Datei `ca_srv_<platform>_<build>.exe`.

   Tipp: Verwenden Sie neue Versionen von Dateikomprimierungssoftware zum Extrahieren der Dateien. Mit älteren Versionen solcher Software können die Dateien möglicherweise nicht extrahiert werden.

2. Wählen Sie die für die Installation zu verwendende Sprache aus.

   Die von Ihnen ausgewählte Sprache bestimmt die Sprache der Benutzeroberfläche. Es werden alle unterstützten Sprachen installiert. Die Sprache der Benutzeroberfläche kann nach der Installation in eine der installierten Sprachen geändert werden.

3. Wählen Sie die Installationsoption **Angepasst** aus und folgen Sie den Anweisungen im Installationsassistenten, um die Dateien auf Ihren Computer zu kopieren.

   - Beachten Sie beim Auswählen des Verzeichnisses Folgendes:

     Installieren Sie Content Manager in einem Verzeichnis, dessen Pfadname ausschließlich aus ASCII-Zeichen besteht. Einige Microsoft Windows-Web-Server unterstützen in Verzeichnisnamen nur ASCII-Zeichen.

     Wenn Sie IBM Cognos Analytics auf einem Computer installieren, auf dem bereits eine frühere Version von IBM Cognos Analytics installiert ist, und Sie die frühere Version weiterhin ausführen möchten, müssen Sie IBM Cognos Analytics in einem anderen Verzeichnis installieren.

- Löschen Sie beim Auswählen der Komponenten alle Komponenten mit Ausnahme des **Inhaltsrepositorys** aus der Installationsoption **Angepasst**.

4. Klicken Sie auf **Fertigstellen**.

Nächste Schritte

Wenn Sie die Installation von IBM Cognos Configuration aus dem Installationsassistenten starten, müssen Sie vor der Ausführung der Services die in diesem Abschnitt beschriebenen zusätzlichen Aufgaben ausführen, um sicherzustellen, dass Ihre Umgebung korrekt eingerichtet ist.

IBM Cognos Configuration kann über die Verknüpfung **IBM Cognos Configuration** im Menü **Start** gestartet werden.

Einrichten der Datenbankverbindung für die Content Store-Datenbank

Möglicherweise müssen Sie Datenbank-Client-Software oder Java Database Connectivity-Treiber (JDBC-Treiber) oder beides auf jedem Computer installieren, auf dem Content Manager installiert wird. Dies ermöglicht Content Manager den Zugriff auf die Content Store-Datenbank.

Einrichten von Datenbankverbindungen für einen Microsoft SQL Server-Content Store

Der Microsoft-JDBC-Treiber ersetzt den JSQLConnect-Treiber für SQL Server. Der Download erfolgt über Microsoft. Dabei muss der neue Typ-4-Treiber im Ordner *installationsposition*/drivers abgelegt werden.

Die JAR-Treiberdatei sqljdbc42.jar ist für die Unterstützung der Java-Version erforderlich, die im Lieferumfang von IBM Cognos Analytics enthalten ist.

Wichtig: Für die Single Sign-on-Authentifizierung (SSO-Authentifizierung) und die Windows-Authentifizierung müssen Sie sqljdbc_auth.dll im Verzeichnis bin64 speichern. Bei der Windows-Authentifizierung handelt es sich um ein Single Sign-on-Setup. Die Auswahl für den Content Manager in Configuration Manager lautet **Microsoft SQL Server-Datenbank (Windows-Authentifizierung)**.

Einrichten von Datenbankverbindungen für einen IBM Db2-Content Store

Diese Prozedur beschreibt die Vorgehensweise beim Einrichten der Datenbankverbindungen für einen Db2-Content Store. Sie müssen diese Prozedur auf jedem Computer ausführen, auf dem Sie Content Manager installieren.

Sie müssen einen JDBC-Treiber vom Typ 4 (Java Database Connectivity) verwenden, um eine Verbindung zu Ihrem Content Store herzustellen.

Der Treiber vom Typ 4 gilt als unabhängiges Produkt. Er setzt nicht voraus, dass der Db2-Client installiert ist.

Vorgehensweise

Kopieren Sie die folgenden Dateien vom Verzeichnis *DB2-Installation*\sqllib\java in das Verzeichnis *Installationsposition*\drivers:

- Die universelle Treiberdatei db2jcc4.jar
- Die Lizenzdatei:

  Für Db2 unter Linux, UNIX oder Windows verwenden Sie die Datei db2jcc_license_cu.jar.

  Für Db2 unter z/OS verwenden Sie die Datei db2jcc_license_cisuz.jar.

  Wenn Sie eine Verbindung mit Db2 unter z/OS herstellen, verwenden Sie die Treiberversion aus Linux, UNIX oder Windows Version 9.1 Fixpack 5 oder Version 9.5 Fixpack 2.

  Tipp: Führen Sie zur Überprüfung der Treiberversion den folgenden Befehl aus:

```
java -cp Pfad\db2jcc4.jar com.ibm.db2.jcc.DB2Jcc -version
```

Generieren einer Scriptdatei zur Erstellung einer Datenbank für einen IBM Db2-Content Store

Sie können eine Scriptdatei zur automatischen Erstellung des Content Store in Db2 auf allen Plattformen generieren. Bei der Scriptdatei handelt es sich um eine DDL-Datei.

Vorgehensweise

1. Starten Sie **IBM Cognos Configuration**.
2. Klicken Sie im Fenster **Explorer** unter **Datenzugriff** > **Content Manager** auf **Content Store**.

   Die Standardkonfiguration gilt für eine Db2-Datenbank. Vergewissern Sie sich, dass als **Typ** die Einstellung **DB2-Datenbank** angegeben ist.
3. Geben Sie im Feld **Datenbankserver und Portnummer** den Namen Ihres Computers und die Portnummer ein, unter denen Db2 ausgeführt wird.
   Beispiel: `localhost:50000`. Dabei ist 50000 die von Db2 verwendete Standardportnummer. Wenn Sie eine andere Portnummer verwenden, müssen Sie diesen Wert verwenden.
4. Klicken Sie neben der Eigenschaft **Benutzerkennung und Kennwort** auf das Feld **Wert** und danach auf das Bearbeitungssymbol. Geben Sie die entsprechenden Werte ein und klicken Sie auf **OK**.
5. Geben Sie im Fenster **Eigenschaften** unter **Datenbankname** einen Namen für die Content Store-Datenbank ein.

   Wichtig: Der Name darf maximal acht Zeichen lang sein und nur Buchstaben, Zahlen, Unterstriche und Bindestriche enthalten.
6. Klicken Sie mit der rechten Maustaste auf **Content Store** und dann auf **DDL generieren**.
7. Klicken Sie auf **Details**, um die Position aufzuzeichnen, unter der sich die generierte DDL-Datei befindet.

   Die DDL-Datei mit dem Namen `createDB.sql` wird erstellt. Das Script wird im Verzeichnis *installationsposition*`\configuration\schemas\content\db2` erstellt.

Nächste Schritte

Verwenden Sie dieses Script zum Erstellen einer Datenbank in Db2. Weitere Informationen zur Verwendung einer DDL-Datei finden Sie in der Dokumentation zu Db2.

Über die Db2-Befehlszeilenschnittstelle können Sie das Script durch Eingeben des folgenden Befehls ausführen:

```
db2 -tvf createDB.sql
```

Erstellen von Tabellenbereichen für einen Content Store in IBM Db2 for z/OS

Um einen Satz von Tabellenbereichen zu erstellen, der für die Content Store-Datenbank erforderlich ist, muss der Datenbankadministrator Scripts ausführen. In diesen Scripts müssen die Platzhalterparameter durch die Parameter für Ihre Umgebung ersetzt werden. Standardmäßig werden im Content Store Benachrichtigungen, benutzergeführte Aufgaben und Anmerkungen gespeichert. Für jede dieser Textsorten können Sie eigene Datenbanken erstellen.

Informationen zu diesem Vorgang

Stellen Sie sicher, dass Sie die Namenskonventionen für Db2 unter z/OS verwenden. Beispielsweise müssen alle Parameternamen mit einem Buchstaben anfangen und dürfen maximal acht Zeichen lang sein. Zur Zeichenlängenbegrenzung gibt es zwei Ausnahmen:

- CMSCRIPT_CS_ID darf nicht mehr als zwei Zeichen umfassen.
- CMSCRIPT_TABLESPACE darf nicht mehr als sechs Zeichen umfassen.

Diese Ausnahmen beruht darauf, dass bei einer Verknüpfung der beiden Parameter die Zeichenlänge nicht mehr als acht Zeichen betragen darf.

Weitere Informationen finden Sie im IBM Db2 for z/OS Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSEPEK/db2z_prodhome.html).

Vorgehensweise

1. Stellen Sie als Benutzer mit Berechtigungen zum Erstellen und Löschen von Tabellenbereichen sowie zum Ausführen von SQL-Anweisungen eine Verbindung zur Datenbank her.
2. Wechseln Sie in das Verzeichnis, das die Scripts enthält:

   installationsposition/configuration/schemas/content/db2z0S
3. Erstellen Sie eine Sicherungskopie der Scriptdatei `tablespace_db2z0S.sql` und speichern Sie die Datei in einem anderen Verzeichnis.
4. Öffnen Sie die ursprüngliche Scriptdatei `tablespace_db2z0S.sql`.
   a) Fügen Sie am Anfang des Scripts eine Verbindungsanweisung hinzu.

      Beispiel:

      ```
      connect to Datenbankname;
      ```

   b) Verwenden Sie die folgende Tabelle, um die generischen Parameter durch die Parameter zu ersetzen, die für Ihre Umgebung geeignet sind.

      Die Tabelle führt auch Parameter auf, die zwar noch nicht im Script enthalten sind, aber möglicherweise noch hinzugefügt werden.

Tabelle 10. Namen und Beschreibungen der Parameter im Tabellenbereichsscript für den Content Store

Parametername	Beschreibung
CMSCRIPT_STOGROUP	Gibt den Namen der Speichergruppe an.
CMSCRIPT_DATABASE	Gibt den Namen der Content Store-Datenbank an.
CMSCRIPT_CS_ID	Legt die Subsystemkennung der Content Store-Datenbank fest. Die Kennung darf maximal zwei Zeichen lang sein.
CMSCRIPT_TABLESPACE	Gibt den Namen des Tabellenbereichs an, der alle Basistabellen des Content Store enthält. Hilfstabellen sind nicht enthalten. Der Name darf maximal sechs Zeichen lang sein.
CMSCRIPT_LARGE_BP	Gibt den Namen des großen Pufferpools an, der für besonders große Objekte reserviert ist. Dies ist der 32 KB große Pufferpool, der bei der Erstellung der Content Store-Datenbank unter z/OS erstellt wurde.

Tabelle 10. Namen und Beschreibungen der Parameter im Tabellenbereichsscript für den Content Store (Forts.)	
Parametername	**Beschreibung**
CMSCRIPT_REGULAR_BP	Gibt den Namen des normal großen Pufferpools an, der für normale und große Objekte reserviert ist. Dies ist der 16 KB große Pufferpool, der bei der Erstellung der Content Store-Datenbank unter z/OS erstellt wurde.
CMSCRIPT_USERNAME	Gibt den Namen des Benutzerkontos an, das auf die Content Store-Datenbank zugreift.

5. Speichern Sie das Script und führen Sie es aus.

   Wenn Sie Ihre `clp.properties`-Datei und Ihren Db2-Alias in Ihrem Profil bzw. in der Scriptdatei `tcshrc` angegeben haben, geben Sie zur Ausführung des Scripts zum Beispiel folgenden Befehl ein:

   ```
   db2 -tvf tablespace_db2z0S.sql
   ```

6. Gewähren Sie dem IBM Cognos-Benutzer die Rechte für die Tabellenbereiche, die beim Ausführen der Scriptdatei `tablespace_db2z0S.sql` erstellt wurden.
   a) Erstellen Sie eine Kopie der Scriptdatei `rightsGrant_db2z0S.sql` und speichern Sie sie unter einer anderen Position.
   b) Öffnen Sie die ursprüngliche Scriptdatei `rightsGrant_db2z0S.sql` im Fernzugriffstool und ersetzen Sie die Platzhalterparameter durch die für Ihre Umgebung geeigneten Werte.

      Stellen Sie sicher, dass Sie dieselben Werte verwenden wie bei der Zuweisung von Ressourcen zu den Pufferpools bzw. zum Benutzerkonto.

      .

   c) Fügen Sie am Anfang des Scripts eine Verbindungsanweisung hinzu.

      Beispiel:

      ```
      connect to Datenbankname user Benutzername using Kennwort;
      ```

   d) Speichern Sie das Script und führen Sie es dann aus.

      Beispiel:

      ```
      db2 -tvf rightsGrant_db2z0S.sql
      ```

7. Wechseln Sie zur Erstellung der Tabellenbereiche mit den Benachrichtigungen in das Verzeichnis *Installationsposition*`/configuration/schemas/delivery/zosdb2`.
   a) Erstellen Sie eine Sicherungskopie der Scriptdatei `NC_TABLESPACES.sql` und speichern Sie die Datei an einer anderen Position.
   b) Öffnen Sie die ursprüngliche Scriptdatei `NC_TABLESPACES.sql` und ersetzen Sie die Platzhalterparameter mithilfe der folgenden Tabelle durch die für Ihre Umgebung geeigneten Parameter.

Tabelle 11. Parameternamen und Beschreibungen für Tabellenbereiche für die Db2-Benachrichtigungsdatenbank unter z/OS	
Parametername	**Beschreibung**
NCCOG	Gibt den Namen der Benachrichtigungsdatenbank an.

Tabelle 11. Parameternamen und Beschreibungen für Tabellenbereiche für die Db2-Benachrichtigungsdatenbank unter z/OS (Forts.)	
Parametername	**Beschreibung**
DSN8G810	Gibt den Namen der Speichergruppe an.
BP32K	Gibt den Namen des Pufferpools an.

Die Tabelle beschreibt auch Parameter, die noch nicht im Script enthalten sind, möglicherweise aber in Zukunft hinzugefügt werden.

c) Speichern Sie das Script und führen Sie es aus.

Beispiel:

```
db2 -tvf NC_TABLESPACES.sql
```

d) Öffnen Sie die Scriptdatei `NC_CREATE_DB2.sql` und ersetzen Sie den Platzhalterparameter NCCOG durch den Namen der Benachrichtigungsdatenbank.

e) Speichern Sie das Script.

Das Script wird von den Services für die Job- und Zeitplanüberwachung automatisch ausgeführt. Sie können es jedoch auch selbst ausführen.

8. Wechseln Sie zur Erstellung der Tabellenbereiche mit den benutzergeführten Aufgaben in das Verzeichnis *installationsposition*`/configuration/schemas/hts/zosdb2`.

a) Erstellen Sie eine Sicherungskopie der Scriptdatei `HTS_tablespaces.sql` und speichern Sie die Datei unter einer anderen Position.

b) Öffnen Sie die ursprüngliche Scriptdatei `HTS_TABLESPACES.sql` und ersetzen Sie mithilfe der folgenden Tabelle die Standardparameter durch die für Ihre Umgebung geeigneten Parameter.

Tabelle 12. Parameternamen für Tabellenbereiche und Beschreibungen für benutzergeführte Aufgaben in Db2 unter z/OS	
Parametername	**Beschreibung**
NCCOG	Legt den Namen der Datenbank fest.
DSN8G810	Gibt den Namen der Speichergruppe an.
BP32K	Gibt den Namen des 32-K-Pufferpools an.

Eine vollständige Liste der erforderlichen Parameter ist im Script enthalten.

c) Speichern Sie das Script und führen Sie es aus.

d) Öffnen Sie die Scriptdatei `HTS2_CREATE_Db2zos.sql` und ersetzen Sie die generischen Parameter durch die für Ihre Umgebung geeigneten Parameter mithilfe der folgenden Tabelle.

Tabelle 13. Parameternamen für Tabellenbereiche und Beschreibungen für benutzergeführte Aufgaben in Db2 unter z/OS	
Parametername	**Beschreibung**
NCCOG	Der Name der Datenbank.

Eine vollständige Liste der erforderlichen Parameter ist im Script enthalten.

e) Speichern Sie das Script und führen Sie es aus.

9. Wechseln Sie zur Erstellung der Tabellenbereiche mit den Anmerkungen in das Verzeichnis *installationsposition*/configuration/schemas/ans/zosdb2.
   a) Erstellen Sie eine Sicherungskopie der Scriptdatei ANN_TABLESPACES.sql und speichern Sie die Datei an einer anderen Position.
   b) Öffnen Sie die ursprüngliche Scriptdatei ANN_TABLESPACES.sql und ersetzen Sie mithilfe der folgenden Tabelle die Standardparameter durch die für Ihre Umgebung geeigneten Parameter.

Tabelle 14. Parameternamen für Tabellenbereiche und Beschreibungen für Anmerkungen in Db2 unter z/OS	
Parametername	**Beschreibung**
NCCOG	Der Name der Datenbank.
DSN8G810	Der Name der Speichergruppe.
BP32K	Der Name des 32-K-Pufferpools.

   Eine vollständige Liste der erforderlichen Parameter ist im Script enthalten.
   c) Speichern Sie das Script und führen Sie es aus.
   d) Öffnen Sie die Scriptdatei ANS2_CREATE_Db2zos.sql und ersetzen Sie die generischen Parameter durch die für Ihre Umgebung geeigneten Parameter mithilfe der folgenden Tabelle.

Tabelle 15. Parameternamen für Tabellenbereiche und Beschreibungen für Anmerkungen in Db2 unter z/OS	
Parametername	**Beschreibung**
NCCOG	Der Name der Datenbank.

   Eine vollständige Liste der erforderlichen Parameter ist im Script enthalten.
   e) Speichern Sie das Script und führen Sie es aus.

Einrichten einer Datenbankverbindung für einen Oracle-Content Store

Diese Prozedur beschreibt die Vorgehensweise beim Einrichten der Datenbankverbindungen für einen Oracle-Content Store. Sie müssen diese Prozedur auf jedem Computer ausführen, auf dem Sie Content Manager installieren.

Vorgehensweise

1. Wechseln Sie auf dem Computer, auf dem der Oracle-Client installiert ist, in das Verzeichnis *ORACLE_HOME*/jdbc/lib.
2. Kopieren Sie die korrekte Bibliotheksdatei für Ihre Version des Oracle-Clients in das Verzeichnis *Installationsposition*\drivers auf dem Computer, auf dem Content Manager installiert ist und auf dem Benachrichtigungen an eine Oracle-Datenbank gesendet werden.

   Wenn Sie mit Oracle Version 12c Release 2 arbeiten, müssen Sie über die Datei 'ojdbc8.jar' verfügen.

   Wenn Sie mit Oracle Version 12c Release 1 arbeiten, müssen Sie über die Datei 'ojdbc7.jar' verfügen.

   Wenn Sie mit Oracle Version 11g Release 2 arbeiten, müssen Sie über die Datei 'ojdbc6.jar' verfügen.

   Anmerkung: Weitere Informationen finden Sie in den FAQ zu Oracle JDBC.

   Die Dateien sind bei Installation eines Oracle-Clients oder -Servers verfügbar oder können von der Technologie-Website von Oracle heruntergeladen werden.

Einrichten einer Datenbankverbindung für einen Informix-Content Store

Diese Prozedur beschreibt die Vorgehensweise beim Einrichten der Datenbankverbindungen für einen Informix-Content Store. Sie müssen diese Prozedur auf jedem Computer ausführen, auf dem Sie Content Manager installieren.

Vorgehensweise

1. Wechseln Sie auf dem Computer, auf dem Informix installiert ist, in das Verzeichnis *Informix_Position*/sqllib/java.
2. Kopieren Sie die folgenden Dateien in das Verzeichnis *Installationsposition*\drivers auf jedem Computer, auf dem Content Manager installiert ist.
   - Die universelle Treiberdatei db2jcc4.jar
   - Die Lizenzdatei db2jcc4_license_cisuz.jar

Kritische Konfigurationsaktionen, die zuerst erledigt werden müssen!

Diese Konfigurationsaktionen sind für den Erfolg der Installation entscheidend. Führen Sie diese Aktionen nach der Installation der Komponenten aus.

Sicherstellen, dass JDBC-Treiber an der richtigen Position sind

Für das Release IBM Cognos Analytics 11.1.x müssen die JDBC-Treiber in das Verzeichnis *Installationsposition*\drivers kopiert werden.

Die Verwendung von *Installationsposition*\webapps\p2pd\WEB-INF\lib für JDBC-Treiber wird nicht unterstützt.

JSQL-Treiber für Microsoft SQL Server durch den Microsoft-JDBC-Treiber ersetzen

Ab IBM Cognos Analytics Version 11.0.5 wurde der JSQL-Treiber für Microsoft SQL Server durch den Microsoft-JDBC-Treiber ersetzt. Sie müssen die erforderliche JAR-Datei herunterladen und in das Verzeichnis *Installationsposition*\drivers platzieren. Weitere Informationen finden Sie in Setup für einen Microsoft SQL Server-Content Store.

Eigenschaft Konfigurationsgruppe angeben

Wenn Sie IBM Cognos Analytics **angepasst** installiert haben, öffnen Sie IBM Cognos Configuration und legen Sie die Eigenschaft **Konfigurationsgruppe** fest. Weitere Informationen finden Sie in Verwalten der Konfigurationsgruppe.

Webbasierte Modellierung aktivieren oder inaktivieren

Standardmäßig werden in IBM Cognos Administration erstellte JDBC-Datenquellen nicht in der **Verwalten** > **Datenserver**-Verwaltungsschnittstelle zur Verwendung in Datenmodulen zugänglich gemacht. Wenn Sie Ihre vorhandenen (aktualisierten) Datenquellenverbindungen zum Erstellen von Datenmodulen verwenden wollen, müssen Sie für diese Verbindungen die webbasierte Modellierung aktivieren.

Einige Datenquellen sind für die Verwendung als Quellen zur Erstellung von Datenmodulen ungeeignet. In diesem Fall können Sie die Verwendung von webbasierter Modellierung für die Datenquellenverbindungen untersagen.

Führen Sie folgende Schritte aus, um die webbasierte Modellierung für Ihre Datenquellenverbindungen zu aktivieren oder zu inaktivieren:

1. Wechseln Sie in IBM Cognos Analytics zu **Verwalten** > **Administrationskonsole**.
2. Wählen Sie in IBM Cognos Administration auf der Registerkarte **Konfiguration** die Option **Datenquellenverbindungen** aus.

3. Suchen Sie die Datenquelle und klicken Sie auf die zugehörige Aktion **Eigenschaften festlegen**.
4. Wählen Sie auf der Registerkarte **Verbindung** das Kontrollkästchen **Webbasierte Modellierung zulassen** aus oder ab.

Starten von IBM Cognos Configuration

Mit IBM Cognos Configuration können Sie IBM Cognos Analytics-Komponenten konfigurieren und IBM Cognos-Services starten und stoppen.

Vorbereitende Schritte

Bevor Sie IBM Cognos Configuration starten, müssen Sie sicherstellen, dass die Betriebsumgebung ordnungsgemäß eingerichtet ist. Prüfen Sie beispielsweise, ob alle Umgebungsvariablen definiert wurden.

Unter dem Microsoft Windows-Betriebssystem können Sie IBM Cognos Configuration nur von der letzten Seite des Installationsassistenten aus starten, wenn keine zusätzlichen Einrichtungsschritte erforderlich sind. Wenn Sie beispielsweise einen anderen Datenbankserver als Microsoft SQL für den Content Store verwenden, kopieren Sie die JDBC-Treiber (Java Database Connectivity) vor dem Starten des Konfigurationstools in den Ordner *installationsposition*/drivers.

Starten Sie unter UNIX- oder Linux-Betriebssystemen IBM Cognos Configuration nicht von der letzten Seite des Installationsassistenten aus. Bevor Sie IBM Cognos Analytics konfigurieren können, sind zusätzliche Einrichtungsschritte erforderlich. Beispielweise müssen Sie die Java-Umgebung aktualisieren.

Vergewissern Sie sich, dass ein Benutzerkonto oder ein Servicekonto für die Ausführung von IBM Cognos eingerichtet ist.

Lesen Sie „Kritische Konfigurationsaktionen, die zuerst erledigt werden müssen!" auf Seite 102.

Vorgehensweise

1. Klicken Sie unter Microsoft Windows auf **Start** > **IBM Cognos Configuration**.

   Wenn Sie einen Windows-Computer verwenden und das Produkt im Verzeichnis Programme (x86) installiert haben, starten Sie IBM Cognos Configuration als Administrator.
2. Wechseln Sie unter UNIX oder Linux in das Verzeichnis *installationsposition*/bin und geben Sie den folgenden Befehl ein:

   ```
   ./cogconfig.sh
   ```

   Wenn IBM Cognos Configuration nicht geöffnet wird, stellen Sie sicher, dass Sie die Umgebungsvariable DISPLAY angegeben haben.

   Wenn eine Nachricht des Typs JAVA.Lang.unsatisfied link angezeigt wird, vergewissern Sie sich, dass Sie eine unterstützte Java-Version verwenden.

   Wenn eine Nachricht des Typs Java.lang.unsupportedClassVersionError angezeigt wird, vergewissern Sie sich, dass Sie die 64-Bit-Version von Java verwenden.

Erstellen der Datenbankverbindungseigenschaften für den Content Store

Sie müssen Datenbankserverinformationen angeben, um sicherzustellen, dass Content Manager eine Verbindung zu der Datenbank herstellen kann, die Sie als Content Store verwenden. Content Manager greift mithilfe der Datenbankanmeldung auf den Content Store zu. Nach der Einrichtung der Datenbankverbindungseigenschaften können Sie die Verbindung zwischen Content Manager und dem Content Store testen.

In einer Produktionsumgebung müssen Sie eine für Unternehmen geeignete Datenbank für den Content Store verwenden. Weitere Informationen finden Sie im Abschnitt über die Bereitstellung des gesamten Content Store im Handbuch 'Verwaltung und Sicherheit'.

Wenn Sie ein Upgrade von IBM Cognos Business Intelligence oder einem früheren Release von IBM Cognos Analytics durchführen, konfigurieren Sie IBM Cognos Analytics so, dass es auf eine Kopie der vorhandenen Content-Store-Datenbank verweist. Nach dem Speichern der Konfiguration und dem Starten des IBM Cognos-Service werden die Daten im Content Store automatisch aktualisiert und können nicht von der früheren Version verwendet werden. Durch die Verwendung der neuen Version mit einer Kopie der ursprünglichen Datenbank können Sie IBM Cognos Analytics oder die frühere Version mit den ursprünglichen Daten weiter betreiben.

Vergewissern Sie sich, dass Sie den Content Store mit einem der unterstützten Datenbankserver erstellt haben.

Einrichten von Datenbankverbindungseigenschaften für einen IBM Db2-Content Store

Sie müssen Datenbankserverinformationen angeben, um sicherzustellen, dass Content Manager eine Verbindung zu der Datenbank herstellen kann, die Sie als Content Store verwenden.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration von der Position aus, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Datenzugriff** auf **Content Manager** und dann auf **Content Store**.
3. Geben Sie im Fenster **Eigenschaften** für die Eigenschaft **Datenbankname** den Namen der Datenbank oder den Datenbankalias ein.
4. Ändern Sie die Anmeldeberechtigungsnachweise, indem Sie eine gültige Kombination aus Benutzer-ID und Kennwort eingeben:
   - Klicken Sie auf das Feld **Wert** neben der Eigenschaft **Benutzer-ID und Kennwort** und klicken Sie auf die Schaltfläche zum Bearbeiten, sobald sie angezeigt wird.
   - Geben Sie die entsprechenden Werte ein und klicken Sie auf **OK**.
5. Geben Sie im Feld **Datenbankserver und Portnummer** den Namen Ihres Computers und die Portnummer ein, unter denen Db2 ausgeführt wird. Beispiel: `localhost:50000`. 50000 ist die von Db2 verwendete Standardportnummer. Wenn Sie eine andere Portnummer verwenden, müssen Sie diesen Wert verwenden.
6. Klicken Sie im Menü **Datei** auf **Speichern**.
7. Um die Verbindung zwischen Content Manager und der Content Store-Datenbank zu testen, klicken Sie im Menü **Aktionen** auf **Test**.

   Content Manager stellt eine Verbindung zur Datenbank her, überprüft die Datenbankberechtigungen, erstellt eine Tabelle und füllt diese aus. Diese Tabelle wird nicht gelöscht, sondern bei jeder Wiederholung des Tests erneut verwendet.

Einrichten von Datenbankverbindungseigenschaften für einen Content Store in IBM Db2 for z/OS

Sie müssen Datenbankserverinformationen angeben, um sicherzustellen, dass Content Manager eine Verbindung zu der Datenbank herstellen kann, die Sie für den Content Store verwenden.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration von der Position aus, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Datenzugriff** > **Content Manager** auf **Content Store**.
3. Geben Sie im Fenster **Eigenschaften** für die Eigenschaft **Datenbankname** den Namen der Datenbank oder den Datenbankalias ein.
4. Ändern Sie die Anmeldeberechtigungsnachweise, indem Sie eine gültige Kombination aus Benutzer-ID und Kennwort eingeben:

- Klicken Sie auf das Feld **Wert** neben der Eigenschaft **Benutzerkennung und Kennwort** und klicken Sie auf das Bearbeitungssymbol, sobald es angezeigt wird. Stellen Sie sicher, dass die eingegebene Benutzer-ID dem Wert entspricht, den Sie beim Erstellen der Tabellenbereiche für **CMSCRIPT_USERNAME** angegeben haben.
- Geben Sie die entsprechenden Werte ein und klicken Sie auf **OK**.

5. Geben Sie in das Feld für die Eigenschaft **Datenbankserver und Portnummer** die Datenbankinformationen in der Form *Hostname*:*Port* ein.
6. Klicken Sie im Fenster **Explorer** auf **Lokale Konfiguration**.
7. Klicken Sie in das Feld **Wert** für **Erweiterte Eigenschaften** und klicken Sie dann auf das Bearbeitungssymbol.

   Das Dialogfeld **Wert - Erweiterte Eigenschaften** wird geöffnet.
8. Klicken Sie auf **Hinzufügen**, um die Parameter für die Datenbankverbindung hinzuzufügen.

   Die Werte in der Tabelle sind Beispiele. Stellen Sie sicher, dass Sie die korrekten Werte für Ihre Umgebung eingeben.

Tabelle 16. Content Store-Verbindungsparameter für Db2 for z/OS

Parametername	**Beispielwert**
CMSCRIPT_CREATE_IN	COGUCS.T1TSCS
CMSCRIPT_STOGROUP	DBOIUSR
CMSCRIPT_DATABASE	COGUCS
CMSCRIPT_CS_ID	T1
CMSCRIPT_TABLESPACE	TSCS
CMSCRIPT_LARGE_BP	BP32K
CMSCRIPT_REGULAR_BP	BP16K0

9. Klicken Sie auf **Datei** > **Speichern**.
10. Um die Verbindung zwischen Content Manager und der Content Store-Datenbank zu testen, klicken Sie im Menü **Aktionen** auf **Test**.

Einrichten von Datenbankverbindungseigenschaften für einen Microsoft SQL Server-, Oracle- oder Informix-Content Store

Sie müssen Datenbankserverinformationen angeben, um sicherzustellen, dass Content Manager eine Verbindung zu der Datenbank herstellen kann, die Sie als Content Store verwenden.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Computer, auf dem Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Datenzugriff** auf **Content Manager**. Klicken Sie dann mit der rechten Maustaste auf **Content Store** und klicken Sie auf **Löschen**.

   Durch diesen Schritt wird die Verbindung zur Standardressource gelöscht. Content Manager kann nur auf einen Content Store zugreifen.
3. Klicken Sie mit der rechten Maustaste auf **Content Manager** und anschließend auf **Neue Ressource**, **Datenbank**.
4. Geben Sie in das Feld **Name** einen Namen für die Ressource ein.
5. Wählen Sie im Feld **Typ** den Datenbanktyp aus und klicken Sie auf **OK**.

   Tipp: Um eine Oracle PDB- oder Oracle RAC-Funktionalität zu verwenden, wählen Sie **Oracle-Datenbank (Erweitert)** aus.
6. Geben Sie im Fenster **Eigenschaften** die für Ihren Datenbanktyp erforderlichen Werte ein:

- Wenn Sie eine Microsoft SQL Server-Datenbank verwenden, geben Sie die entsprechenden Werte für die Eigenschaften **Datenbankserver mit Portnummer oder Instanzname** und **Datenbankname** ein.

  Wenn Sie eine Microsoft SQL Server-Datenbank verwenden, können Sie als Wert für die Eigenschaft **Datenbankserver und Portnummer oder Instanzname** eine Portnummer (z. B. 1433) oder eine benannte Instanz verwenden.

  Geben Sie bei der Eigenschaft **Datenbankserver mit Portnummer oder Instanzname** den Instanznamen an, wenn mehrere Instanzen von Microsoft SQL Server vorhanden sind.

  Zum Verbinden mit einer benannten Instanz müssen Sie den Namen der Instanz als JDBC-URL-Eigenschaft (Java Database Connectivity) oder als Datenquelleneigenschaft angeben. Sie können beispielsweise `localhost\instance1` eingeben. Wenn keine Instanznameneigenschaft angegeben wurde, wird eine Verbindung zur Standardinstanz hergestellt.

  Die für die benannte Instanz angegebenen Eigenschaften werden zusammen mit der Benutzer-ID, dem Kennwort und dem Datenbanknamen verwendet, um eine JDBC-URL zu erstellen. Beispiel:

  ```
  jdbc:JSQLConnect://localhost\\instance1/user=sa/weitere Eigenschaften nach Bedarf
  ```

- Wenn Sie eine Oracle-Datenbank verwenden, geben Sie die entsprechenden Werte für die Eigenschaften **Datenbankserver und Portnummer** und **SID** ein.
- Wenn Sie eine Oracle PDB Oracle PDB (Pluggable Database) verwenden, geben Sie für die Eigenschaft **Datenbankspezifikation** Folgendes an: *//<server>/<servicename>*. Beispiel: `//corp-serv1:1522/PDB1`
- Wenn Sie eine erweiterte Oracle Net 8-Datenbank verwenden, geben Sie für die Eigenschaft **Datenbankspezifikation** das Oracle Net8-Schlüsselwort/Wertepaar für die Verbindung ein.

  Es folgt ein Beispiel für ein Oracle Net8-Schlüsselwort/Wertepaar:

  ```
  (description=(address=(host=myhost)(protocol=tcp)(port=1521)
  (connect_data=(sid=(orcl)))))
  ```

  Wenn Sie die erweiterte Oracle-Datenbank auswählen, verwendet IBM Cognos Analytics unternehmensorientierte Oracle-Funktionen zum Auswählen eines Empfängers, zum Wechseln auf einen anderen Empfänger (sollte der erste Empfänger ausfallen), zur automatischen Herstellung einer neuen Datenbankverbindung (sollte die Verbindung fehlschlagen) sowie zum Verteilen von Verbindungsanforderungen unter den Empfängern bzw. den Dispatchern.
- Wenn Sie eine Informix-Datenbank verwenden, geben Sie die entsprechenden Werte für die Eigenschaften **Datenbankserver und Portnummer** und **Datenbankname** ein.

7. Um Anmeldeberechtigungsnachweise zu konfigurieren, legen Sie eine Benutzer-ID und ein Kennwort fest:
   - Klicken Sie auf das Feld **Wert** neben der Eigenschaft **Benutzerkennung und Kennwort** und klicken Sie auf das Bearbeitungssymbol, sobald es angezeigt wird.
   - Geben Sie die entsprechenden Werte ein und klicken Sie auf **OK**.
8. Wenn Sie mehr als eine Content Store-Datenbank in Ihrer Informix-Instanz speichern, erstellen Sie die erweiterte Eigenschaft CMSCRIPT_CS_ID und geben Sie den das Konto an, unter dem die Instanz ausgeführt wird:
   - Klicken Sie im Fenster **Explorer** auf **Lokale Konfiguration**.
   - Klicken Sie im Fenster **Eigenschaften** auf die Spalte **Wert** für **Erweiterte Eigenschaften** und anschließend auf das Bearbeitungssymbol.
   - Klicken Sie im Dialogfeld **Wert - Erweiterte Eigenschaften** auf **Hinzufügen**.
   - Geben Sie in der Spalte **Name** den Text `CMSCRIPT_CS_ID` ein.
   - Geben Sie in der Spalte **Wert** die Benutzer-ID des Kontos ein, unter dem die Instanz des Content Store ausgeführt wird.

Verwenden Sie für jede Instanz des Informix-Content Store ein anderes Benutzerkonto.

9. Klicken Sie im Menü **Datei** auf **Speichern**.

   Die Anmeldeberechtigungsnachweise werden sofort verschlüsselt.

10. Um die Verbindung zwischen Content Manager und der Content Store-Datenbank zu testen, klicken Sie im Menü **Aktionen** auf **Test**.

    Content Manager stellt eine Verbindung zur Datenbank her, überprüft die Datenbankberechtigungen, erstellt eine Tabelle und füllt diese aus. Diese Tabelle wird nicht gelöscht, sondern bei jeder Wiederholung des Tests erneut verwendet.

Ergebnisse

Mit Content Manager können die erforderlichen Tabellen im Content Store beim ersten Start des IBM Cognos-Service erstellt werden. Wenn die Verbindungseigenschaften nicht korrekt angegeben sind, können Sie die IBM Cognos-Services nicht starten.

Konfigurieren von Umgebungseigenschaften für Content Manager-Computer

Die Content Manager-Computer müssen die Position des Content Store, der anderen Content Manager-Computer und der Datenbank kennen, die für die Benachrichtigung verwendet wird.

Nachdem Sie Content Manager auf den Computern installiert haben, die dem Ausfallschutz dienen, müssen Sie Content Manager auf diesen Computern konfigurieren. Wenn Sie mehrere Content Manager installiert haben, müssen auf allen Content Manager-Computern alle Content Manager-URIs angegeben werden.

Nachdem Sie die erforderlichen Konfigurationsaufgaben durchgeführt und den IBM Cognos Analytics-Service gestartet haben, kann der Zertifizierungsstellenservice Zertifikate für andere Computer ausstellen. Sie können nun die erforderlichen Konfigurationsaufgaben auf anderen Computern ausführen, wie zum Beispiel auf Computern mit Komponenten der Anwendungsebene und Gateway-Computern. Andernfalls können Sie mit der Konfiguration der Content Manager-Computer fortfahren, indem Sie die Einstellungen für die Standardeigenschaften an Ihre Umgebung anpassen (siehe „Ändern der Standardkonfigurationseinstellungen” auf Seite 171). Sie können zum Beispiel IBM Cognos Analytics-Komponenten für die Verwendung eines Authentifizierungsproviders konfigurieren (siehe Kapitel 13, „Konfigurieren von Authentifizierungsprovidern ”, auf Seite 257), auf den Content Manager-Computern Services aktivieren und inaktivieren (siehe „Aktivieren und inaktivieren von Services” auf Seite 183) oder globale Einstellungen ändern (siehe „Ändern globaler Einstellungen” auf Seite 235).

Hinweis: Wenn Sie globale Einstellungen auf einem Content Manager-Computer ändern, müssen die gleichen Änderungen auch auf den anderen Content Manager-Computern vorgenommen werden.

Konfigurieren des aktiven Content Manager

Den Content Manager-Computern muss die Speicherposition des Content Store, der anderen Content Manager-Computer und der Datenbank bekannt sein, die für die Benachrichtigung verwendet wird.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Content Manager-Computer, den Sie als standardmäßig aktiven Content Manager definieren möchten.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Klicken Sie im Fenster **Eigenschaften** auf den Wert für **Content Manager-URIs** und anschließend auf die Schaltfläche **Bearbeiten**.
4. Geben Sie die URIs für die anderen Content Manager-Computer an:
   - Klicken Sie im Dialogfeld **Content Manager-URIs** auf **Hinzufügen**.
   - Klicken Sie in die leere Tabellenzeile und geben Sie den vollständigen URI des Content Manager-Computers ein.

Löschen Sie den ersten Tabellenwert nicht. Dieser Wert identifiziert den lokalen Content Manager-Computer und ist erforderlich.

Ersetzen Sie die localhost-Komponente des URI mit einem Hostnamen oder einer IP-Adresse. Alle URI-Eigenschaften müssen dasselbe Format verwenden, also einheitlich nur Hostnamen oder nur IP-Adressen.

- Wiederholen Sie die beiden vorherigen Schritte für jeden hinzuzufügenden URI.

  Sie müssen alle Content Manager-URIs in die Liste aufnehmen.
- Klicken Sie auf **OK**.

5. Klicken Sie im Menü **Datei** auf **Speichern**.

Konfigurieren von Content Manager-Standby-Computern

Den Content Manager-Computern muss die Speicherposition des Content Store, der anderen Content Manager-Computer und der Datenbank bekannt sein, die für die Benachrichtigung verwendet wird.

Vorgehensweise

1. Stellen Sie sicher, dass Sie die Umgebungseigenschaften bereits auf mindestens einem Content Manager-Computer konfiguriert haben und dass IBM Cognos Analytics-Komponenten auf diesem Computer ausgeführt werden.
2. Starten Sie IBM Cognos Configuration auf dem Content Manager-Standby-Computer.
3. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
4. Klicken Sie im Fenster **Eigenschaften** auf den Wert für **Content Manager-URIs** und anschließend auf die Schaltfläche **Bearbeiten**.
5. Geben Sie die URIs für die anderen Content Manager-Computer an:
   - Klicken Sie im Dialogfeld **Content Manager-URIs** auf **Hinzufügen**.
   - Klicken Sie in die leere Tabellenzeile und geben Sie den vollständigen URI des Content Manager-Computers ein.

     Löschen Sie den ersten Tabellenwert nicht. Dieser Wert identifiziert den lokalen Content Manager-Computer und ist erforderlich.

     Ersetzen Sie die localhost-Komponente des URI mit einem Hostnamen oder einer IP-Adresse. Alle URI-Eigenschaften müssen dasselbe Format verwenden, also einheitlich nur Hostnamen oder nur IP-Adressen.
   - Wiederholen Sie die beiden vorherigen Schritte für jeden hinzuzufügenden URI.

     Sie müssen alle Content Manager-URIs in die Liste aufnehmen.
   - Klicken Sie auf **OK**.
6. Klicken Sie im Fenster **Explorer** unter **Sicherheit** > **Verschlüsselung** auf den standardmäßigen Verschlüsselungsprovider **Cognos**.
7. Stellen Sie sicher, dass alle kryptografischen Einstellungen mit der Konfiguration des standardmäßig aktiven Content Manager-Computers übereinstimmen.
8. Klicken Sie im Fenster **Explorer** unter **Datenzugriff** > **Content Manager** auf **Content Store**.
9. Stellen Sie sicher, dass die Werte aller Eigenschaften den Werten entsprechen, die Sie auf dem standardmäßig aktiven Content Manager-Computer konfiguriert haben.
10. Klicken Sie im Menü **Datei** auf **Speichern**.

Angeben einer Verbindung zu einem E-Mail-Server

Wenn Sie Cognos Analytics-Inhalte per E-Mail versenden möchten, müssen Sie eine Verbindung zu Ihrem E-Mail-Server konfigurieren.

Vorgehensweise

1. Klicken Sie im Fenster **Explorer** unter **Datenzugriff** auf **Benachrichtigung**.
2. Geben Sie im Fenster **Eigenschaften** für die Eigenschaft **SMTP-Mail-Server** den Hostnamen und den Port Ihres SMTP-E-Mail-Servers (ausgehend) ein.

   Damit Sie per E-Mail gesendete Inhalte öffnen können, müssen Sie den Hostnamen im **Gateway-URI** von 'localhost' in die IP-Adresse oder den Namen des Computers ändern. Andernfalls enthält die URL in der E-Mail die Komponente 'localhost' und Remotebenutzer können die Inhalte nicht öffnen.

   Damit als Verknüpfung gesendete Inhalte geöffnet werden können, müssen Sie sicherstellen, dass der **Gateway-URI** auf Berichts- und Benachrichtigungsservern einen Web-Server mit IBM Cognos-Inhalten angibt, auf den zugegriffen werden kann. Wenn mobile Benutzer über eine Fernverbindung auf Verknüpfungen zugreifen, sollte ein externer URI in Betracht gezogen werden.
3. Klicken Sie auf das Feld **Wert** neben der Eigenschaft **Benutzerkonto und Kennwort** und klicken Sie anschließend auf die Schaltfläche zum Bearbeiten, wenn Sie angezeigt wird.
4. Geben Sie die entsprechenden Werte in das Dialogfeld **Wert - Benutzerkonto und Kennwort** ein und klicken Sie anschließend auf **OK**.

   Wenn für den SMTP-Server keine Anmeldeberechtigungsnachweise erforderlich sind, entfernen Sie die Standardinformationen für die Eigenschaft **Benutzerkonto und Kennwort**. Wenn Sie dazu aufgefordert werden, zu bestätigen, dass diese Eigenschaft leer bleiben soll, klicken Sie auf **OK**. Stellen Sie sicher, dass der Standardbenutzername entfernt wurde. Ist dies nicht der Fall, wird das Standardkonto verwendet und Benachrichtigungen funktionieren nicht ordnungsgemäß.
5. Geben Sie im Fenster **Eigenschaften** die entsprechenden Werte für das Standardabsenderkonto ein.
6. Klicken Sie im Fenster **Explorer** mit der rechten Maustaste auf **Benachrichtigung** und klicken Sie dann auf **Test**.

   IBM Cognos Analytics testet die E-Mail-Server-Verbindung.

Aktivieren einer sicheren TLS-Verbindung zum E-Mail-Server

Sie können eine sichere TLS-Verbindung zum E-Mail-Server aktivieren, um die verschlüsselte TLS-Kommunikation zu ermöglichen.

Wenn die SSL-Verschlüsselung konfiguriert, jedoch keine sichere TLS-Verbindung aktiviert ist, schlägt die Verbindung fehl und die folgende Nachricht wird angezeigt: `502 Unbekannter Befehl`.

Vorbereitende Schritte

Ein für den E-Mail-Server einheitliches Zertifikat, normalerweise im .crt-Format, ist erforderlich.

Vorgehensweise

1. Importieren Sie das Zertifikat in den JRE-Keystore, um eine Vertrauensbeziehung zwischen Cognos Analytics und dem E-Mail-Server zu ermöglichen.
   - Geben Sie unter Windows *Installationsposition*`\bin\DLS_SSL_CertImportTool.bat` *Zertifikatsposition*`\`*E-Mail-Zertifikat*`.crt -p` *Keystore-Kennwort* ein.
   - Geben Sie unter UNIX oder Linux *Installationsposition*`/bin/DLS_SSL_CertImportTool.sh` *Zertifikatsposition*`/email_certificate.crt -p` *Keystore-Kennwort* ein.
2. Wählen Sie in Cognos Configuration **Datenzugriff** > **Benachrichtigung** aus und bearbeiten Sie die Eigenschaften wie folgt:

   SMTP-E-Mail-Server
   Legen Sie den Wert für *E-Mail-Servername*:*Portnummer* fest. Dabei stellt *Portnummer* einen Port dar, der für TLS/SSL oder STARTTLS aktiviert ist.

   Konto und Kennwort
   Legen Sie eine Benutzer-ID und ein Kennwort fest, falls eine Authentifizierung beim E-Mail-Server erforderlich ist.

Standardabsender
Legen Sie das E-Mail-Konto fest, über das E-Mails vom E-Mail-Server gesendet werden.

SSL-Verschlüsselung aktiviert
Setzen Sie den Wert auf "True".

3. Wählen Sie in Cognos Configuration **Lokale Konfiguration** aus.
   a) Klicken Sie auf das Feld **Wert** für **Erweiterte Eigenschaften**.
   b) Klicken Sie auf das Stiftsymbol .
   c) Klicken Sie auf **Hinzufügen**.
   d) Geben Sie im Feld **Name** `emf.mail.tls.enabled` ein.
   e) Geben Sie im Feld **Wert** `true` ein.
   f) Klicken Sie auf **OK**.
4. Konfigurieren Sie in Cognos Administration für die erweiterte Einstellung `emf.mail.tls.enabled` den Wert `true`. Weitere Informationen finden Sie in *Konfigurieren erweiterter Einstellungen für bestimmte Services*.

   Anmerkung: Sie müssen den Zustellungsservice neu starten, nachdem Sie diese Änderung vorgenommen haben.

Aktivieren der Sicherheit

Standardmäßig ist der anonyme Zugriff in IBM Cognos Analytics möglich. Wenn Sie in Ihrer IBM Cognos Analytics-Umgebung Sicherheitsfunktionen verwenden möchten, müssen Sie den anonymen Zugriff inaktivieren und IBM Cognos Analytics für die Verwendung eines Authentifizierungsproviders konfigurieren.

Vorgehensweise

1. Klicken Sie in IBM Cognos Configuration im Fenster **Explorer** auf **Sicherheit** >**Authentifizierung** > **Cognos**.
2. Klicken Sie auf das Feld **Wert**, um **Anonymen Zugriff zulassen** aufzurufen, und wählen Sie **Falsch**.
3. Klicken Sie mit der rechten Maustaste auf **Authentifizierung** und wählen Sie **Neue Ressource** > **Namespace**.
4. Geben Sie im Feld **Name** einen Namen für den Authentifizierungs-Namespace ein.
5. Klicken Sie in der Liste **Typ** auf den entsprechenden Namespace-Typ und anschließend auf **OK**.

   Die neue Authentifizierungsprovider-Ressource wird im Fenster **Explorer** unter der Komponente **Authentifizierung** angezeigt.
6. Geben Sie im Fenster **Eigenschaften** für die Eigenschaft **Namespace-Kennung** eine eindeutige Kennung für den Namespace ein.
7. Klicken Sie im Menü **Datei** auf **Speichern**.

Starten von Content Manager

Nach dem Festlegen der Datenbankverbindungseigenschaften für den Content Store und dem Konfigurieren des Sicherheitsnamespace können Sie den Content Manager-Computer starten.

Vorbereitende Schritte

Vergewissern Sie sich, dass ein Benutzerkonto oder Servicekonto eingerichtet ist. Weitere Informationen finden Sie in „Konfigurieren eines Benutzer- oder Netzservicekontos für IBM Cognos Analytics” auf Seite 12.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.

Wenn Sie eine aktuellere Version installieren, wird eine Nachricht angezeigt, die angibt, dass Konfigurationsdateien gefunden und auf die neue Version aktualisiert wurden.

2. Stellen Sie sicher, dass Sie Ihre Konfiguration speichern. Andernfalls können Sie den IBM Cognos-Service nicht starten.
3. Klicken Sie im Menü **Aktionen** auf **Test**.

   IBM Cognos Configuration überprüft die CSK-Verfügbarkeit (Common Symmetric Keys), testet die Namespace-Konfiguration sowie die Verbindungen mit dem Content Store und anderen Ressourcen.

   Tipp: Wenn **Test** nicht zur Auswahl steht, klicken Sie im Fenster **Explorer** auf **Lokale Konfiguration**.
4. Wenn der Test fehlschlägt, müssen Sie die entsprechenden Eigenschaften neu konfigurieren und den Test wiederholen.

   Sie können einige Komponenten einzeln testen, indem Sie im Fenster **Explorer** mit der rechten Maustaste auf die Komponente klicken und **Test** auswählen.

   Starten Sie den Service erst, wenn alle Tests fehlerfrei sind.
5. Klicken Sie im Menü **Aktionen** auf **Starten**.

   Es kann einige Minuten dauern, bis der IBM Cognos-Service gestartet wird.

   Die Aktion startet alle installierten Services, die nicht ausgeführt werden, und registriert den IBM Cognos-Service unter Windows.

Testen der Content Manager-Installation

Sie können die Installation mithilfe eines Web-Browsers testen.

Vorgehensweise

1. Öffnen Sie einen Web-Browser.
2. Testen Sie, ob Content Manager ausgeführt wird, indem Sie die URI des aktiven Content Manager eingeben.
   Beispiel: `http://Hostname:Port/p2pd/servlet`

   Der Standardwert für *Hostname:Port* lautet "localhost:9300".

   Content Manager ist verfügbar, wenn der Statuswert **Running** (Aktiv) oder **Standby** lautet.

Installieren und Konfigurieren der Anwendungsservices

Sie können die Anwendungsservicekomponenten auf einem oder auf mehreren Computern installieren.

Installieren der Anwendungsservicekomponenten

Stellen Sie sicher, dass der aktive Content Manager-Computer konfiguriert und verfügbar ist, bevor Sie die Computer mit den Anwendungsservicekomponenten konfigurieren.

Wenn Sie ein Upgrade durchführen, verwendet IBM Cognos Analytics die vorhandenen Konfigurationsdaten für die Computer mit den Anwendungsservicekomponenten. Wenn Sie jedoch die Anwendungsservicekomponenten an einer neuen Position installiert haben, müssen Sie die Umgebungseigenschaften konfigurieren.

64-Bit-Installationen

Die Berichtsserverkomponente, die in die Anwendungsservicekomponenten integriert ist, wird sowohl in der 32- als auch in der 64-Bit-Version bereitgestellt. Die Auswahl der von Ihnen verwendeten Version wird nach der Installation mithilfe von IBM Cognos Configuration vorgenommen. Standardmäßig wird für die Berichtsserverkomponente die Verwendung des 32-Bit-Modus festgelegt, auch auf einem 64-Bit-Computer. Mit dem 32-Bit-Modus können Sie alle Berichte ausführen, wohingegen Sie mit dem 64-Bit-Modus lediglich Berichte ausführen können, die für den dynamischen Abfragemodus erstellt wurden.

Druckeranforderungen

Um sicherzustellen, dass Berichte unter dem Betriebssystem Microsoft Windows ordnungsgemäß ausgedruckt werden, müssen Sie aufgrund der Anforderungen von Adobe Reader mindestens einen Drucker auf dem Betriebssystem konfigurieren, auf dem die Anwendungsservicekomponenten installiert sind. Alle Berichte werden unabhängig vom Druckformat, das Sie auswählen, zum Ausdrucken als temporäre PDF-Dateien an Adobe Reader gesendet.

Installieren der Anwendungsservicekomponenten unter UNIX oder Linux

Sie können die Anwendungsservicekomponenten abhängig von Ihrer Umgebung auf einem oder mehreren Computern installieren.

Vorbereitende Schritte

Rufen Sie die Webseite IBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235) auf um zu überprüfen, ob die erforderlichen Patches auf Ihrem Computer installiert sind.

Vorgehensweise

1. Wechseln Sie an die Speicherposition, an der die Installationsdateien heruntergeladen und extrahiert wurden.

   Tipp: Verwenden Sie neue Versionen von Dateikomprimierungssoftware zum Extrahieren der Dateien. Mit älteren Versionen solcher Software können die Dateien möglicherweise nicht extrahiert werden.
2. Wechseln Sie zum Starten des Installationsassistenten in das Betriebssystemverzeichnis und geben Sie Folgendes ein: `./ca_srv_<platform>_<build>.bin`

   Tipp: Bei Verwendung des Befehls `ca_srv_<platform>_<build>.bin` mit XWindows werden japanische Zeichen in Nachrichten und Protokolldateien möglicherweise fehlerhaft angezeigt. Bei einer Installation der japanischen Version unter UNIX oder Linux müssen Sie zunächst die Umgebungsvariablen LANG=C und LC_ALL=C festlegen (wobei C für den Sprachcode steht, z. B. ja_JP.PCK unter Solaris) und dann den Installationsassistenten starten.

   Wenn Sie nicht mit XWindows arbeiten, führen Sie eine unbeaufsichtigte Installation durch. Weitere Informationen finden Sie im Installationshandbuch.
3. Folgen Sie den Anweisungen im Installationsassistenten, um die Dateien auf Ihren Computer zu kopieren.
   - Beachten Sie beim Auswählen des Verzeichnisses Folgendes:

     Installieren Sie die Anwendungsservicekomponenten in einem Verzeichnis, dessen Pfadname ausschließlich aus ASCII-Zeichen besteht. Einige UNIX- und Linux-Web-Server unterstützen nur ASCII-Zeichen in Verzeichnisnamen.
   - Nehmen Sie beim Auswählen der Komponenten die Auswahl für alle Komponenten mit Ausnahme der **Anwendungsservices** zurück.
4. Klicken Sie auf **Fertigstellen**.

   Sie sollten IBM Cognos Analytics nicht sofort konfigurieren, da Sie zunächst andere Aufgaben ausführen müssen, um sicherzustellen, dass Ihre Umgebung ordnungsgemäß eingerichtet ist.

Nächste Schritte

Konfigurieren Sie IBM Cognos Analytics mithilfe von IBM Cognos Configuration. Öffnen Sie dieses Tool, indem Sie `cogconfig.sh` im Verzeichnis *`Installationsposition`*`/bin64` eingeben.

Installieren der Anwendungsservicekomponenten unter Windows

Sie können die Anwendungsservicekomponenten abhängig von Ihrer Umgebung auf einem oder mehreren Computern installieren.

Bei Windows-Computern ist die Standardinstallationsposition das Verzeichnis **Programme**. Wenn Sie die Installation an dieser Position durchführen, müssen Sie sicherstellen, dass Sie IBM Cognos Configuration als Administrator ausführen. Alternativ können Sie das Produkt außerhalb des Verzeichnisses **Programme** installieren, z. B. im Verzeichnis `C:\IBM\cognos\analytics`.

Vorgehensweise

1. Wechseln Sie zu der Position, an der die Installationsdateien heruntergeladen und extrahiert wurden, und klicken Sie doppelt auf die Datei `ca_srv_<platform>_<build>.exe`.

   Tipp: Verwenden Sie neue Versionen von Dateikomprimierungssoftware zum Extrahieren der Dateien. Mit älteren Versionen solcher Software können die Dateien möglicherweise nicht extrahiert werden.
2. Wählen Sie die für die Installation zu verwendende Sprache aus.

   Die von Ihnen ausgewählte Sprache bestimmt die Sprache der Benutzeroberfläche. Es werden alle unterstützten Sprachen installiert. Die Sprache der Benutzeroberfläche kann nach der Installation in eine der installierten Sprachen geändert werden.
3. Wählen Sie die Installationsoption **Angepasst** aus und folgen Sie den Anweisungen im Installationsassistenten, um die Dateien auf Ihren Computer zu kopieren.
   - Beachten Sie beim Auswählen des Verzeichnisses Folgendes:

     Installieren Sie die Anwendungsservicekomponenten in einem Verzeichnis, dessen Pfadname ausschließlich aus ASCII-Zeichen besteht. Einige Web-Server unterstützen in Verzeichnisnamen nur ASCII-Zeichen.
   - Nehmen Sie beim Auswählen der Komponenten die Auswahl für alle Komponenten mit Ausnahme der **Anwendungsservices** zurück.
4. Klicken Sie auf **Fertigstellen**.

Nächste Schritte

IBM Cognos Configuration kann über die Verknüpfung **IBM Cognos Configuration** im Menü **Start** gestartet werden.

Einrichten der Datenbankverbindung für die Berichtsdatenbanken

Zur Unterstützung der Kommunikation zwischen IBM Cognos Analytics und den Datenquellen müssen Sie auf dem Computer, auf dem sich der Berichtsserver befindet, zusätzliche Software für Ihre Datenquellen installieren. Je nach Datenquelle und Abfragemodus kann die erforderliche Software Datenbankclients oder JDBC-Treiberdateien (JDBC - Java Database Connectivity) oder beides enthalten.

Bei IBM Cognos Analytics wird auf die Abfragedatenbank (auch Berichtsdatenbank genannt) nur über die Berichtsengine zugegriffen, die Berichte ausführt. Die Berichtsengine wird zusammen mit Komponenten der Anwendungsebene installiert und auch von Framework Manager und IBM Cognos Transformer verwendet.

Kompatibler Abfragemodus

Um Berichte auszuführen, die den kompatiblen Abfragemodus verwenden, müssen Sie 32-Bit-Datenquellen-Clientbibliotheken verwenden und den Berichtsserver so konfigurieren, dass er im 32-Bit-Modus arbeitet. Der kompatible Abfragemodus verwendet native Client- und ODBC-Verbindungen, um mit den Datenquellen zu kommunizieren.

Dynamischer Abfragemodus

Der dynamische Abfragemodus ermöglicht die Kommunikation mit Datenquellen über Java/XMLA-Verbindungen.

Für unterstützte relationale Datenbanken ist eine JDBC-Verbindung vom Typ 4 erforderlich. JDBC-Treiber vom Typ 4 konvertieren JDBC-Aufrufe direkt in das anbieterspezifische Datenbankprotokoll. Dies erfolgt in reinem Java und ist plattformunabhängig.

Für unterstützte OLAP-Datenquellen optimiert die Java/XMLA-Konnektivität den Zugriff. Durch die Bereitstellung von benutzerdefinierten und erweiterten MDX-Abfragen (Multidimensional Expression) für die spezifische Quelle und Version Ihrer OLAP-Technologie werden alle Möglichkeiten der OLAP-Datenquelle ausgeschöpft.

Eine aktuelle Liste der Umgebungen, die von den IBM Cognos Analytics Produkten unterstützt werden, einschließlich Informationen zu Betriebssystemen, Patches, Browsern, Webservern, Verzeichnisservern, Datenbankservern und Anwendungsservern, finden Sie auf der Seite IBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235).

Zugreifen auf OLAP-Datenquellen unter Windows-Betriebssystemen

Um auf die relationalen Datenbanken und OLAP-Datenquellen für die Berichterstellung zugreifen zu können, müssen Sie die von Ihrem Datenquellenanbieter zur Verfügung gestellte Client-API-Software installieren. Die Software muss auf demselben Computer installiert werden, auf dem auch die Komponenten der Anwendungsebene installiert sind.

Vorgehensweise

1. Installieren Sie die Datenbank-API-Software für die relationalen Datenbanken und OLAP-Datenquellen auf dem Computer, auf dem sich der Berichtsserver befindet (auf dem die Komponenten der Anwendungsebene installiert sind).

   Unter Microsoft Windows unterstützt die Berichtsengine entweder native Datenbankverbindungen oder ODBC.
2. Falls Framework Manager unter einer anderen Position als die Komponenten der Anwendungsebene installiert ist, müssen Sie die Client-API-Software auf demselben Computer wie Framework Manager installieren.

   Weitere Informationen finden Sie im Abschnitt „Festlegen von Variablen für Datenquellenverbindungen für Framework Manager” auf Seite 155.

Zugreifen auf ODBC-Datenquellen unter UNIX- oder Linux-Betriebssystemen

Zur Verwendung einer ODBC-Datenquelle unter UNIX oder Linux zur Herstellung einer Verbindung zu einer unterstützten Datenquelle müssen Sie die Umgebung so konfigurieren, dass die Datei `.odbc.ini` gesucht wird, die die Verweise auf die Datenquelle, die Konnektivitätsbibliotheken und die zugehörigen Treibermanagerbibliotheken enthält.

Informationen zu unterstützten ODBC-Datenquellen finden Sie in IBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235).

Nachdem Sie die ODBC-Verbindungen konfiguriert haben, müssen Sie Verbindungen zu Datenquellen in IBM Cognos Administration erstellen. Weitere Informationen finden Sie im Handbuch *IBM CognosVerwaltung und Sicherheit*.

Wenn Ihr Datenbankanbieter keinen Treibermanager bereitstellt, können Sie abhängig vom verwendeten Betriebssystem 'unixODBC' oder 'iODBC' verwenden.

Unter Linux-Betriebssystemen enthält das unixODBC-Package, das zusammen mit dem Betriebssystem geliefert wird, den ODBC-Treibermanager. Sie müssen unixODBC Version 2.2.11 oder eine spätere Version des Produkts installieren, bevor Sie Datenquellenverbindungen einrichten können. Um die installierte Version zu überprüfen, verwenden Sie den folgenden Befehl: `odbcinst --version`. Überprüfen Sie, welche Version von 'unixODBC' für die verwendete Datenbank erforderlich ist, und stellen Sie sicher, dass Sie diese Version verwenden.

Unter UNIX-Betriebssystemen wird der Open-Source-Treibermanager 'iODBC' als Teil der IBM Cognos-Installation bereitgestellt.

Vorgehensweise

1. Erstellen Sie eine Umgebungsvariable, um die Position der Datei `.odbc.ini` anzugeben.

   Zum Beispiel

   ```
   export ODBCINI=/usr/local/etc/.odbc.ini
   ```

2. Geben Sie für die entsprechende Bibliothekspfad-Umgebungsvariable die Position der 32-Bit-Konnektivitätsbibliotheken und des Treibermanagers für Ihre Datenbank an.

   Die folgende Tabelle enthält die Umgebungsvariablen für alle Betriebssysteme, die die Position der Treibermanagerbibliotheken enthalten müssen.

Tabelle 17. Umgebungsvariablen für Ihr Betriebssystem

Betriebssystem	**Umgebungsvariable**
AIX	LIBPATH
Linux	LD_LIBRARY_PATH

3. Wenn Ihr Datenbankanbieter keinen Treibermanager bereitstellt, können Sie den Bibliothekspfad so einstellen, dass er den Pfad zum lokalen Treibermanager enthält.

   - Unter UNIX wird iODBC als Teil der IBM Cognos-Installation bereitgestellt. Die Bibliotheksdateien befinden sich im Verzeichnis *installationsposition*`/bin`. Ihr Bibliothekspfad sollte bereits das Verzeichnis *installationsposition*`/bin` enthalten.

     Zum Beispiel

     ```
     LIBPATH=/usr/IBM/cognos/bin:$LIBPATH
     ```

   - Unter Linux enthält das unixODBC-Package die erforderlichen Treibermanagerbibliotheken.

     Zum Beispiel

     ```
     LD_LIBRARY_PATH=/usr/lib:$LD_LIBRARY_PATH
     ```

Nächste Schritte

Wenn Sie unter UNIX- oder Linux-Betriebssystemen mehrere ODBC-Quellen verwenden, dann werden Sie möglicherweise Abhängigkeiten von Bibliotheksdateien mit allgemeinen Namen, jedoch unterschiedlichen Implementierungen für die Konnektivität und den Treibermanager feststellen. In einem Szenario, in dem eine ODBC-Quelle gültig ist, eine andere aufgrund einer Abhängigkeit jedoch nicht, sollten Sie sich an die Kundenunterstützung wenden. Wenn Sie eine allgemeine `.odbc.ini`-Datei verwenden, kann dies zu nicht kompatiblen Einträgen für unterschiedliche Treibermanager führen. Um dieses Problem zu beheben, sollten Sie die Strukturanforderungen zwischen den Treibermanagern überprüfen, die von Ihnen verwendet werden, und versuchen, eine Syntax zu verwenden, die für die betroffenen Treibermanager gilt.

Konfigurieren von IBM Cognos Analytics für die Verwendung von Oracle Essbase

Wenn Sie IBM Cognos Analytics mit einer Oracle Essbase-Datenquelle der Version 11.1.1 verwenden, müssen Sie eine Konfigurationsdatei bearbeiten, um dem IBM Cognos Analytics-Server Ihre Version mitzuteilen.

Standardmäßig wird IBM Cognos Analytics für die Verwendung von Oracle Essbase Version 11.1.2 konfiguriert. Deshalb ist keine Konfiguration erforderlich, wenn Sie diese Version verwenden. Wenn Sie jedoch eine andere unterstützte Version von Oracle Essbase verwenden, müssen Sie die Datei 'qfs.config.xml' für Ihre Version entsprechend bearbeiten.

Außerdem müssen Sie bei der Verwendung von Oracle Essbase Version 11.1.2 Oracle Foundation Services sowie den Oracle Essbase-Client installieren.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *Installationsposition*/configuration.
2. Öffnen Sie die Datei 'qfs_config.xml' in einem XML-Editor oder in einem Texteditor.
3. Suchen Sie nach den folgenden Zeilen:

```
<!--provider name="DB2OlapODP" libraryName="essodp111" connectionCode="DO"-->
<provider name="DB2OlapODP" libraryName="essodp1112" connectionCode="DO">
```

4. Ändern Sie sie für Oracle Essbase 11.1.1 wie folgt:

```
<provider name="DB2OlapODP" libraryName="essodp111" connectionCode="DO">
<!--provider name="DB2OlapODP" libraryName="essodp1112" connectionCode="DO"-->
```

5. Stellen Sie für Oracle Essbase 11.1.2 sicher, dass die Zeilen wie folgt aussehen:

```
<!--provider name="DB2OlapODP" libraryName="essodp111" connectionCode="DO"-->
<provider name="DB2OlapODP" libraryName="essodp1112" connectionCode="DO">
```

6. Speichern Sie die Datei und starten Sie den IBM Cognos-Service erneut.

Konfigurieren von Oracle Essbase auf einem UNIX- oder Microsoft Windows-64-Bit-Betriebssystem

Wenn Sie eine Oracle Essbase-Datenquelle der Version 11.1.2 mit IBM Cognos Analytics unter einem UNIX- oder Microsoft Windows-64-Bit-Betriebssystem verwenden, müssen Sie die Umgebungsvariablen **ARBORPATH** und **ESSBASEPATH** manuell konfigurieren.

Die Umgebungsvariablen **ARBORPATH** und **ESSBASEPATH** werden während der Installation des Oracle Essbase-Clients erstellt. IBM Cognos Analytics verwendet diese Variablen zum Suchen nach der Position des Oracle Essbase-Clients.

Wenn Sie Oracle Essbase mit IBM Cognos Analytics unter einem UNIX- oder einem Microsoft Windows-64-Bit-Betriebssystem verwenden möchten, müssen Sie den Oracle Essbase-64-Bit-Client installieren. Dieser 64-Bit-Client enthält einen 32-Bit-Client, der von IBM Cognos Analytics verwendet wird. Damit auf diesen 32-Bit-Client verwiesen wird, müssen Sie die Umgebungsvariablen **ARBORPATH** und **ESSBASEPATH** manuell ändern, um `EssbaseClient` durch `EssbaseClient-32` zu ersetzen. Im folgenden Beispiel wird davon ausgegangen, dass der Client auf Laufwerk C installiert ist. Ihr Installationsverzeichnis weicht eventuell davon ab.

```
ARBORPATH=C:\Hyperion\EPMSystem11R1\products\Essbase\EssbaseClient-32
```

```
ESSBASEPATH=C:\Hyperion\EPMSystem11R1\products\Essbase\EssbaseClient-32
```

Wenn Sie mit einem Microsoft Windows-32-Bit-Betriebssystem und einem Oracle Essbase-32-Bit-Client arbeiten, müssen diese Umgebungsvariablen nicht geändert werden.

Starten von IBM Cognos Configuration

Mit IBM Cognos Configuration können Sie IBM Cognos Analytics-Komponenten konfigurieren und IBM Cognos-Services starten und stoppen.

Vorbereitende Schritte

Bevor Sie IBM Cognos Configuration starten, müssen Sie sicherstellen, dass die Betriebsumgebung ordnungsgemäß eingerichtet ist. Prüfen Sie beispielsweise, ob alle Umgebungsvariablen definiert wurden.

Unter dem Microsoft Windows-Betriebssystem können Sie IBM Cognos Configuration nur von der letzten Seite des Installationsassistenten aus starten, wenn keine zusätzlichen Einrichtungsschritte erforderlich sind. Wenn Sie beispielsweise einen anderen Datenbankserver als Microsoft SQL für den Content Store verwenden, kopieren Sie die JDBC-Treiber (Java Database Connectivity) vor dem Starten des Konfigurationstools in den Ordner *installationsposition*/drivers.

Starten Sie unter UNIX- oder Linux-Betriebssystemen IBM Cognos Configuration nicht von der letzten Seite des Installationsassistenten aus. Bevor Sie IBM Cognos Analytics konfigurieren können, sind zusätzliche Einrichtungsschritte erforderlich. Beispielweise müssen Sie die Java-Umgebung aktualisieren.

Vergewissern Sie sich, dass ein Benutzerkonto oder ein Servicekonto für die Ausführung von IBM Cognos eingerichtet ist.

Lesen Sie „Kritische Konfigurationsaktionen, die zuerst erledigt werden müssen!" auf Seite 102.

Vorgehensweise

1. Klicken Sie unter Microsoft Windows auf **Start** > **IBM Cognos Configuration**.

   Wenn Sie einen Windows-Computer verwenden und das Produkt im Verzeichnis `Programme (x86)` installiert haben, starten Sie IBM Cognos Configuration als Administrator.
2. Wechseln Sie unter UNIX oder Linux in das Verzeichnis *`installationsposition`*`/bin` und geben Sie den folgenden Befehl ein:

   `./cogconfig.sh`

   Wenn IBM Cognos Configuration nicht geöffnet wird, stellen Sie sicher, dass Sie die Umgebungsvariable DISPLAY angegeben haben.

   Wenn eine Nachricht des Typs `JAVA.Lang.unsatisfied link` angezeigt wird, vergewissern Sie sich, dass Sie eine unterstützte Java-Version verwenden.

   Wenn eine Nachricht des Typs `Java.lang.unsupportedClassVersionError` angezeigt wird, vergewissern Sie sich, dass Sie die 64-Bit-Version von Java verwenden.

Konfigurieren von Umgebungseigenschaften für Computer mit Anwendungsservicekomponente

Wenn Sie die Anwendungsservicekomponente auf einem anderen Computer als Content Manager installieren, müssen Sie den Computer mit den Anwendungsservicekomponenten so konfigurieren, dass er den Pfad zu Content Manager kennt. Die verteilten Komponenten können dann miteinander kommunizieren.

Dem Computer mit den Anwendungsservicekomponenten muss die Speicherposition der Content Manager-Computer und der Benachrichtigungsdatenbank mit den Job- und Zeitplaninformationen bekannt sein. Der Computer mit den Anwendungsservicekomponenten muss dieselbe Benachrichtigungsdatenbank wie der Content Manager-Computer verwenden. Weitere Informationen finden Sie im Abschnitt „Ändern der Benachrichtigungsdatenbank" auf Seite 199.

Wenn Sie mehrere Content Manager installiert haben, müssen Sie alle Content Manager-URIs auf jedem Computer mit den Anwendungsservicekomponenten auflisten.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Ändern Sie im Fenster **Eigenschaften** den Bestandteil **localhost** der Eigenschaft **Content Manager-URIs** in den Namen eines Content Manager-Computers.
4. Geben Sie die URIs für die anderen Content Manager-Computer an:
   - Klicken Sie im Dialogfeld **Content Manager-URIs** auf **Hinzufügen**.
   - Klicken Sie in die leere Tabellenzeile und geben Sie den vollständigen URI des Content Manager-Computers ein.

     Ersetzen Sie die localhost-Komponente des URI mit einem Hostnamen oder einer IP-Adresse. Alle URI-Eigenschaften müssen dasselbe Format verwenden, also einheitlich nur Hostnamen oder nur IP-Adressen.
   - Wiederholen Sie die beiden vorherigen Schritte für jeden hinzuzufügenden URI.

Sie müssen alle Content Manager-URIs in die Liste aufnehmen.

- Klicken Sie auf **OK**.

5. Ändern Sie den Bestandteil **localhost** der Eigenschaft **Gateway-URI** in den Namen des Computers, auf dem die Gateway-Komponente installiert werden soll.

   Dadurch wird sichergestellt, dass Benutzer an unterschiedlichen Orten auf Berichte und Arbeitsbereiche zugreifen können, die per E-Mail gesendet werden.
6. Ändern Sie den Teil **localhost** der übrigen URI-Eigenschaften in den Namen oder die IP-Adresse Ihres IBM Cognos Analytics-Servers.
7. Klicken Sie im Fenster **Explorer** unter **Sicherheit** > **Verschlüsselung** auf den standardmäßigen Verschlüsselungsprovider **Cognos**.
8. Stellen Sie in der Eigenschaftengruppe **Einstellungen für Zertifizierungsstelle** für die Eigenschaft **Kennwort** den gleichen Wert ein, der auf dem standardmäßig aktiven Content Manager-Computer konfiguriert ist.
9. Stellen Sie sicher, dass alle anderen kryptografischen Einstellungen den Einstellungen entsprechen, die Sie auf dem standardmäßig aktiven Content Manager-Computer festgelegt haben.
10. Klicken Sie im Menü **Datei** auf **Speichern**.

Aktivieren der 64-Bit-Version des Berichtsservers

Sie können wählen, ob eine 32-Bit- oder eine 64-Bit-Version der Berichtsserverkomponente verwendet werden soll. Wenn Sie die 64-Bit-Version verwenden möchten, müssen Sie sie in IBM Cognos Configuration aktivieren. Die Standardoption ist 32-Bit.

Ein 32-Bit-Berichtsserver kann sowohl mit Packages im dynamischen Abfragemodus als auch mit Packages im kompatiblen Abfragemodus verwendet werden. Ein 64-Bit-Berichtsserver kann nur mit Packages im dynamischen Abfragemodus verwendet werden.

Der Berichtsserver arbeitet mit dem Abfrageservice. Beim Abfrageservice handelt es sich um die Engine, die den dynamischen Abfragemodus und dynamische Cubes steuert. In einer 64-Bit-Installation wird die 64-Bit-Version des Abfrageservice verwendet, unabhängig davon, ob die Berichtsserverkomponente als 32-Bit- oder als 64-Bit-Version konfiguriert ist.

Durch die Verwendung der 64-Bit-Version des Berichtsservers steht zusätzlicher adressierbarer Hauptspeicher für die Wiedergabe von Berichtsausgaben zur Verfügung. So kann zum Beispiel vermieden werden, dass während der Wiedergabephase der Berichtsausführung nicht mehr ausreichend Hauptspeicher verfügbar ist. Nur für große Berichtsausgaben, z. B. PDF-Berichte mit mehr als 1000 Seiten, ist die 64-Bit-Version der Berichtsserverkomponente erforderlich.

Für Packages, für die kein dynamischer Abfragemodus aktiviert ist, muss die 32-Bit-Version des Berichtsservers verwendet werden. Basiert Ihr Package beispielsweise auf IBM Cognos PowerCubes, so müssen Sie die 32-Bit-Version des Berichtsservers verwenden.

Wenn Ihre Umgebung mehrere Instanzen der Komponenten der Anwendungsebene enthält, können Sie eine davon für den 32-Bit-Berichtsserver verwenden. Mittels Routing-Regeln können Sie dann Berichtsanforderungen für Packages ohne dynamischen Abfragemodus an die Instanz weiterleiten, in der die 32-Bit-Version des Berichtsservers ausgeführt wird. Weitere Informationen zu Routing-Regeln finden Sie im Handbuch *Verwaltung und Sicherheit*.

Zur Aktivierung der 64-Bit-Version müssen Sie die 64-Bit-Version der Komponenten der Anwendungsebene auf einem 64-Bit-Computer installieren. Wenn Sie die 32-Bit-Version der Komponenten der Anwendungsebene installieren oder mit einem 32-Bit-Computer arbeiten, dürfen Sie die 64-Bit-Version des Berichtsservers nicht aktivieren.

Vorgehensweise

1. Klicken Sie im Fenster **Explorer** von IBM Cognos Configuration auf **Umgebung**.
2. Klicken Sie auf das Feld **Wert**, um **Ausführungsmodus für Berichtsserver** aufzurufen, und wählen Sie **64-Bit** aus.

3. Klicken Sie im Menü **Datei** auf **Speichern**.
4. Wenn die IBM Cognos-Services ausgeführt werden, starten Sie sie nun neu.

Starten der Anwendungsservicekomponenten

Nach dem Konfigurieren der Umgebungseigenschaften können Sie die Services auf dem Computer mit den Anwendungsservicekomponenten starten.

Vorbereitende Schritte

Wenn Sie IBM Cognos Analytics für die Berichterstellung verwenden möchten, müssen Sie die Serverkomponenten installieren und konfigurieren, den IBM Cognos-Service starten und ein Package besitzen, das auf eine verfügbare Datenquelle verweist. Beachten Sie, dass Sie bei einer Aktualisierung weiterhin dieselben Datenquellen verwenden können.

Vergewissern Sie sich, dass ein Benutzerkonto oder Servicekonto eingerichtet ist. Weitere Informationen finden Sie in „Konfigurieren eines Benutzer- oder Netzservicekontos für IBM Cognos Analytics” auf Seite 12.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.

   Wenn Sie eine aktuellere Version installieren, wird eine Nachricht angezeigt, die angibt, dass Konfigurationsdateien gefunden und auf die neue Version aktualisiert wurden.
2. Stellen Sie sicher, dass Sie Ihre Konfiguration speichern. Andernfalls können Sie den IBM Cognos-Service nicht starten.
3. Klicken Sie im Menü **Aktionen** auf **Test**.

   IBM Cognos Configuration überprüft die CSK-Verfügbarkeit (Common Symmetric Keys), testet die Namespace-Konfiguration sowie die Verbindungen mit dem Content Store und anderen Ressourcen.

   Tipp: Wenn **Test** nicht zur Auswahl steht, klicken Sie im Fenster **Explorer** auf **Lokale Konfiguration**.
4. Wenn der Test fehlschlägt, müssen Sie die entsprechenden Eigenschaften neu konfigurieren und den Test wiederholen.

   Sie können einige Komponenten einzeln testen, indem Sie im Fenster **Explorer** mit der rechten Maustaste auf die Komponente klicken und **Test** auswählen.

   Starten Sie den Service erst, wenn alle Tests fehlerfrei sind.
5. Klicken Sie im Menü **Aktionen** auf **Starten**.

   Es kann einige Minuten dauern, bis der IBM Cognos-Service gestartet wird.

   Die Aktion startet alle installierten Services, die nicht ausgeführt werden, und registriert den IBM Cognos-Service unter Windows.

Testen der Anwendungsservicekomponenten

Sie können die Installation mit einem Web-Browser testen.

Vorgehensweise

1. Öffnen Sie einen Web-Browser.
2. Prüfen Sie die Verfügbarkeit des Dispatchers, indem Sie den Wert für **Externer Dispatcher-URI** aus IBM Cognos Configuration eingeben. Zum Beispiel

   `http://`*`Hostname:Port`*`/bi`

   Der Standardwert für *`Hostname:Port`* lautet "localhost:9300".

   Der Dispatcher ist verfügbar, wenn das Portal angezeigt wird.

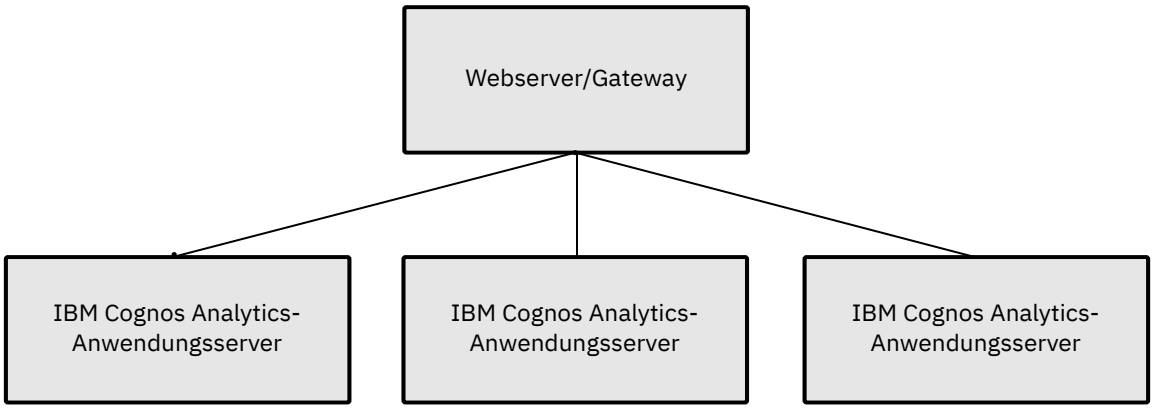
Kapitel 10. Konfigurieren des Gateways

Sie können das optionale Gateway auf einem oder mehreren Computern installieren. Installieren Sie das Gateway, wenn Sie erweiterte Optionen einrichten möchten, z. B. Single Sign-on mit Kerberos-Sicherheit mit IIS oder eine Architektur, bei der der Web-Server außerhalb einer Firewall öffentlich verfügbar ist.

IBM Cognos Analytics verwendet den Web-Server für den Lastausgleich für bestimmte Anforderungen sowie für das Hosting und Bereitstellen von statischem Inhalt wie beispielsweise Symbolen und Bilddateien.

Stellen Sie sicher, dass der Computer, auf dem Sie die aktiven Anwendungsservices installiert haben, konfiguriert und verfügbar ist, bevor Sie die Gateway-Computer konfigurieren.

Das folgende Diagramm zeigt den Gateway-Server und mehrere Cognos Analytics-Server. Bei aktiviertem Lastausgleich kann die Arbeitslast über mehrere Server verteilt werden.



Diese Konfiguration wird auch in einer Umgebung mit einer einzelnen Anwendungsebene empfohlen, da das Routing nur auf einen einzigen Server ausgerichtet wäre und die Bereitschaft bestände, bei Bedarf weitere Tier-Server hinzuzufügen.

Installieren des Cognos Analytics-Gateways

Sie können das IBM Cognos Analytics-Gateway auf einem oder mehreren Computern installieren. Wenn Sie über eine Web-Farm verfügen, können Sie ein IBM Cognos Analytics-Gateway auf jedem Web-Server installieren.

Vorbereitende Schritte

Rufen Sie die Webseite IBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235) auf um zu überprüfen, ob die erforderlichen Patches auf Ihrem Computer installiert sind.

Stellen Sie sicher, dass das temporäre Verzeichnis mindestens über 5 GB Speicherplatz verfügt.

Tipp: Das temporäre Verzeichnis wird mit der Umgebungsvariablen *IATEMPDIR* für das Betriebssystem UNIX oder Linux oder mit der Umgebungsvariablen *TMP* für das Betriebssystem Microsoft Windows festgelegt.

Vorgehensweise

1. Starten Sie den Installationsassistenten.
   a) Wechseln Sie unter UNIX oder Linux in das Betriebssystemverzeichnis und geben Sie Folgendes ein: `./ca_srv_Plattform_Build.bin`

Tipp: Bei Verwendung des Befehls `ca_srv_<platform>_<build>.bin` mit XWindows werden japanische Zeichen in Nachrichten und Protokolldateien möglicherweise fehlerhaft angezeigt. Bei einer Installation der japanischen Version unter UNIX oder Linux müssen Sie zunächst die Umgebungsvariablen LANG=C und LC_ALL=C festlegen (wobei C für den Sprachcode steht, z. B. ja_JP.PCK unter Solaris) und dann den Installationsassistenten starten.

Wenn Sie nicht mit XWindows arbeiten, führen Sie eine unbeaufsichtigte Installation durch. Weitere Informationen finden Sie im Abschnitt Kapitel 5, „Unbeaufsichtigte Installation, Deinstallation und Konfiguration", auf Seite 31.

b) Wechseln Sie unter Microsoft Windows in das Betriebssystemverzeichnis oder in das Verzeichnis, in das die Installationsdateien heruntergeladen wurden, und klicken Sie doppelt auf `ca_srv_`*`Platform_Build`*`.exe`.

2. Wählen Sie die für die Installation zu verwendende Sprache aus.

   Die von Ihnen ausgewählte Sprache bestimmt die Sprache der Benutzeroberfläche. Es werden alle unterstützten Sprachen installiert. Die Sprache der Benutzeroberfläche kann nach der Installation in eine der installierten Sprachen geändert werden.

3. Wählen Sie die Installationsoption **Angepasst** aus und folgen Sie den Anweisungen im Installationsassistenten, um die erforderlichen Dateien auf Ihren Computer zu kopieren.

   - Beachten Sie beim Auswählen des Verzeichnisses Folgendes:

     Installieren Sie Gateway-Komponenten in einem Verzeichnis, dessen Pfadname ausschließlich aus ASCII-Zeichen besteht. Einige UNIX- und Linux-Web-Server unterstützen in Verzeichnisnamen nur ASCII-Zeichen.

   - Löschen Sie beim Auswählen der Komponenten alle Komponenten außer **Gateway**.

4. Klicken Sie auf **Fertigstellen**.

Cognos Analytics mit Ihrem Web-Server konfigurieren

Sie müssen Ihren Web-Server konfigurieren, bevor Benutzer eine Verbindung zu IBM Cognos Analytics herstellen können.

Für die Berichterstellung mit IBM Cognos Analytics müssen Sie auf dem Web-Server außerdem festlegen, wann die Inhalte für das Bildverzeichnis ablaufen, damit der Web-Browser den Bildstatus nach dem ersten Zugriff nicht mehr überprüft.

Dateiberechtigungen

Das Konto, unter dem der Web-Server ausgeführt wird, muss über die Lese-, Schreib- und Ausführungsberechtigungen für das Cognos-Installationsverzeichnis verfügen. Lesezugriff ist für die Datei `cogstartup.xml` im Verzeichnis `./configuration` erforderlich. Schreibzugriff ist für `./logs` erforderlich, wenn die Tracefunktion für die Fehlerbehebung erforderlich ist. Ausführungszugriff ist für das Verzeichnis `./cgi-bin` erforderlich, damit SSO-Module für Apache HTTP Server, IBM HTTP Server oder Microsoft Internet Information Services vom Web-Server ausgeführt werden können.

Referenzwerte für die Konfigurationsprozeduren

Verweisen Sie bei Bedarf auf die folgenden Werte:

- Servername (server name): Der Hostname des Web-Servers.
- Portnummer (port #): 80 (Nicht-SSL) oder 443 (SSL)
- Name des virtuellen Verzeichnisses (virtual directory name): ibmcognos
- Cognos Analytics-Servername (Cognos Analytics server name): Der Hostname des IBM Cognos Analytics-Servers bzw. der Cognos Analytics-Server

  Wichtig: Wenn Ihre Umgebung mehr als einen Cognos Analytics-Server enthält, beziehen Sie den Server, auf dem der Content Manager-Service ausgeführt wird, nicht in die nachfolgenden Schritte ein.

Nur Cognos Analytics-Server einschließen, bei denen die Anwendungsserverkomponenten installiert und konfiguriert sind.

- Cognos Analytics-Portnummer: 9300

Einige oder alle dieser URI-Einstellungen befinden sich abhängig vom Typ der verwendeten Installation in der Cognos Configuration:

- **Gateway-URI**: Verwenden Sie für Nicht-SSL `http://`*`web_server_host_name`*`:80/ibmcognos/bi/v1/disp`. Verwenden Sie für SSL `https://`*`web_server_host_name`*`:443/ibmcognos/bi/v1/disp`

  Dies ist die URL für nicht verbundene Inhalte (Disconnected Content), wie z. B. Links in PDFs, Excel und aktiven Berichten. Sie wird auch in Links verwendet, die per E-Mail versendet werden.
- **Dispatcher-URIs für das Gateway**: `http(s)://`*`IBM_Cognos_Analytics_server_host_name`*`:9300/bi/v1/disp`

  Dies ist die Liste der URIs, zu denen das Cognos Apache-Modul oder der ISAPI-Code beim Weiterleiten von Anforderungen eine Verbindung herstellt. Für die Failover-Funktionalität stehen mehrere Einträge zur Verfügung. Beziehen Sie alle relevanten IBM Cognos Analytics-Anwendungsserver ein.
- **Dispatcher-URI für externe Anwendungen**: `http(s)://`*`IBM_Cognos_Analytics_server_host_name`*`:9300/bi/v1/disp`

  Externe Anwendungen (wie z. B. Framework Manager) stellen eine Verbindung über diese URL her, um SDK-Operationen auszuführen.

Microsoft Internet Information Services (IIS)

Ausführlichere Informationen zu IIS und Cognos Analytics finden Sie in Konfigurieren von IIS und Cognos Analytics.

Installieren Sie die Erweiterung Application Request Routing für IIS. Weitere Informationen hierzu finden Sie in https://www.iis.net/downloads/microsoft/application-request-routing. Hiermit wird auch die URL-Rewrite-Erweiterung installiert.

Die URL-Umschreibung ermöglicht es Webadministratoren, leistungsfähige Regeln zu erstellen, mit denen URLs implementiert werden können, die sich Benutzer besser merken können und die von Suchmaschinen einfacher gefunden werden. ARR (Application Request Routing, Anwendungsanforderungsrouting) ermöglicht es Web-Server-Administratoren, die Skalierbarkeit und Zuverlässigkeit von Webanwendungen zu erhöhen, indem regelbasiertes Routing, Client- und Hostnamenaffinität, Lastausgleich bei HTTP-Serveranforderungen und verteiltes Plattencaching angewendet werden.

Wenn Sie bei einem Upgrade von Cognos Analytics 11.0.3 auf Cognos Analytics 11.0.4 (oder höher) die Datei `server.xml` so geändert haben, dass ein Pfad `sso/login` konfiguriert wird, der auf `/ibmcognos/cgi-bin/cognosisapi.dll` verweist, entfernen Sie den folgenden Eintrag aus *`installationsposition`*`/wlp/usr/servers/cognosserver/server.xml`.

```
<jndiEntry jndiName="glass/sso/login" value="/ibmcognos/cgi-bin/cognosisapi.dll"/>
```

Details zur Konfiguration für Active Directory Server finden Sie in „Aktivieren der Einzelanmeldung zwischen Active Directory Server und IBM Cognos-Komponenten” auf Seite 267.

32-Bit-Web-Gateway aktivieren

Für einen 32-Bit-Web-Server müssen Sie die Dateien des 32-Bit-Gateways in Ihrem Installationsverzeichnis manuell verschieben.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *`installationsposition`*`/cgi-bin`.
2. Geben Sie den folgenden Befehl ein:

- Geben Sie unter UNIX oder Linux den Befehl `./copyGateMod.sh 32bit` ein.
- Geben Sie unter Windows den Befehl `copyGateMod.bat 32bit` ein.

Ergebnisse

Die Dateien des 32-Bit-Gateways werden aus dem Verzeichnis `cgi-bin/lib` in das Verzeichnis `cgi-bin` kopiert.

Anmerkung: Wenn Sie die Standarddateien des 64-Bit-Gateways wiederherstellen wollen, führen Sie die Prozedur mit `./copyGateMod.sh 64bit` bzw. `copyGateMod.bat 64bit` aus. Die 64-Bit-Gateway-Dateien werden aus dem Verzeichnis `cgi-bin/lib64` in das Verzeichnis `cgi-bin` kopiert.

Dispatcher-URIs konfigurieren

Wenn Sie die Gateway-Komponente auf einem anderen Computer als dem Content Manager-Computer oder dem Computer mit den Komponenten der Anwendungsebene installieren, müssen Sie den Gateway-Computer so konfigurieren, dass er den Pfad eines Dispatchers kennt. Ein Dispatcher wird auf jedem Content Manager-Computer und Computer mit Komponenten der Anwendungsebene installiert. Konfigurieren Sie das Gateway so, dass der Dispatcher auf einem Computer mit Komponenten der Anwendungsebene genutzt wird.

Als Ausfallschutz können Sie mehrere Dispatcher für einen Gateway-Computer konfigurieren. Wenn mehrere Dispatcher konfiguriert wurden, werden Anforderungen normalerweise an den ersten Dispatcher in der Liste weitergeleitet. Wenn dieser Dispatcher nicht mehr verfügbar ist, ermittelt das Gateway den nächsten funktionsbereiten Dispatcher in der Liste und leitet Anforderungen dorthin weiter. Der Status des primären Dispatchers wird vom Gateway überwacht und Anforderungen werden zurück an diese Komponente geleitet, sobald sie wieder zur Verfügung steht.

Nachdem Sie die erforderlichen Konfigurationsaufgaben ausgeführt haben, können Sie den Gateway-Computer in Ihrer Umgebung verwenden.

Vorbereitende Schritte

Stellen Sie sicher, dass die Computer, auf denen Sie Content Manager installiert haben, konfiguriert sind und der standardmäßig aktive Content Manager-Computer zur Verfügung steht, bevor Sie die Gateway-Computer konfigurieren.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
   a) Klicken Sie unter Microsoft Windows auf **Start** > **IBM Cognos Configuration**.

      Wenn Sie einen Windows 7- oder Windows 2008-Computer verwenden und das Produkt im Verzeichnis `Programme (x86)` installiert haben, starten Sie IBM Cognos Configuration als Administrator.

   b) Wechseln Sie unter UNIX oder Linux in das Verzeichnis *installationsposition*`/bin` und geben Sie den folgenden Befehl ein:

      `./cogconfig.sh`

      Wenn IBM Cognos Configuration nicht geöffnet wird, stellen Sie sicher, dass Sie die Umgebungsvariable *DISPLAY* angegeben haben.

      Wenn eine Nachricht des Typs `JAVA.Lang.unsatisfied link` angezeigt wird, vergewissern Sie sich, dass Sie eine unterstützte Java-Version verwenden.

      Wenn eine Nachricht des Typs `Java.lang.unsupportedClassVersionError` angezeigt wird, vergewissern Sie sich, dass Sie die 64-Bit-Version von Java verwenden.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.

3. Geben Sie im Fenster **Eigenschaften** unter **Gateway-Einstellungen** die Werte für **Dispatcher-URIs für das Gateway** ein:
   - Klicken Sie auf die Spalte **Wert**.
   - Klicken Sie auf die Schaltfläche **Bearbeiten**.
   - Ändern Sie den Abschnitt *localhost* der URI in den Namen oder die IP-Adresse eines Application Tier Components-Computers.

     Dadurch wird sichergestellt, dass Benutzer an unterschiedlichen Orten auf Berichte und Arbeitsbereiche zugreifen können, die per E-Mail gesendet werden.

     Tipp: Wenn Sie von einer Software Development Kit-Anwendung oder einem IBM Cognos Analytics-Modellierungstool außerhalb einer Netzfirewall Anforderungen an den Dispatcher senden möchten, stellen Sie eine Verbindung zu einem dedizierten Gateway her, das für den Verbindungsaufbau zum Dispatcher über den internen Dispatcher-URI für die Umgebung (z. B. http://localhost:9300/p2pd/servlet/dispatch) konfiguriert ist. Aus Sicherheitsgründen wird mit der Standardeinstellung der Gateway-Eigenschaft für den Dispatcher-URI verhindert, dass der Dispatcher Anforderungen von Software Development Kit-Anwendungen oder Modellierungstools außerhalb der Firewall entgegennimmt. Vergewissern Sie sich, dass für dieses dedizierte Gateway geeignete Sicherheitseinstellungen, wie SSL, konfiguriert sind (siehe „Konfigurieren des SSL-Protokolls für Cognos Analytics-Komponenten" auf Seite 208). Verwenden Sie den internen Dispatcher-URI nicht für das Hauptgateway. Dadurch würde die Sicherheit des IBM Cognos Analytics-Portals und der Studios verringert.
   - Wenn Sie eine andere URI hinzufügen möchten, klicken Sie auf **Hinzufügen** und ändern Sie den Abschnitt *localhost* der neuen URI in den Namen oder die IP-Adresse eines anderen Application Tier Components-Computers.

     Tipp: Wenn Sie den Dispatcher auf einem Content Manager-Standby-Computer verwenden möchten, stellen Sie sicher, dass Sie zuerst die Computer mit Komponenten der Anwendungsebene hinzugefügt haben, bevor Sie ihn hinzufügen. Wenn Sie den Dispatcher vom aktiven Content Manager-Computer hinzufügen, muss dieser der letzte in der Liste sein.
   - Klicken Sie nach dem Festlegen aller URIs auf **OK**.
4. Klicken Sie im Fenster **Explorer** unter **Sicherheit** > **Verschlüsselung** auf den standardmäßigen Verschlüsselungsprovider **Cognos**.
5. Stellen Sie in der Eigenschaftengruppe **Einstellungen für Zertifizierungsstelle** für die Eigenschaft **Kennwort** den gleichen Wert ein, der auf dem standardmäßig aktiven Content Manager-Computer konfiguriert ist.
6. Stellen Sie sicher, dass alle anderen kryptografischen Einstellungen den Einstellungen entsprechen, die Sie auf dem standardmäßig aktiven Content Manager-Computer festgelegt haben.
7. Testen Sie, ob der Symmetric Key abgerufen werden kann. Klicken Sie im Fenster **Explorer** mit der rechten Maustaste auf **Verschlüsselung** und klicken Sie auf **Test**.

   IBM Cognos Analytics-Komponenten überprüfen die CSK-Verfügbarkeit (Common Symmetric Keys).
8. Klicken Sie im Menü **Datei** auf **Speichern**.

Apache HTTP Server oder IBM HTTP Server konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie Apache HTTP Server oder IBM HTTP Server als Web-Server in IBM Cognos Analytics konfigurieren.

Konfigurieren von IBM HTTP Server V9

Sie können Web-Server von IBM HTTP Server (IHS) V9 zur Unterstützung von Lastausgleich und Ausfällen auf mehreren IBM Cognos Analytics-Anwendungsservern verwenden.

Hierfür müssen Sie IHS V9 und die Web-Server-Plug-ins für IBM WebSphere Application Server V9 installieren und anschließend IHS V9 für die Verwendung der Datei `cognos.conf` konfigurieren.

Weitere Informationen zum Installieren der Web-Server-Plug-ins für IBM WebSphere Application Server V9 finden Sie in diesem Abschnitt (www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/rins_plugins_info.html).

Vorbereitende Schritte

Es gelten folgende Voraussetzungen:

- IBM SDK, Java Technology Edition, Version 8 for Windows (CND15ML)
- IBM WebSphere Application Server V9.0 - Ergänzungen - Web Server Plug-ins (CND1EML)
- IBM WebSphere Application Server V9.0 - Ergänzungen - IBM HTTP Server (CND1DML)

Informationen zu diesem Vorgang

Die Verzeichnisse und Aliasnamen für Windows-basierte IBM HTTP Server-Setups (IHS) müssen richtig angegeben werden. Beispielsweise muss der Aliasname `ibmcognos` muss auf `/ibmcognos "c:/`*`position_von_cognos_analytics`*`/cognos/webcontent"` gesetzt werden. Stellen Sie sicher, dass der Schrägstrich (/) im Pfad verwendet wird und die Position in doppelte Anführungszeichen ("") eingeschlossen ist.

Vorgehensweise

1. Installieren Sie IBM Installation Manager (IIM), und zwar bevorzugt Version 1.8.5 oder höher, wenn Sie das Produkt noch nicht installiert haben.

   Sie können IIM über diese Adresse (www.ibm.com/support/docview.wss?uid=swg24041188) herunterladen.
2. Installieren Sie mithilfe von IIM das Produkt IBM HTTP Server (IHS) V9 und die Web-Server-Plug-ins für IBM WebSphere Application Server V9 über die Seite Online product repositories for Liberty offerings (Onlineproduktrepositorys für Liberty-Produktangebote) (www.ibm.com/support/knowledgecenter/SSEQTP_liberty/com.ibm.websphere.wlp.nd.multiplatform.doc/ae/cwlp_ins_repositories.html).

   Stellen Sie sicher, dass Sie die folgenden Installationspfade verwenden:

   - `/opt/IHS90` als IHS V9-Installationsstammverzeichnis
   - `/opt/IHS90Plugin` als Installationsstammverzeichnis für Web-Server-Plug-ins für IBM WebSphere Application Server

     Sie können die Plug-ins nicht im Installationsstammverzeichnis von IHS V9 installieren.
3. Verknüpfen Sie die Web-Server-Plug-ins für WAS V9 und IHS V9, indem Sie die folgenden Befehle ausführen:

   ```
   cd /opt/IHS90
   bin/simplepct.sh /opt/IHS90Plugin
   ```

   Die Datei `simplepct.sh` wurde in IHS V9 Fixpack 5 eingeführt und ist in früheren Versionen von IHS V9 nicht verfügbar. Weitere Informationen finden Sie in diesem Artikel (www.ibm.com/support/docview.wss?uid=swg24044965).

   Tipp: Überprüfen Sie unter UNIX die Datei `httpd.conf` in der IHS V9-Installation nach dem Ausführen dieses Befehls. Wird dort der Ordner $PLG_ROOT angezeigt, ersetzen Sie ihn durch den Ordner des Installationsstammverzeichnisses für Web-Server-Plug-ins für WAS V9, zum Beispiel `/opt/IHS90Plugin`.
4. Erstellen Sie die Datei `plugin-cfg.xml` für Web-Server-Plug-ins für WAS. Weitere Informationen finden Sie im Abschnitt „Erstellen der plugin-cfg.xml für Cognos Analytics-Server ” auf Seite 128.
5. Kopieren Sie die Datei `plugin-cfg.xml`, die in Schritt 4 erstellt wurde, in das Verzeichnis *`WAS_Web_Server_Plugins_Installationsstammverzeichnis`*`/config/webserver1`, zum Beispiel `/opt/IHS90Plugin/config/webserver1`.

Tipp: Stellen Sie unter UNIX sicher, dass die Datei `plugin-cfg.xml` nach dem Kopieren der Datei über Berechtigungen zum Lesen und Ausführen verfügt.

6. Konfigurieren Sie IHS V9 durch Ausführen der folgenden Schritte:
   a) Greifen Sie auf die Vorlagendatei `cognos_IHS9_SSO.conf` oder `cognos_IHS9.conf` im Cognos Analytics-Verzeichnis *gateway_install_location*`/cgi-bin/templates` zu.
   b) Kopieren Sie die Vorlagendatei in das Verzeichnis *IHS9_Installationsstammverzeichnis*`/conf`, zum Beispiel `/opt/IHS90/conf`, und benennen Sie sie um in `cognos.conf`. Ändern Sie die Datei `cognos.conf` entsprechend, damit sie auf die richtige Installationsposition verweist.
   c) Konfigurieren Sie `httpd.conf` wie im Abschnitt „Konfigurieren von Cognos Analytics mit Apache HTTP Server oder IBM HTTP Server" auf Seite 134 beschrieben.
   d) Starten Sie den Web-Server von IHS V9 neu.

Konfigurieren von IBM HTTP Server V9 mit SSL

Wenn Sie Secure Sockets Layer (SSL) für IBM Cognos Analytics mit IBM HTTP Server V9 als Web-Server verwenden, müssen Sie SSL zwischen den Plug-ins für WAS-Web-Server und dem Cognos Analytics-Anwendungsserver einrichten. Dazu müssen Sie das IBM Cognos-Zertifikat extrahieren und anschließend zum Truststore der Plug-ins für WAS-Web-Server hinzufügen.

Wenn Sie SSL für IBM HTTP Server V9 verwenden, konfigurieren Sie Ihre Umgebung wie im Abschnitt „IBM HTTP Server mit SSL verwenden" auf Seite 130 beschrieben.

Vorgehensweise

1. Starten Sie den IBM Cognos Analytics-Anwendungsserver, der für die Verwendung von SSL konfiguriert ist.
2. Kopieren Sie den Abschnitt `Server` aus der Datei *Stammverzeichnis der Cognos Analytics-Anwendungsserverinstallation*`/wlp/usr/servers/cognosserver/logs/state/plugin-cfg.xml` in die Datei `plug-in/config/webserver1/plugin-cfg.xml`. Stellen Sie sicher, dass der `https`-Eingangspunkt für Cognos Analytics angegeben ist, wie im folgenden Beispiel dargestellt:

```
<Server CloneID="a4949c5e-cb36-40dd-9f43-58702daf7b1a" ConnectTimeout="5"
ExtendedHandshake="false" LoadBalanceWeight="20" MaxConnections="-1"
Name="default_node_cognosserver" ServerIOTimeout="900" WaitForContinue="false">
   <Transport Hostname="hostname" Port="xxx" Protocol="https">
   <Property Name="keyring" Value="D:\install\IBM\WebSphere\Plugins\config\
         webserver1\plugin-key.kdb"/>
   <Property Name="stashfile" Value="D:\install\IBM\WebSphere\Plugins\config\
         webserver1\plugin-key.sth"/>
   </Transport>
</Server>
```

3. Fügen Sie in der Datei `Plug-in/config/webserver1/plugin-cfg.xml` das folgende Attribut zum Abschnitt `Config` hinzu:

```
AutoSecurity="false"
```

4. Rufen Sie das IBM Cognos-Zertifikat ab, indem Sie die folgenden Schritte ausführen:
   a) Wechseln Sie in das Verzeichnis Cognos Analytics *Anwendungsserver_Installationsstammverzeichnis*`/bin`.
   b) Extrahieren Sie das Zertifikat, in dem Sie den für Ihr Betriebssystem geeigneten Befehl eingeben.

      Geben Sie unter UNIX oder Linux Folgendes ein:

```
ThirdPartyCertificateTool.sh -E -T -r destination file -p NoPassWordSet
```

      Geben Sie unter Windows Folgendes ein:

```
ThirdPartyCertificateTool.bat -E -T -r destination file -p NoPassWordSet
```

5. Kopieren Sie die `.cert`-Datei, zum Beispiel `ca-host1.cert`, die in Schritt 4 erstellt wurde, auf den Host der Plug-ins für WAS-Web-Server.
6. Fügen Sie die Datei Cognos Analytics `.cert` zum Plug-in-Keystore für WAS-Web-Server `plugin-key.kdb` hinzu. Wenn die Datei `plugin-key.kdb` nicht vorhanden ist, erstellen Sie eine solche Datei, wie in Schritt 7 beschrieben.

   Zum Hinzufügen der `.cert`-Datei zum Keystore können Sie verschiedene Methoden verwenden. In den folgenden Schritten wird beschrieben, wie Sie die Datei mithilfe des Tools `gskcapicmd`, das im Lieferumfang von IHS V9 enthalten ist, hinzufügen können.

   a) Wechseln Sie zum Ordner IHS9 ROOT.

   b) Geben Sie den für Ihr Betriebssystem geeigneten Befehl ein.

      Geben Sie unter UNIX oder Linux Folgendes ein:

      ```
      bin/gskcapicmd -cert -add -db WAS_Plugin_root/config/webserver1/plugin-key.kdb
      -stashed -label ca-host1 -file ca-host1.cert
      ```

      Geben Sie unter Windows Folgendes ein:

      ```
      bin\gskcapicmd.bat -cert -add -db WAS_Plugin_root\config\webserver1\plugin-key.kdb
      -stashed -label ca-host1 -file ca-host1.cert
      ```

      Informationen zu anderen Methoden zum Hinzufügen von Zertifikatsdateien zum Keystore finden Sie im IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0).
7. Erstellen Sie einen leeren Keystore für Plug-ins für WAS-Web-Server:

   a) Wechseln Sie zum Ordner IHS9 ROOT.

   b) Geben Sie den für Ihr Betriebssystem geeigneten Befehl ein.

      Geben Sie unter UNIX oder Linux Folgendes ein:

      ```
      bin/gskcapicmd -keydb -create -db WAS_Plugin_root/config/webserver1
        /plugin-key.kdb -pw xxx -stash
      ```

      Geben Sie unter Windows Folgendes ein:

      ```
      bin\gskcapicmd.bat -keydb -create -db WAS_Plugin_root\config\webserver1
         \plugin-key.kdb -pw xxx -stash
      ```

Erstellen der plugin-cfg.xml für Cognos Analytics-Server

In einer Umgebung mit WebSphere Application Server enthält die Datei `plugin-cfg.xml` Konfigurationsinformationen, die bestimmen, wie das Web-Server-Plug-in Anforderungen weiterleitet.

Informationen zu diesem Vorgang

Diese Prozedur trifft nicht auf die IBM Cognos Analytics-Server zu, die zum Ausführen des Content Manager-Service verwendet werden.

Vorgehensweise

1. Wechseln Sie in die Installationsposition des Cognos Analytics-Anwendungsservers.
2. Öffnen Sie die Datei *ca_Anwendungsserver_Installationsstammverzeichnis*`/wlp/usr/servers/cognosserver/server.xml` und fügen Sie der Datei die folgende Einstellung hinzu:

   ```
   <pluginConfiguration pluginInstallRoot="WAS_plugin_install_root”
   webserverPort="IHS9_port"/>
   ```

   Beispiel:

   ```
   <pluginConfiguration pluginInstallRoot="/opt/IHS90Plugin" webserverPort="8080"/>
   ```

3. Konfigurieren und starten Sie den Cognos Analytics-Anwendungsserver.

   Nach dem Starten des Servers wird eine Datei mit dem Namen `plugin-cfg.xml` im Verzeichnis Cognos Analytics *`applicaton_server_install_root`*`/wlp/usr/servers/cognosserver/logs/state` generiert.
4. Öffnen Sie die Datei `plugin-cfg.xml` und ändern Sie den Abschnitt `UriGroup`, indem Sie alles mit Ausnahme der beiden folgenden Elemente löschen:

```
<UriGroup Name="default_host_cognosserver_default_node_Cluster_URIs">
    <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
        Name="/bi/*"/>
    <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
        Name="/bi/v1/*"/>
</UriGroup>
```

   Tipp: Der zweite `Uri`-Eintrag ist in der Datei nicht vorhanden. Sie müssen ihn hinzufügen.
5. Speichern Sie die Datei `plugin-cfg.xml`.

   Sie haben nun einen Cognos Analytics-Anwendungsserver für den `ServerCluster` konfiguriert.
6. Wenn Sie einen weiteren Cognos Analytics-Anwendungsserver zum `ServerCluster` hinzufügen möchten, führen Sie die folgenden Schritte aus:
   a) Öffnen Sie vom Verzeichnis Cognos Analytics *`Anwendungsserver_Installationsstammverzeichnis`*`/wlp/usr/servers/cognosserver/logs/state` aus die Datei `plugin-cfg.xml`. Kopieren Sie das Element `Server` unter den Abschnitt `ServerCluster`. Kopieren Sie beispielsweise das folgende `Server`-Element:

```
<Server CloneID="081cd7c5-bb6c-4a93-a074-33fa07e587f3" ConnectTimeout="5"
ExtendedHandshake="false" LoadBalanceWeight="20" MaxConnections="-1"
Name="default_node_cognosserver" ServerIOTimeout="900" WaitForContinue="false">
<Transport Hostname="caserverhost" Port="9300" Protocol="http"/>
</Server>
```

   b) Fügen Sie das Element `Server` in den Abschnitt `ServerCluster` in der in Schritt 4 erstellten Datei `plugin-cfg.xml` ein. Stellen Sie sicher, dass von Ihrem Web-Server-Host Zugriff auf den im Element `Server` angegebenen Endpunkt besteht.
   c) Ändern Sie den Namen des Servers, indem Sie den Wert des Attributs `Name` ändern. Stellen Sie sicher, dass sich der Name von den anderen Servernamen im `ServerCluster` unterscheidet. Ändern Sie den Wert beispielsweise von `default_node_cognosserver` in `default_node_cognosserver_1`.
   d) Fügen Sie den neuen Server zum Abschnitt `PrimaryServers` hinzu wie nachfolgend dargestellt:

```
<PrimaryServers>
    <Server Name="default_node_cognosserver"/>
    <Server Name="default_node_cognosserver_1"/>
</PrimaryServers>
```

   e) Speichern Sie die Datei `plugin-cfg.xml`. Der neue Server wird zum `ServerCluster` hinzugefügt.
7. Wenn Sie weitere Server hinzufügen möchten, wiederholen Sie Schritt 6.

Nächste Schritte

Weitere Informationen zum Zusammenführen der Datei `plugin-cfg.xml` von mehreren eigenständigen WebSphere Liberty-Profilservern finden Sie in diesem Abschnitt (www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/twsv_merge_configfiles.html).

Konfigurieren von WebDAV auf einem IBM HTTP Server oder auf einem Apache HTTP Server

Konfigurieren Sie Web Distributed Authoring and Versioning (WebDAV) auf Ihrem Web-Server, um Bilder in Reporting anzeigen und durchsuchen zu können.

Berichtsersteller können ähnlich wie beim Durchsuchen eines Dateisystems nach Bildern suchen, die zu Berichten hinzugefügt werden sollen. Auf einem IBM HTTP Server oder einem Apache HTTP Server müssen Sie der Serverkonfigurationsdatei Anweisungen hinzufügen und danach den Verzeichniszugriff konfigurieren.

Gehen Sie wie im Folgenden beschrieben vor, um WebDAV auf Apache 2.4 zu konfigurieren.

Vorgehensweise

1. Öffnen Sie im Verzeichnis *Web-Server-Verzeichnis*/conf die Datei httpd.conf in einem Texteditor.
2. Kommentieren Sie die Anweisungen aus, mit denen modules/mod_dav.so und modules/mod_dav_fs.so geladen werden.

```
LoadModule dav_module modules/mod_dav.so
LoadModule dav_fs_module modules/mod_dav_fs.so
```

3. Geben Sie ein Verzeichnis für die Anweisung DAVLockDB an.

   Zum Beispiel

   DAVLockDB "*Web-Server-Position*/var/DavLock"

   Stellen Sie sicher, dass das Verzeichnis vorhanden ist.
4. Erstellen Sie einen Alias für das Verzeichnis, in dem Ihre Bilder gespeichert sind.
5. Fügen Sie Dav On zu den <Directory>-Informationen für den Alias hinzu.

   Beispiel für Apache 2.4:

```
Alias /images "Pfad/shared_images"

<Directory "path/shared_images">
   Dav On
   Options Indexes MultiViews
   AllowOverride None
   Require all granted
</Directory>
```

6. Speichern Sie die Datei.
7. Starten Sie den Web-Server erneut.

Ergebnisse

Wenn WebDAV aktiviert ist, können Reporting-Benutzer ihren Berichten Bilder hinzufügen. Klicken die Benutzer im Bildbrowser auf **Durchsuchen**, ist http://*Servername*/ibmcognos/bi/samples/images das Standardsuchverzeichnis. Wenn Sie ein anderes Verzeichnis erstellt haben, können Benutzer dieses Verzeichnis eingeben.

IBM HTTP Server mit SSL verwenden

Wenn Sie Secure Sockets Layer (SSL) auf einem IBM HTTP Server verwenden, müssen Sie die Werte für **Gateway-URI** in IBM Cognos Configuration ändern, um auf das Portal zugreifen zu können.

Um SSL auf Ihrem Web-Server zu aktivieren, müssen Sie ein von einer Zertifikatsstelle signiertes Web-Server-Zertifikat einholen und auf Ihrem Web-Server installieren. Weitere Informationen zur Verwendung von Zertifikaten auf Ihrem Web-Server finden Sie in der Dokumentation zum Web-Server. Diese Zertifikate sind nicht im Lieferumfang von IBM Cognos-Produkten enthalten.

Um Benutzern den Zugriff auf das IBM Cognos-Portal über SSL zu ermöglichen, müssen Sie in IBM Cognos Configuration die Werte für **Gateway-URI** für alle Computer ändern, auf denen die Komponenten der Anwendungsebene und Framework Manager sind.

Vorbereitende Schritte

Auf dem IBM HTTP Server muss IBM Global Security Kit (GSKit) installiert sein. Weitere Informationen zu den unterstützten Versionen von GSKit für IBM HTTP Server finden Sie im entsprechenden IBM Software Compatibility Report.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf allen Computern, auf denen die Komponenten der Anwendungsebene und Framework Manager installiert sind.
2. Klicken Sie unter **Lokale Konfiguration** auf **Umgebung** und ändern Sie den Wert für **Gateway-URI** von `http` in `https`.
3. Ändern Sie im Wert **Gateway-URI** die Portnummer in die SSL-Portnummer, die für Ihren Web-Server definiert ist.
   Die Standardportnummer für SSL-Verbindungen ist für gewöhnlich 443.
4. Wechseln Sie auf jedem Computer, auf dem die Komponenten der Anwendungsebene oder Framework Manager installiert sind, in das Verzeichnis *installationsposition*`/bin` und importieren Sie alle Zertifikate in den IBM Cognos-Truststore, die zur Zertifikatskette gehören, beginnend mit dem Stammzertifikat der Zertifizierungsstelle.

   Importieren Sie die Zertifikate durch die Eingabe des folgenden Befehls:

   Geben Sie unter UNIX oder Linux Folgendes ein:

   `ThirdPartyCertificateTool.sh -T -i -r` *Pfad/Zertifikatsdateiname* `-p` *Kennwort*

   Geben Sie unter Windows Folgendes ein:

   `ThirdPartyCertificateTool.bat -T -i -r` *Pfad\Zertifikatsdateiname* `-p` *Kennwort*

   Anmerkung: Wenn das Kennwort nicht festgelegt wurde, lautet das Standardkennwort 'NoPassWordSet'.
5. Geben Sie folgenden Befehl vom Verzeichnis *ihs-installationsverzeichnis*`/bin` des Web-Servers ein:
   ihs-installationsverzeichnis`/bin/`*scriptname*

   Dabei ist *ihs-installationsverzeichnis* das Verzeichnis, in dem IBM HTTP Server installiert ist und *scriptname* ist bei Microsoft Windows `gskver.bat` und bei UNIX oder Linux `gskver.sh`.

   Die gemeinsam genutzten Bibliotheken und die Versionsinformation zu GSKit werden angezeigt. Überprüfen Sie, dass die angezeigte Version die unterstützte Mindestversion ist, die im Unterstützungsdokument im Abschnitt mit der *Einführung* für diese Prozedur genannt wird.
6. Starten Sie das Dienstprogramm 'iKeyman', indem Sie den folgenden Befehl eingeben:
   ihs-installationsverzeichnis`/bin/`*scriptname*

   Dabei ist *ihs-installationsverzeichnis* das Verzeichnis, in dem IBM HTTP Server installiert ist und *scriptname* ist bei Microsoft Windows `ikeyman.bat` und bei UNIX oder Linux `ikeyman.sh`.
7. Wählen Sie im Menü **Schlüsseldatenbankdatei** > **Neu** aus.
8. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**:

   Dateiname
   Der Name der Schlüsseldatenbankdatei. Der Standardwert ist `key.kdb`.

   Position
   Position zum Speichern der Datei `key.kdb`. Der Standardwert ist *ihs-installationsverzeichnis*`/bin`.
9. Geben Sie im Fenster **Aufforderung zur Kennworteingabe** ein Kennwort ein, wählen Sie das Markierungsfeld zum verdeckten Speichern des Kennworts in der Datei aus und klicken Sie auf **OK**.

Wenn Sie das Markierungsfeld zum verdeckten Speichern des Kennworts in der Datei ausgewählt haben, wird das Kennwort verschlüsselt und in einer Datei mit der Erweiterung `.sth` in demselben Verzeichnis gespeichert wie die Schlüsseldatenbankdatei.

Eine Nachricht über den erfolgreichen Abschluss wird angezeigt.

10. Öffnen Sie die Datei *ihs-installationsverzeichnis*/conf/httpd.conf in einem Texteditor.
11. Fügen Sie die Anweisung Keyfile mit dem Pfad zu Ihrer Schlüsseldatenbankdatei hinzu. Stellen Sie die Anweisung nach dem Abschnitt VirtualHost in die Datei.
Zum Beispiel

```
<VirtualHost *:443>
...
</VirtualHost>
KeyFile ihs_installationsverzeichnis/key.kdb
```

12. Speichern und schließen Sie die Datei httpd.conf.
13. Extrahieren Sie das Cognos Analytics-Zertifikat in einer Datei. Führen Sie den folgenden Befehl vom IBM Cognos Analytics-Server in *ca_install*/bin aus.

```
scriptname -E -T -r ca-zertifikatsdatei -p NoPassWordSet
```

Dabei ist *scriptname* für Microsoft Windows ThirdPartyCertificateTool.bat und für UNIX oder Linux ThirdPartyCertificateTool.sh. Ferner ist *ca-zertifikatsdatei* der Name der Zertifikatsdatei.

14. Kopieren Sie die Zertifikatsdatei in *ihs_installationsverzeichnis/schlüsseldatenbankdateiverzeichnis* wobei *ihs-installationsverzeichnis* das Verzeichnis ist, in dem IBM HTTP Server installiert ist und *schlüsseldatenbankdateiverzeichnis* das Verzeichnis ist, in dem die Schlüsseldatenbankdatei gespeichert ist.
15. Geben Sie in *ihs_installationsverzeichnis*/bin den folgenden Befehl ein:

```
scriptname -cert -import -db ca-zertifikatsdatei
-pw NoPassWordSet -target key.kdb -target_pw schlüsseldatenbankdateikennwort
```

Dabei ist *scriptname* für Microsoft Windows gskcapicmd.bat und für UNIX oder Linux gskcapicmd.sh. Ferner ist *schlüsseldatenbankdateikennwort* das Kennwort für die Schlüsseldatenbankdateidatei.

16. Starten Sie IBM HTTP Server. Geben Sie den folgenden Befehl in ihs-installationsverzeichnis/bin ein:

```
scriptname -k start
```

Dabei ist *scriptname* für Microsoft Windows apchectl.bat oder für UNIX oder Linux ./apachectl. Unter Microsoft Windows können Sie das Script auch als Service starten.

17. Stellen Sie sicher, dass IBM HTTP Server aktiv ist, indem Sie die folgende URI in das Adressfeld eines Web-Browsers eingeben:

```
https://hostname_des_web-servers:port
```

Dabei ist *hostname_des_web-servers* der Hostname von IBM HTTP Server und *port* ist die Portnummer von IBM HTTP Server.

18. Speichern Sie die Konfiguration und starten Sie anschließend die Services neu.

Ergebnisse

Wenn Sie über https://**servername**:443/ibmcognos auf das Portal zugreifen, werden Sie zur Installation eines Zertifikats aufgefordert. Installieren Sie das Zertifikat in einem der Zertifikatspeicher Ihres Web-Browsers, damit Sie nicht bei jeder neuen Sitzung einen Sicherheitsalert erhalten.

Konfigurieren von Apache HTTP Server oder IBM HTTP Server für Cognos Analytics

Nachdem Sie diese Prozedur ausgeführt haben, kann der Server Anforderungen für statische Dateien (wie beispielsweise `.js`, `.html`, `.css`), Lastausgleichsanforderungen an IBM Cognos Analytics und SSO-Weiterleitungsanforderungen über den Gateway-Code von IBM Cognos Analytics bearbeiten.

Informationen zu diesem Vorgang

Sie können eine der Beispielkonfigurationsdateien verwenden, die mit IBM Cognos Analytics bereitgestellt werden. Die Beispieldateien befinden sich in *installationsposition_der_gatewaykomponente*`/cgi-bin/templates`, wobei *installationsposition_der_gatewaykomponente* das Verzeichnis ist, in dem die Gateway-Komponente installiert ist. Die folgende Tabelle beschreibt die Beispieldateien. Wählen Sie die Datei für Ihre Umgebung aus.

Umgebung	Beispieldateiname
Apache 2.2 Nicht-SSO	cognos_apache22_loadbalance.conf
Apache 2.2 SSO	cognos_apache22_loadbalance_SSO.conf
Apache 2.4 Nicht-SSO	cognos_apache24_loadbalance.conf
Apache 2.4 SSO	cognos_apache24_loadbalance_SSO.conf
IBM HTTP Server 8.5 Nicht-SSO	cognos_IHS85_loadbalance.conf
IBM HTTP Server 8.5 SSO	cognos_IHS85_loadbalance_SSO.conf

Die Verzeichnisse und Aliasnamen für Windows-basierte IBM HTTP Server-Setups (IHS) müssen richtig angegeben werden. Beispielsweise muss der Aliasname `ibmcognos` muss auf `/ibmcognos "c:/`*position_von_cognos_analytics*`/cognos/webcontent"` gesetzt werden. Stellen Sie sicher, dass der Schrägstrich (/) im Pfad verwendet wird und die Position in doppelte Anführungszeichen ("") eingeschlossen ist.

Vorgehensweise

1. Kopieren Sie die Beispielkonfigurationsdatei in das Verzeichnis *installationsverzeichnis_von_apache_oder_ihs*`/conf` und benennen Sie sie in `cognos.conf` um.
2. Öffnen Sie `cognos.conf` in einem Texteditor und ändern Sie die Anweisung `BalancerMember` für die Verwendung von https und einem vollständig qualifizierten Domänennamen.
   Beispiel:

   ```
   <Proxy balancer://mycluster>
       BalancerMember https://ica-host1.domain:9300 route=1
       BalancerMember https://ica-host2.domain:9300 route=2
   </Proxy>
   ```

3. Vergewissern Sie sich, dass der folgenden Abschnitt in der Beispieldatei enthalten ist.

   ```
   # Statische Referenzen für gespeicherte Ausgabe und Anzeigefunktion neu schreiben
   RewriteRule ^/ibmcognos/bi/rv/(.*)$ /ibmcognos/rv/$1 [PT,L]
   ```

   Ist dieser Abschnitt nicht vorhanden, fügen Sie ihn nach dem Abschnitt `# Statische Referenzen für Event Studio neu schreiben` hinzu.
4. Wenn Sie Cognos Analytics for Jupyter Notebook Server integrieren möchten, positionieren Sie den Cursor VOR `RewriteRule ^/ibmcognos$ /ibmcognos/ [R,L]` und geben Sie die folgende Rewrite-Regel für gesicherte Cognos Analytics-Server ein:

```
RewriteRule ^/ibmcognos/bi/v1/jupyter/(user/[^/]*)/(api/kernels/[^/]+/chan-
nels)(.*) wss://jupyter_host_name:jupyter_host_port/bi/v1/jupyter/$1/$2$3
[P,L]
```

jupyter_host_name und *jupyter_host_port* werden in der Datei `config.conf` definiert, wenn Sie Jupyter Notebook Server konfigurieren.

Wichtig:

- Für nicht gesicherte Server lautet die Rewrite-Regel: `ws://jupyter_host_name:jupyter_host_port/bi/v1/jupyter/$1/$2$3 [P,L]`.
- 11.1.6 Ab Cognos Analytics Version 11.1.6 unterstützt Jupyter Notebook nur Apache 2.4-Gateways. Die Gateway-Vorlage für Apache 2.4 enthält die erforderlichen Regeln für das Umschreiben. Sie müssen nur die Kommentarzeichen entfernen und die gewünschten Änderungen vornehmen.

5. Suchen Sie den Abschnitt `Directory` und stellen Sie sicher, dass auf das Installationsverzeichnis von IBM Cognos Analytics verwiesen wird.
6. Speichern Sie die Datei `cognos.conf`.
7. Konfigurieren Sie `httpd.conf` wie im Abschnitt „Konfigurieren von Cognos Analytics mit Apache HTTP Server oder IBM HTTP Server” auf Seite 134 beschrieben.

Konfigurieren von Cognos Analytics mit Apache HTTP Server oder IBM HTTP Server

In diesem Abschnitt wird beschrieben, wie Sie Apache HTTP Server oder IBM HTTP Server für eine Verwendung der Datei `cognos.conf` konfigurieren. Diese Konfigurationsdatei enthält alle für IBM Cognos Analytics erforderlichen Einstellungen.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um den Web-Server so konfigurieren, dass die Datei `cognos.conf` verwendet werden kann. Diese Konfigurationsdatei enthält alle für IBM Cognos Analytics erforderlichen Einstellungen.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis `apache/conf`.
2. Öffnen Sie die Datei `httpd.conf` in einem Texteditor.
3. Führen Sie bei Verwendung von SSL die folgenden Schritte aus
   a) Fügen Sie in dieser Datei folgende Zeilen hinzu:

```
<VirtualHost *:443>
SSLEnable
SSLClientAuth None
SSLProxyEngine on
# IBM Cognos Analytics-Konfiguration
  Include conf/cognos.conf
</VirtualHost>
SSLDisable
```

   b) Führen Sie die folgenden Schritte aus, wenn Sie SSL mit IBM HTTP Server verwenden:
      i) Entfernen Sie die Kommentarzeichen bei folgender Zeile:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
```

      ii) Aktualisieren Sie den Wert des Verzeichnisses `ServerName` mit dem Hostnamen von IBM HTTP Server.
4. Wenn Sie SSL nicht verwenden, fügen Sie folgende Zeilen zur Datei hinzu:

```
<VirtualHost *:80>
  Include conf/cognos.conf
</VirtualHost>
```

5. Speichern und schließen Sie die Datei `httpd.conf`.

Nur für UNIX - Definieren Sie den MIME-Typ für SVG-Dateien.

6. Öffnen Sie die Datei `etc/mime.types` in einem Texteditor und fügen Sie folgende Zeilen hinzu:

```
#MIME type          Extensions
image/svg+xml      svg
```

7. Speichern Sie die Datei und schließen Sie sie.
8. Damit das Cognos Analytics-Webmodul in UNIX- und Linux-Umgebungen ausgeführt werden kann, müssen Sie das IBM Cognos Analytics-Gateway-Verzeichnis `cgi-bin` an den Bibliothekspfad anhängen.

Betriebssystem	**Variable**
AIX	LIBPATH
Solaris oder Linux	LD_LIBRARY_PATH

   Melden Sie sich in einer Linux-Umgebung beispielsweise als der Benutzer an, der den Web-Server startet. Wenn Sie die Bash-Shell verwenden, müssen Sie Folgendes an das Ende von $HOME/.bashrc anhängen: `Export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/ibm/cognos/analytics/cgi-bin`

9. Starten Sie den Web-Server neu.

Lastausgleich für den Apache-Web-Server

Mithilfe des Lastausgleichs können Sie den Apache-Web-Server skalieren.

Informationen zum Lastausgleich bei Apache finden Sie in den folgenden Ressourcen:

- https://httpd.apache.org/docs/2.4/mod/mod_proxy_balancer.html
- https://httpd.apache.org/docs/2.4/mod/mod_proxy.html#balancermember

Anmerkung: Weitere Konfigurationsoptionen für die Cognos Analytics-Umgebung erhalten Sie beim zuständigen Apache-Administrator.

Aktivieren von HTTP/2 für einen Web-Server

HTTP/2 ist ein Netzprotokoll für den Transport von Inhalten mit niedriger Latenzzeit. Dieses Protokoll ist für den Lastausgleich bestimmter Anforderungen und für den effizienten Einsatz von statischen Inhalten, wie z. B. Symbolen und Bilddateien, von wesentlicher Bedeutung.

Für IBM Cognos Analytics ist die Konfiguration eines Web-Servers wie Microsoft IIS oder Apache HTTP Server für HTTP/2 nicht erforderlich. Als bewährtes Verfahren empfiehlt sich jedoch eine solche Konfiguration.

Die Aktivierung von HTTP/2 auf Ihrem Web-Server kann die Reaktionsfähigkeit einiger Ihrer Cognos Analytics-Dashboards verbessern. Im Vergleich zum traditionellen HTTP/1.1-Protokoll bietet HTTP/2 die folgenden beiden Hauptvorteile, durch die die Ladezeiten von Widgets in Ihren Dashboards verbessert werden können.

- Headerkomprimierung

  Die HTTP-Headergröße ist in HTTP/2 im Vergleich zu HTTP/1.1 wesentlich kleiner, was eine schnellere Übertragung von Informationen bedeutet.
- Verbesserter gemeinsamer Zugriff auf Anforderungen

HTTP/2 unterstützt mehrere Anforderungen für dieselbe TCP-Verbindung. Dashboarding in Cognos Analytics ist für die parallele Verarbeitung von Widgets konzipiert, HTTP/1.1 drosselt die Anzahl gleichzeitiger Abfragen jedoch viel mehr als HTTP/2. Durch die Verwendung von HTTP/2 kann im Vergleich zu HTTP/1.1 eine größere Anzahl von Dashboard-Widgets gleichzeitig verarbeitet werden.

Die persistente Client/Server-Verbindung ist ein weiterer Vorteil von HTTP/2. Dies bedeutet, dass ein TLS-Handshake (TLS ist der Nachfolger von SSL) nur ein Mal erfolgt und nicht bei jeder Anforderung. Bei Umgebungen mit höherer Latenzzeit kann dieser Faktor erhebliche Auswirkungen auf die Wartezeiten des Benutzers haben.

Beachten Sie die folgenden Faktoren, bevor Sie HTTP/2 aktivieren:

- HTTP/2 wird nur über TLS unterstützt. Sie müssen daher der URL `https://` voranstellen, wenn Sie auf Ihre Cognos-Umgebung zugreifen. Andernfalls greift das System auf die Verwendung von HTTP/1.1 zurück.
- Nicht alle Web-Browser-Versionen unterstützen HTTP/2 und stellen stattdessen eine Verbindung über HTTP/1.1 her. Ein Beispiel hierfür ist Internet Explorer 11 unter Windows 7.
- Wenn HTTP/2 aktiviert ist, begrenzt der Web-Browser die Anzahl gleichzeitig ablaufender Abfragen nicht mehr. HTTP/2 ermöglicht es einem ausgelasteten Dashboard, die Workload auf dem Cognos Analytics-Server und auf allen zugrunde liegenden Datenservern auf eine Weise zu erhöhen, die mit HTTP/1.1 nicht möglich ist. Weniger Benutzer sind nun in der Lage, eine viel größere Last auf Back-End-Servern auszuführen.

Vorgehensweise

Weitere Informationen zu HTTP/2 und dessen Aktivierung finden Sie auf den folgenden Websites:

- Apache: https://httpd.apache.org/docs/2.4/howto/http2.html
- IIS: https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-10/http2-on-iis
- NGINX: https://www.nginx.com/blog/http2-module-nginx/#config

Konfigurieren Sie Microsoft Internet Information Services

In diesem Abschnitt wird beschrieben, wie Sie Microsoft Internet Information Services (IIS) als Web-Server in IBM Cognos Analytics konfigurieren.

Konfigurieren von WebDAV auf IIS

Konfigurieren Sie WebDAV (Web Distributed Authoring and Versioning) auf Ihrem Web-Server, wenn Sie in Reporting Bilder anzeigen und nach Bildern suchen wollen. Berichtsersteller können ähnlich wie beim Durchsuchen eines Dateisystems nach Bildern suchen, die zu Berichten hinzugefügt werden sollen. Auf Web-Servern mit Microsoft Internet Information Services (IIS) müssen Sie zunächst die WebDAV-Funktion aktivieren und den Web-Server danach so konfigurieren, dass er auf das Bildverzeichnis zugreifen kann.

Vorgehensweise

1. Klicken Sie in Microsoft Windows in der **Systemsteuerung** auf **Programme** > **Programme und Funktionen**.

   In Microsoft Windows 8 oder 2012 Server befindet sich der Link **Programme und Funktionen** direkt in der **Systemsteuerung**.
2. Klicken Sie auf **Windows-Funktionen aktivieren oder deaktivieren**.
3. Wenn Sie Microsoft Windows 2008 Server verwenden, gehen Sie folgendermaßen vor:
   a) Klicken Sie auf **Server-Manager** > **Rollen** > **Webserver (IIS)**.
   b) Wählen Sie im Abschnitt **Role Services** (Rollendienste) die Option **Add Role Services** (Rollendienste hinzufügen) aus.

c) Wählen Sie unter **Web Server** > **Common HTTP Features** (Allgemeine HTTP-Funktionen) die Option **WebDAV Publishing** (WebDAV-Veröffentlichung) aus.

d) Klicken Sie auf **Weiter** und dann auf **Installieren**.

4. Wenn Sie Microsoft Windows 2012 Server verwenden, gehen Sie folgendermaßen vor:
   a) Klicken Sie im Assistenten zum Hinzufügen von Rollen und Funktionen auf **Role-based or feature-based installation** (Rollen- oder funktionsbasierte Installation) und danach auf **Weiter**.
   b) Wählen Sie Ihren Server aus und klicken Sie auf **Weiter**.
   c) Erweitern Sie **Web Server (IIS)** > **Web Server** > **Common HTTP Features** (Allgemeine HTTP-Funktionen) und wählen Sie **WebDAV Publishing** (WebDAV-Veröffentlichung) aus.
   d) Klicken Sie auf **Weiter** > **Weiter** und anschließend auf **Installieren**.
5. Wenn Sie Microsoft Windows 7 oder 8 verwenden, gehen Sie folgendermaßen vor:
   a) Erweitern Sie **Internet Information Services** > **World Wide Web Services** > **Common HTTP Features** (Allgemeine HTTP-Funktionen).
   b) Wählen Sie **WebDAV Publishing** (WebDAV-Veröffentlichung) aus und klicken Sie auf **OK**.
6. Wählen Sie in der Konsole von Internet Information Services (IIS) Manager unter **Connections** Ihren Servernamen aus.
   - Wenn Sie Microsoft Windows 2012 Server verwenden, wählen Sie in **Server-Manager IIS** aus, klicken Sie mit der rechten Maustaste auf den Namen Ihres Servers und wählen Sie **Internet Information Services (IIS) Manager** aus.
   - Wenn Sie Microsoft Windows 2008 Server verwenden, erweitern Sie in **Server-Manager** die Knoten **Rollen** > **Webserver (IIS)** und klicken Sie dann auf **Internet Information Services (IIS) Manager**.
   - Wenn Sie Microsoft Windows 8 verwenden, klicken Sie in der **Systemsteuerung** auf **Verwaltung**, um auf die **Internet Information Services (IIS) Manager**-Konsole zuzugreifen.
   - Wenn Sie Microsoft Windows 7 verwenden, klicken Sie in der **Systemsteuerung** auf **System und Sicherheit** > **Verwaltung**, um auf die **Internet Information Services (IIS) Manager**-Konsole zuzugreifen.
7. Erweitern Sie unter **Verbindungen** Ihren Web-Server, danach **Sites** und wählen Sie dann Ihre Website aus.
   Beispiel: **Standard-Website**.
8. Klicken Sie doppelt auf **WebDAV Authoring**.
9. Klicken Sie auf **Enable WebDAV** (WebDAV aktivieren).
10. Klicken Sie auf **WebDAV Settings** (WebDAV-Einstellungen).
11. Wenn anonymer Zugriff aktiviert ist, setzen Sie **Allow Anonymous Property Queries** (Anonyme Eigenschaftsabfragen zulassen) auf **True** (Wahr) und klicken Sie auf **Apply** (Übernehmen).
12. Wählen Sie das Verzeichnis bzw. virtuelle Verzeichnis aus, auf das Sie WebDAV-Zugriff erlauben möchten.
13. Klicken Sie doppelt auf **WebDAV Authoring**.
14. Klicken Sie auf **Add Authoring Rule** (Authoring-Regel hinzufügen) und fügen Sie die Regeln für Ihre Umgebung hinzu.
    Wenn Sie z. B. die Beispiele installiert haben und den Standardpfad verwenden möchten, erweitern Sie nun unter dem virtuellen Verzeichnis `ibmcognos` das Verzeichnis `bi/samples`, wählen `images` aus und fügen eine Authoring-Regel für die Bilddateien hinzu.
15. Klicken Sie mit der rechten Maustaste auf das Verzeichnis bzw. virtuelle Verzeichnis, dem Sie die Authoring-Regeln hinzugefügt haben, und wählen Sie **Edit Permissions** (Berechtigungen bearbeiten) aus.
16. Klicken Sie auf **Security** (Sicherheit) und fügen Sie die gewünschten Berechtigungen hinzu.
    Fügen Sie zum Beispiel die Berechtigungen für den Benutzer mit anonymem Zugriff hinzu, wenn anonymer Zugriff auf den Web-Server erlaubt ist. Diesen Benutzer finden Sie, indem Sie die Website

auswählen, auf **Authentication** (Authentifizierung) doppelt klicken und die Eigenschaften der angezeigten Benutzer anzeigen.

Ergebnisse

Wenn WebDAV aktiviert ist, können Reporting-Benutzer ihren Berichten Bilder hinzufügen. Klicken die Benutzer im Bildbrowser auf **Durchsuchen**, ist `http://`*`Servername`*`/ibmcognos/bi/samples/images` das Standardsuchverzeichnis. Wenn Sie ein anderes Verzeichnis erstellt haben, können Benutzer dieses Verzeichnis eingeben.

Konfigurieren von IIS mit SSL

Um Microsoft Internet Information Services (IIS) mit Secure Sockets Layer (SSL) zu konfigurieren, extrahieren Sie das IBM Cognos-Zertifikat und fügen es zum IIS-Truststore hinzu.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *`installationsposition`*`/bin`.
2. Extrahieren Sie das IBM Cognos-Zertifikat durch Eingabe des folgenden Befehls:

   Geben Sie unter UNIX- oder Linux-Betriebssystemen Folgendes ein: `ThirdPartyCertificateTool.sh -E -T -r destination_file -p NoPassWordSet`.

   Geben Sie unter Microsoft Windows-Betriebssystemen Folgendes ein: `ThirdPartyCertificateTool.bat -E -T -r destination_file -p NoPassWordSet`.
3. Führen Sie folgendes Aktion aus: CA-Zertifikat auf IBM Cognos-Server kopieren.
4. Importieren Sie das Zertifikat auf den IIS-Truststore.

   Weitere Informationen dazu, wie das Zertifikat auf den IIS-Truststore importiert wird, finden Sie in Zertifikate für einen lokalen Computer zum Trusted Root Certification Authorities-Store hinzufügen.

Konfigurieren von IIS in Cognos Analytics

Anhand dieser Informationen kann Microsoft Internet Information Services (IIS) for IBM Cognos Analytics konfiguriert werden.

Nach Abschluss dieser Schritte ist IIS so konfiguriert, dass statischer Inhalt (wie z. B. Dateien des Typs `.js`, `.html`, `.css`) direkt von IIS aus bearbeitet wird, während REST-Anforderungen und andere Serveranforderungen an die Cognos Analytics-Back-End-Server gesendet werden.

Das automatisierte Script ist hier verfügbar.

Vorgehensweise

1. Installieren Sie die ARR-Erweiterung (Application Request Routing) für IIS.
   a) Installieren Sie die ARR-Erweiterung für IIS über die folgende URL: http://www.iis.net/downloads/microsoft/application-request-routing
   b) Klicken Sie nach dem Öffnen der Microsoft-Webseite auf die grüne Schaltfläche "Install this extension".

      Folgen Sie den Anweisungen zum Herunterladen und Ausführen der ARR-Erweiterung.
   c) Rufen Sie den IIS-Manager im Windows-Menü **Start\Verwaltung** auf, um sicherzustellen, dass die ARR-Erweiterung erfolgreich installiert wurde. Klicken Sie nach dem Starten des IIS-Managers auf den Servernamen in der linken oberen Ecke der Anzeige, um die verfügbaren Features anzuzeigen. Im mittleren IIS-Bereich sollte nun das **URL-Rewrite**-Feature sichtbar sein. Es wird installiert, wenn ARR installiert wird.
2. Erstellen Sie einen neuen dedizierten Anwendungspool. Sie können ihn z. B. `CAPool` nennen.
   a) Klicken Sie mit der rechten Maustaste auf **Anwendungspools**. Klicken Sie auf **Anwendungspool hinzufügen**.

3. Optional können Sie eine Server-Farm erstellen, um Lastausgleichs- und Failover-Funktionen für Cognos Analytics-Serviceanforderungen bereitzustellen. Beziehen Sie alle Cognos Analytics-Server ein, für die die Anwendungsserverkomponenten installiert und konfiguriert sind.
   a) Klicken Sie mit der rechten Maustaste auf **Server-Farmen** in der linken Verzeichnisstruktur und wählen Sie **Server-Farm erstellen** aus.
   b) Benennen Sie die neue Server-Farm. Beispiel: `ca_servers`.
   c) Führen Sie für jeden Cognos Analytics-Server folgende Schritte aus:
      - Geben Sie die Serveradresse ein. Beispiel: `ca-host1`.
      - Klicken Sie auf **Erweiterte Einstellungen** und erweitern Sie **applicationRequestRouting**. Legen Sie den `httpPort` bzw. `httpsPort` (falls Sie HTTPS verwenden) fest. Beispiel: `9300`.
   d) Klicken Sie auf **Fertigstellen**.
   e) Klicken Sie auf **Nein**, wenn Sie angewiesen werden, das Erstellen einer Regel für das Umschreiben (Rewrite) durch den IIS-Manager zuzulassen.
   f) Wählen Sie die Server-Farm in der linken Verzeichnisstruktur aus und klicken Sie doppelt auf **Serveraffinität**.
   g) Wählen Sie das Kontrollkästchen **Clientaffinität** aus.
   h) Klicken Sie auf **Anwenden**.
   i) Wählen Sie die Server-Farm in der linken Verzeichnisstruktur aus und klicken Sie doppelt auf **Caching**.
   j) Ändern Sie **Abfragezeichenfolgenunterstützung** in **Abfragezeichenfolge einbeziehen**.
   k) Klicken Sie auf **Anwenden**.
   l) Wählen Sie die Server-Farm in der linken Verzeichnisstruktur aus und klicken Sie doppelt auf **Statustest**.
   m) Geben Sie im Abschnitt **URL-Test** die URL ein: `http://ca_servers/bi/v1/ping`.
   n) Klicken Sie auf **Anwenden**.
   o) Wählen Sie die Server-Farm in der linken Verzeichnisstruktur aus und klicken Sie doppelt auf **Proxy**.
   p) Ändern Sie im Feld **Zeitlimit (Sekunden)** den Wert in `120`.
   q) Klicken Sie auf **Anwenden**.
4. Klicken Sie mit der rechten Maustaste auf **Standardwebsite** und anschließend auf **Anwendung hinzufügen**.
   - Der Aliasname ist `ibmcognos`.
   - Bei dem Anwendungspool handelt es sich um den in Schritt 1 erstellten.
   - Der physische Pfad ist *`Installationsposition`*`\webcontent`.
   a) Aktivieren Sie das Ablaufdatum für Webinhalte.
      i) Wählen Sie `ibmcognos` aus und klicken Sie doppelt auf **HTTP-Antwortheader**.
      ii) Klicken Sie auf **Gemeinsam genutzte Header festlegen**.
      iii) Wählen Sie **Ablauf des Webinhalts** aus und legen Sie ein geeignetes Ablaufdatum fest.
   b) Wählen Sie `ibmcognos` aus und doppelklicken Sie auf **MIME-Typen**.

      Fügen Sie folgende MIME-Typen zu Ihrer IIS-Konfiguration hinzu, falls sie noch nicht vorhanden sind.
      - `.svg : image/svg+xml`
      - `.woff : application/x-font-woff`
      - `.json : application/json`
      - `.woff2 : font/woff2`
      - `.template : text/html`

- `.txt : text/plain`

5. Wenn Sie Single Sign-on zwischen IIS und Cognos Analytics konfigurieren, klicken Sie mit der rechten Maustaste auf `ibmcognos` und klicken Sie dann auf **Anwendung hinzufügen**.
   - Legen Sie für **Alias** `sso` fest.
   - Bei dem **Anwendungspool** handelt es sich um den in Schritt 1 erstellten.
   - Der **physische Pfad** ist *`Installationsposition`*`\cgi-bin`.

   a) Wählen Sie **sso** aus und klicken Sie doppelt auf **Handlerzuordnungen**.

   b) Klicken Sie auf **Modulzuordnung hinzufügen** im Aktionsfenster auf der rechten Seite.
      - Der Anforderungspfad ist `cisapi`.
      - Das Modul ist **IsapiModule**.
      - Die ausführbare Datei ist `install_location\cgi-bin\cognosisapi.dll`.
      - Der Name ist `Cognos SSO`.
      - Klicken Sie auf die Anforderungseinschränkungen und stellen Sie sicher, dass **Handler aufrufen** nicht markiert ist.
      - Klicken Sie zweimal auf **OK**.
      - Klicken Sie im Dialogfeld **Scriptzuordnung bearbeiten** auf **Ja**.
      - Wählen Sie **sso** aus und klicken Sie doppelt auf **Module**. Falls "WebDAVModule" in der Liste angezeigt wird, entfernen Sie das Modul.

6. Erstellen Sie URL-Umschreibungsregeln für die Zuordnung von Anforderungen zu den korrekten Handlern.

   a) Klicken Sie auf das Verzeichnis `bi` unter **ibmcognos**.

   b) Doppelklicken Sie auf **URL-Rewrite**.

   c) Fügen Sie eine Servervariable zur Identifizierung der Cognos Analytics-Position hinzu, indem Sie auf **Servervariablen anzeigen** klicken.
      - Klicken Sie auf **Hinzufügen**.
      - Benennen Sie die Variable `HTTP_X_BI_PATH`.
      - Kehren Sie zu den Regeln zurück.
      - Klicken Sie auf die Option zum Anzeigen von Servervariablen.
      - Klicken Sie auf **Hinzufügen**.
      - Benennen Sie die Variable `HTTP_X_WEBCONTENTROOT`.
      - Kehren Sie zu den Regeln zurück.
      - Klicken Sie auf die Option zum Anzeigen von Servervariablen.
      - Klicken Sie auf **Hinzufügen**.
      - Benennen Sie die Variable `HTTP_X_FORWARDED_HOST`.
      - Kehren Sie zu den Regeln zurück.

   d) Wenn Sie Cognos Analytics for Jupyter Notebook Server integrieren möchten, müssen Sie eine Regel hinzufügen, die WebSocket-Anforderungen von IBM Cognos Analytics-Notebooks dem Back-End-Server für Jupyter-Notebook zuordnet.

      Weitere Informationen finden Sie im Abschnitt Kapitel 6, „Installation von IBM Cognos Analytics for Jupyter Notebook Server", auf Seite 39.

      Wichtig: Für diese Schritte wird das WebSocket-Protokoll verwendet, das nur in IIS-Versionen 8.0 und höher verfügbar ist.

      i) Stellen Sie sicher, dass IIS Version 8.0 oder höher installiert ist.

      ii) Installieren Sie die WebSocket-Protokollunterstützung in IIS.

Weitere Informationen finden Sie im Abschnitt WebSocket <webSocket> (https://docs.microsoft.com/en-us/iis/configuration/system.webserver/web socket).

iii) Klicken Sie auf das Verzeichnis **bi**, das sich unter dem in Schritt 4 erstellten Alias **ibmcognos** befindet.

iv) Klicken Sie auf **Regeln hinzufügen** > **Eingehende Regeln** > **Leere Regel**.

- Falls die Proxys noch nicht aktiviert sind, werden Sie dazu aufgefordert, sie zu aktivieren. Klicken Sie auf **OK**.
- Der Servername und -port wird in der Datei `config.conf` definiert, wenn Sie Jupyter Notebook Server konfigurieren.

Wählen Sie die neu erstellte Regel aus und klicken Sie auf **Bearbeiten**.

- Das Muster ist `v1/jupyter/(user/[^/]*)/(api/kernels/[^/]+/channels)`
- Der Aktionstyp ist **Rewrite**.
- Die Rewrite-URL (für die SSL-Konfiguration) lautet `https://`*`jupyter_host_name`*`:`*`jupyter_host_port`*`/bi/v1/jupyter/{R:1}/{R:2}`

  Verwenden Sie für Konfigurationen, bei denen es sich nicht um SSL-Konfigurationen handelt, die folgende Rewrite-URL: `http://`*`jupyter_host_name`*`:`*`jupyter_host_port`*`/bi/v1/jupyter/{R:1}/{R:2}`
- Aktivieren Sie die Option **Abfragezeichenfolge anhängen**.
- Aktivieren Sie die Option für das Stoppen der Verarbeitung nachfolgender Regeln.
- Klicken Sie auf **Anwenden** und kehren Sie zu den Regeln zurück.

e) Wählen Sie das Verzeichnis `bi` unter **ibmcognos** erneut aus.

f) Fügen Sie eine Regel hinzu, mit der die Cognos Analytics-Position an die `ca-host`-Maschinen gesendet wird, indem Sie auf **Regeln hinzufügen** > **Eingehende Regeln** > **Leere Regel** klicken.

- Der Name ist `Headers`.
- Das Muster ist `(.*)`.
- Der Aktionstyp ist **none**.
- Erweitern Sie **Servervariablen** und gehen Sie wie folgt vor:
  - Klicken Sie auf **Hinzufügen**. Wählen Sie `HTTP_X_BI_PATH` aus und legen Sie `/ibmcognos/bi/v1` als Wert fest.
  - Klicken Sie auf **Hinzufügen**. Wählen Sie `HTTP_X_FORWARDED_HOST` aus und legen Sie `{HTTP_HOST}` als Wert fest.
  - Klicken Sie auf **Hinzufügen**. Wählen Sie `HTTP_X_WEBCONTENTROOT` aus und legen Sie `/ibmcognos` als Wert fest.
- Wählen Sie die Option für das Stoppen der Verarbeitung nachfolgender Regeln ab. .
- Klicken Sie auf **Anwenden** und kehren Sie zu den Regeln zurück.

g) Wenn Sie die SSO-Anwendung in einem vorherigen Schritt konfiguriert haben, fügen Sie Regeln hinzu, mit denen Anmeldeanforderungen und UI-Serviceanforderungen einer älteren Version dem SSO-Handler zugeordnet werden.

i) Klicken Sie auf **Regeln hinzufügen** > **Eingehende Regeln** > **Leere Regel**.

- Der Name ist `SSO  Login`.
- Das Muster ist `v1/login$`
- Der Aktionstyp ist **Rewrite**.
- Die Rewrite-URL lautet `/ibmcognos/sso/cisapi/bi/v1/login`.
- Aktivieren Sie die Option für das Stoppen der Verarbeitung nachfolgender Regeln.
- Klicken Sie auf **Anwenden** und kehren Sie zu den Regeln zurück.

ii) Klicken Sie auf **Regeln hinzufügen** > **Eingehende Regeln** > **Leere Regel**.

- Der Name ist `Legacy SSO`.
- Das Muster ist `(v1/disp(/.*)?)`
- Der Aktionstyp ist **Rewrite**.
- Die Rewrite-URL ist `/ibmcognos/sso/cisapi/bi/{R:1}`
- Aktivieren Sie die Option für das Stoppen der Verarbeitung nachfolgender Regeln.
- Klicken Sie auf **Anwenden** und kehren Sie zu den Regeln zurück.

h) Fügen Sie eine Regel hinzu, mit der Cognos Analytics-REST-Serviceanforderungen den Cognos Analytics-Back-End-Servern zugeordnet werden.

i) Klicken Sie auf **Regeln hinzufügen** > **Eingehende und ausgehende Regeln** > **Reverse Proxy**.

- Falls die Proxys noch nicht aktiviert sind, werden Sie dazu aufgefordert, sie zu aktivieren. Klicken Sie auf **OK**.
- Der Servername ist `ca-host:9300/bi`.

  - oder - wenn Sie eine Server-Farm konfiguriert haben - `http://ca_servers/bi`

  Wählen Sie die neu erstellte Regel aus und klicken Sie auf **Bearbeiten**.
- Das Muster ist `(^$)|(^v1(/.*)?)|(^[^/]+\.jsp)|(^login$)`
- Der Aktionstyp ist **Rewrite**.
- Die Rewrite-URL ist `http://ca-host:9300/bi/{R:0}`

  oder - wenn Sie eine Server-Farm konfiguriert haben - `http://ca_servers/bi/{R:0}`
- Aktivieren Sie die Option für das Stoppen der Verarbeitung nachfolgender Regeln.
- Klicken Sie auf **Anwenden** und kehren Sie zu den Regeln zurück.

ii) Klicken Sie auf **Regeln hinzufügen** > **Eingehende Regeln** > **Leere Regel**.

- Der Name ist `Event Studio`.
- Das Muster ist `^(ags|cr1|prompting|ccl|common|skins|ps|cps4)/(.*)`
- Öffnen Sie den Abschnitt **Bedingungen**.
- Ändern Sie die Option **Logische Gruppierung** in **Beliebige Übereinstimmung**.
- Klicken Sie auf **Hinzufügen**.
  - Die Eingabe für **Bedingung** ist `{HTTP_REFERER}`.
  - Für die Option zum Überprüfen der Eingabezeichenfolge muss `Entspricht dem Muster` ausgewählt sein.
  - Das Muster ist `v1/disp`.
  - Wählen Sie **Groß-/Kleinschreibung ignorieren** aus.
- Klicken Sie auf **Hinzufügen**
  - Die Eingabe für **Bedingung** ist `{HTTP_REFERER}`.
  - Für die Option zum Überprüfen der Eingabezeichenfolge muss `Entspricht dem Muster` ausgewählt sein.
  - Das Muster ist `(ags|cr1|prompting|ccl|common|skins|ps|cps4)/(.*)\.css`
  - Wählen Sie **Groß-/Kleinschreibung ignorieren** aus.
- Der Aktionstyp ist **Rewrite**.
- Die Rewrite-URL ist `/ibmcognos/{R:0}`.
- Aktivieren Sie die Option für das Stoppen der Verarbeitung nachfolgender Regeln.
- Klicken Sie auf **Anwenden** und kehren Sie zu den Regeln zurück.

iii) Klicken Sie auf die Optionen für **Regeln hinzufügen** > **Eingehende Regeln** > **Leere Regel**

- Der Name ist `Report Viewer`

- Das Muster ist `^rv/(.*)`
- Der Aktionstyp ist **Rewrite**.
- Die Rewrite-URL ist `/ibmcognos/{R:0}`.
- Aktivieren Sie die Option für das Stoppen der Verarbeitung nachfolgender Regeln.
- Klicken Sie auf **Anwenden** und kehren Sie zu den Regeln zurück.

i) Fügen Sie eine Regel hinzu, die das Laden von Cognos Analytics-Seiten ohne abschließenden Schrägstrich in der URL ermöglicht.

i) Klicken Sie auf den Aliasnamen **ibmcognos**.

ii) Klicken Sie doppelt auf **URL Rewrite**.

iii) Klicken Sie auf die Optionen für **Regeln hinzufügen** > **Eingehende Regeln** > **Leere Regel**

- Der Name ist `Add Trailing Slash`.
- Das Muster ist `^bi$`.
- Der Aktionstyp ist **Redirect**.
- Die Weiterleitungs-URL ist `{R:0}/`.
- Aktivieren Sie die Option **Abfragezeichenfolge anhängen**.
- Der Weiterleitungstyp ist **Permanent (301)**.
- Klicken Sie auf **Anwenden** und kehren Sie zu den Regeln zurück.

7. Passen Sie die Grenzwerte für die Anforderungsgröße an.

a) Wählen Sie das Verzeichnis `bi` unter der zuvor erstellten Anwendung **ibmcognos** aus.

b) Doppelklicken Sie auf **Filterung anfordern**.

c) Klicken Sie auf **Funktionseinstellungen bearbeiten...** in der rechten Anzeige.

- Legen Sie für **Maximale URL-Länge (Byte)** den Wert 8192 fest.
- Legen Sie für **Maximale Abfragezeichenfolge (Byte)** den Wert 8192 fest.
- Klicken Sie auf **OK**.

d) Doppelklicken Sie auf **Filterung anfordern**.

e) Wählen Sie die Registerkarte **Header** aus und klicken Sie auf **Header hinzufügen**.

f) Geben Sie im Feld **Header** den Headerfeldnamen `Referrer` ein.

g) Geben Sie im Feld **Größenbeschränkung** den Wert 8192 ein.

h) Klicken Sie auf **OK**.

i) Wiederholen Sie den Vorgang für den Headerfeldnamen `Cookie` mit der **Größenbeschränkung** 4096.

j) Klicken Sie auf **OK**.

k) Klicken Sie auf das virtuelle Verzeichnis **ibmcognos**.

l) Klicken Sie im Abschnitt **Verwaltung** der Startansicht doppelt auf **Konfigurationseditor**.

m) Erweitern Sie in der Dropdown-Liste **Abschnitt** den Eintrag **system.web** und wählen Sie **httpRuntime** aus.

n) Legen Sie für die Eigenschaft **maxQueryStringLength** den Wert 8192 fest.

o) Wenden Sie die Konfigurationsänderung an.

8. Konfigurieren Sie IIS, um ein Passieren der angepassten 441 Fehler zu ermöglichen, die für behebbare Ausnahmen von CAM verwendet werden. IIS kann andernfalls diese Fehler blockieren und dem Kunden wird beim Anmeldeversuch ein Fehlertext mit der Information angezeigt, dass die Antwort auf die Anmeldung ungültig war.

a) Klicken Sie auf das virtuelle Verzeichnis `ibmcognos`.

b) Klicken Sie in der Startansicht im Abschnitt für das **Verwaltung** doppelt auf die Option für **Konfigurationseditor**.

c) Erweitern Sie in der Dropdown-Liste **Abschnitt** den Eintrag **system.webServer** und wählen Sie **httpErrors** aus.

d) Legen Sie für die Eigenschaft **existingResponse** die Einstellung **PassThrough**.

e) Wenden Sie die Konfigurationsänderung an.

9. Wenn Sie die SSO-Anwendung in einem vorherigen Schritt konfiguriert haben, aktivieren Sie die Option für die **Windows-Authentifizierung**.

a) Wählen Sie die SSO-Anwendung aus. Wählen Sie für den Browser Microsoft Edge die Anwendung `ibmcognos` aus.

b) Klicken Sie doppelt auf **Authentifizierung**. Wählen Sie die **Anonyme Authentifizierung** ab und aktivieren Sie die Option für die **Windows-Authentifizierung**.

Cognos Analytics sollte nun unter der Adresse `http://iis-host/ibmcognos` verfügbar sein.

Anmerkung: Wenn Sie einen Ordner für ein virtuelles Verzeichnis mit mehreren Ebenen oberhalb der Anwendung 'ibmcognos' konfiguriert haben, z. B. 'Default Web Site > MyVirtualDirectoryFolder > ibmcognos', verwenden Sie '/MyVirtualDirectoryFolder/ibmcognos' anstelle von '/ibmcognos' in den URL-Rewrite-Regeln, die Sie in Schritt 6 erstellt haben.

Konfigurieren des CGI-Gateways in IIS Version 7 oder neueren Versionen

Wenn Sie Microsoft Internet Information Services (IIS) Version 7 oder höher verwenden, konfigurieren Sie das CGI-Gateway. Dies ist für Single Sign-on erforderlich.

Das CGI-Gateway ist für 32-Bit- und für 64-Bit-Web-Server verfügbar.

Informationen zu diesem Vorgang

Wenn Sie Microsoft IIS als Web-Server verwenden und mehr als ein IBM Cognos Analytics-Produkt oder mehrere Instanzen desselben Produkts auf einem Computer ausführen möchten, müssen Sie einen separaten Anwendungspool für jedes Produkt bzw. jede Instanz erstellen und dann die Aliasse für das Produkt oder die Instanz dem Anwendungspool zuordnen.

Weitere Informationen zur Erstellung eines Anwendungspools finden Sie in der Dokumentation zum Web-Server.

Vorgehensweise

1. Installieren Sie die ARR-Erweiterung (ARR, Application Request Routing) für IIS.

a) Installieren Sie die ARR-Erweiterung für IIS, indem Sie die folgende URL aufrufen:
http://www.iis.net/downloads/microsoft/application-request-routing

b) Klicken Sie nach dem Öffnen der Microsoft-Webseite auf die grüne Schaltfläche mit der Beschriftung **Install this extension**.

Folgen Sie den Anweisungen zum Herunterladen und Ausführen der ARR-Erweiterung.

c) Um sicherzustellen, dass die ARR-Erweiterung erfolgreich installiert wurde, rufen Sie den IIS-Manager im Windows-Menü **Start\Verwaltung** auf. Klicken Sie nach dem Starten des IIS-Managers auf den Servernamen in der linken oberen Ecke der Anzeige, um die verfügbaren Features anzuzeigen. Im mittleren IIS-Bereich sollte nun das **URL-Rewrite**-Feature sichtbar sein. Es wird installiert, wenn ARR installiert wird.

2. Klicken Sie in Microsoft Windows in der **Systemsteuerung** auf **Programme** > **Programme und Funktionen**.

In Microsoft Windows 8 oder 2012 Server befindet sich der Link **Programme und Funktionen** direkt in der **Systemsteuerung**.

3. Klicken Sie auf **Windows-Funktionen aktivieren oder deaktivieren**.
4. Wenn Sie Microsoft Windows 2008 Server verwenden, gehen Sie folgendermaßen vor:

a) Klicken Sie auf **Server-Manager** > **Rollen** > **Webserver (IIS)**.

b) Stellen Sie sicher, dass **Common HTTP Features** (Allgemeine HTTP-Funktionen) bzw. nur die benötigten Funktionen aktiviert sind.

c) Wenn die Option **CGI** auf **Not installed** festgelegt ist, wählen Sie **CGI** aus und klicken Sie dann auf **Add Role Service**.

5. Wenn Sie Microsoft Windows 2012 Server verwenden, gehen Sie folgendermaßen vor:
   a) Klicken Sie im Assistenten zum Hinzufügen von Rollen und Funktionen auf **Role-based or feature-based installation** (Rollen- oder funktionsbasierte Installation) und danach auf **Weiter**.
   b) Wählen Sie Ihren Server aus und klicken Sie auf **Weiter**.
   c) Wählen Sie **Webserver (IIS)** aus (sofern noch nicht installiert), stellen Sie sicher, dass **Common HTTP Features** (Allgemeine HTTP-Funktionen) aktiviert ist, und klicken Sie so oft auf **Weiter**, bis Sie zum Abschnitt **Role Services** (Rollendienste) des Assistenten gelangen.
   d) Erweitern Sie **Application Development** (Anwendungsentwicklung).
   e) Wählen Sie **CGI**, sofern noch nicht ausgewählt, und klicken Sie auf **Weiter**.
   f) Klicken Sie auf **Installieren**.
6. Wenn Sie Microsoft Windows 7 oder 8 verwenden, gehen Sie folgendermaßen vor:
   a) Wählen Sie **Internet Information Services**, sofern noch nicht ausgewählt.
   b) Erweitern Sie **Internet Information Services** > **World Wide Web Services** (WWW-Dienste).
   c) Stellen Sie sicher, dass **Common HTTP Features** (Allgemeine HTTP-Funktionen) bzw. nur die benötigten Funktionen aktiviert sind.
   d) Erweitern Sie **Application Development Features** (Anwendungsentwicklungsfunktionen).
   e) Wenn **CGI** nicht ausgewählt ist, aktivieren Sie das Kontrollkästchen.
   f) Klicken Sie auf **OK**.
7. Wählen Sie in der Konsole von Internet Information Services (IIS) Manager unter **Connections** Ihren Servernamen aus.
   - Wenn Sie Microsoft Windows 2012 Server verwenden, wählen Sie in **Server-Manager IIS** aus, klicken Sie mit der rechten Maustaste auf den Namen Ihres Servers und wählen Sie **Internet Information Services (IIS) Manager** aus.
   - Wenn Sie Microsoft Windows 2008 Server verwenden, erweitern Sie in **Server-Manager** die Knoten **Rollen** > **Webserver (IIS)** und klicken Sie dann auf **Internet Information Services (IIS) Manager**.
   - Wenn Sie Microsoft Windows 8 verwenden, klicken Sie in der **Systemsteuerung** auf **Verwaltung**, um auf die **Internet Information Services (IIS) Manager**-Konsole zuzugreifen.
   - Wenn Sie Microsoft Windows 7 verwenden, klicken Sie in der **Systemsteuerung** auf **System und Sicherheit** > **Verwaltung**, um auf die **Internet Information Services (IIS) Manager**-Konsole zuzugreifen.
8. Klicken Sie doppelt auf **ISAPI and CGI Restrictions** (ISAPI- und CGI-Einschränkungen).
9. Klicken Sie unter **Aktionen** auf **Hinzufügen**.
10. Geben Sie den Pfad zur Datei `cognos.cgi` ein. Die Datei befindet sich im Verzeichnis *installationsposition*`\cgi-bin`.

    Sie müssen den vollständigen Pfad und den Dateinamen eingeben. Wenn der Pfad Leerzeichen enthält, stellen Sie sicher, dass Sie den Pfad in Anführungszeichen einschließen. Beispiel:

    `"C:\Programme\ibm\cognos\analytics\cgi-bin\cognos.cgi"`
11. Geben Sie eine **Beschreibung** ein, beispielsweise `CognosCGI`.
12. Wählen Sie **Ausführung des Erweiterungspfads zulassen** aus und klicken Sie auf **OK**.
13. Erweitern Sie unter **Connections** (Verbindungen) den Eintrag **Sites** und fügen Sie unter Ihrer Website die virtuellen Verzeichnisse aus der nachfolgenden Tabelle hinzu:

Tabelle 18. Erforderliche virtuelle Verzeichnisse	
Alias	**Position**
ibmcognos	*installationsposition*/webcontent
ibmcognos/cgi-bin	*installationsposition*/cgi-bin

Wichtig: In IBM Cognos Configuration ist bi der Standardwert für **Gateway-URI** und **Steuerungs-URI für Gateway**. Wenn Sie als Alias einen anderen Wert als bi verwenden, müssen Sie die Werte für **Gateway-URI** und **Steuerungs-URI für Gateway** entsprechend anpassen.

14. Wählen Sie das von Ihnen erstellte virtuelle Verzeichnis "cgi-bin" aus.
15. Klicken Sie doppelt auf **Handlerzuordnungen**.
16. Klicken Sie unter **Aktionen** auf **Modulzuordnung hinzufügen**.
    a) Geben Sie für **Anforderungspfad** die Bezeichnung cognos.cgi ein.
    b) Wählen Sie für **Modul** den Eintrag CgiModule aus.
    c) Lassen Sie das Feld **Ausführbare Datei (optional)** leer.
    d) Geben Sie unter **Name** einen Namen für den Eintrag ein, beispielsweise CognosCGI.
    e) Klicken Sie auf **OK**.
17. Konfigurieren Sie den Reverse Proxy.

    Diese Prozedur enthält die Schritte, die erforderlich sind, um den Reverse Proxy entsprechend einzurichten, dass IIS die Gateway-Anforderungen neu schreiben und an die Anwendungsebene weiterleiten kann. Für diese Schritte wird eine Architektur mit zwei Servern vorausgesetzt, bei der das IBM Cognos Analytics-Gateway auf Server1_Gateway und die IBM Cognos Analytics-Anwendung auf Server2_Application installiert ist.

    a) Starten Sie auf dem Server Server1_Gateway den IIS-Manager und wählen Sie den Ordner "**bi**" im zuvor eingerichteten virtuellen Verzeichnis ibmcognos aus.
    b) Starten Sie in der Ansicht "Features" das Feature **URL-Rewrite**.
    c) Klicken Sie im Bereich **Aktionen** auf **Regel hinzufügen** und wählen Sie anschließend **Reverse Proxy** aus. Klicken Sie auf **OK**.
    d) Füllen Sie im Dialogfeld zum Hinzufügen von Reverse Proxy-Regeln im Abschnitt für eingehende Regeln das Feld zur Eingabe des Servernamens oder der IP-Adresse im folgenden Format aus. *<Server2_Application:Port>*/bi. Beispiel: Server2_Application:9300/bi
    e) Stellen Sie sicher, dass das Kontrollkästchen zum Aktivieren von SSL-Auslagerung ausgewählt ist, und klicken Sie anschließend auf **OK**.
    f) Klicken Sie auf der Seite **Regeln** im Bereich **Aktion** auf die Option zum Anzeigen von Servervariablen.
    g) Klicken Sie auf **Hinzufügen** und fügen Sie eine Variable mit dem Namen HTTP_X_BI_PATH hinzu. Klicken Sie danach auf **OK**, um die Variable zu erstellen.
    h) Klicken Sie im Bereich **Aktionen** auf die Option zum Zurückkehren zu den Regeln.
    i) Wählen Sie die zuvor erstellte Regel aus und klicken Sie rechts im Bereich für eingehende Regeln auf **Bearbeiten**
    j) Erweitern Sie den Abschnitt **Servervariablen**.
    k) Klicken Sie im Abschnitt **Servervariablen** auf die Schaltfläche **Hinzufügen**.
    l) Wählen Sie im Dialogfeld zum Festlegen von Servervariablen die Servervariable **HTTP_X_BI_PATH** aus und legen Sie für das Feld **Wert** den Wert /ibmcognos/bi/v1 fest.
    m) Stellen Sie sicher, dass das Kontrollkästchen zum Ersetzen des bestehenden Werts ausgewählt ist.
    n) Klicken Sie auf **OK** zum Speichern und anschließend im Bereich **Aktion** auf **Anwenden**.

o) Klicken Sie im Bereich **Aktion** in der rechten oberen Ecke auf die Option zum Zurückkehren zu den Regeln, um das Definieren der Regel zu Beenden.

p) Testen Sie die Konfiguration, indem Sie das folgende URL-Muster über einen Browser eingeben: `http(s)://<web_server>:<web_server_port>/<alias>/bi/`. Im vorliegenden Beispiel lautet die URL folgendermaßen: `http://Server1_Gateway:80/ibmcognos/bi/`

Ergebnisse

Benutzer können auf das CGI-Gateway zugreifen, indem sie `http://servername/ibmcognos/bi/` in ihren Web-Browsern eingeben.

Konfigurieren des Gateways und Web-Servers für die Verwendung bestimmter Namespaces

Sie können IBM Cognos Analytics so konfigurieren, dass der Gateway-Namespace mit allen unterstützten Web-Servern verwendet wird, oder Sie können einen bestimmten Namespace für jeden Web-Server konfigurieren.

Abhängig von Ihren Konfigurationsanforderungen können Sie die Namespaces auf folgende Weise konfigurieren:

- Geben Sie den Gateway-Namespace in IBM Cognos Configuration an.

  Diese Option kann für Namespaces verwendet werden, die für Single Sign-on (SSO) konfiguriert sind, und gilt für alle unterstützten Web-Server. Weitere Informationen finden Sie im Abschnitt „Konfigurieren eines Gateway-Namespace" auf Seite 148.

- Fügen Sie einen HTTP-Header zur Web-Server-Konfiguration hinzu.

  Diese Option kann für Namespaces verwendet werden, die für Single Sign-on (SSO) konfiguriert sind oder die für Single Sign-on (SSO) konfiguriert sind. Die Konfigurationsschritte sind bei allen Web-Servern unterschiedlich. Weitere Informationen finden Sie unter „Konfigurieren eines Namespace, der mit IIS verwendet werden soll" auf Seite 147 und „Konfigurieren eines Namespace, der mit Apache oder IBM HTTP Server verwendet werden soll " auf Seite 148.

Konfigurieren eines Namespace, der mit IIS verwendet werden soll

Sie können einen bestimmten Cognos Analytics-Namespace konfigurieren, der mit Microsoft Internet Information Services (IIS) verwendet werden soll.

Informationen zu diesem Vorgang

Diese Option kann bei Namespaces verwendet werden, die für Single Sign-on (SSO) konfiguriert sind oder die für Single Sign-on (SSO) konfiguriert sind.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Konfigurieren von IIS in Cognos Analytics" auf Seite 138 aus, um IIS mit IBM Cognos Analytics zu konfigurieren.
2. Fügen Sie einen HTTP-Header mit dem Namen **HTTP_CAM_Namespace** hinzu, indem Sie die folgenden Schritte ausführen:
   a) Klicken Sie auf das Verzeichnis `bi` unter `ibmcognos`.
   b) Doppelklicken Sie auf **URL-Rewrite**.
   c) Klicken Sie auf **Servervariablen anzeigen** und fügen Sie eine Servervariable mit dem Namen **HTTP_CAM_Namespace** wie folgt hinzu:
      - Klicken Sie auf **Hinzufügen**.
      - Geben Sie der Variablen den Namen **HTTP_CAM_Namespace**.

- Kehren Sie zu den Regeln zurück.

d) Klicken Sie auf die Regel für das Umschreiben mit dem Namen **Header** und klicken Sie auf **Bearbeiten**.

e) Erweitern Sie **Servervariablen** und klicken Sie auf **Hinzufügen**.

- Klicken Sie auf **Hinzufügen**.
- Wählen Sie **HTTP_CAM_Namespace** aus und setzen Sie den Wert auf die in IBM Cognos Configuration angegebene **Namespace-ID** des Namespace, den Sie verwenden möchten.
- Klicken Sie auf **Anwenden** und kehren Sie zu den Regeln zurück.

3. Starten Sie IIS erneut.

Konfigurieren eines Namespace, der mit Apache oder IBM HTTP Server verwendet werden soll

Sie können einen bestimmten Cognos Analytics-Namespace konfigurieren, der mit Apache HTTP Server oder IBM HTTP Server verwendet werden soll.

Informationen zu diesem Vorgang

Diese Option kann bei Namespaces verwendet werden, die für Single Sign-on (SSO) konfiguriert sind oder die für Single Sign-on (SSO) konfiguriert sind.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Konfigurieren von Apache HTTP Server oder IBM HTTP Server für Cognos Analytics" auf Seite 133 aus, um Apache HTTP Server oder IBM HTTP Server mit IBM Cognos Analytics zu konfigurieren.
2. Fügen Sie einen HTTP-Header mit dem Namen **`CAM-Namespace`** hinzu, indem Sie die folgenden Schritte ausführen:

   a) Öffnen Sie die Datei `cognos.conf`, die Sie in Schritt 1 konfiguriert haben, in einem Texteditor.

   b) Fügen Sie für den Parameter `Location` den Parameter `RequestHeader` mit dem Namen **`CAM-Namespace`** hinzu und setzen Sie den Wert auf die in IBM Cognos Configuration angegebene **Namespace-ID** des Namespace, den Sie verwenden möchten.

```
# Definition der Cognos-Position
<Location /ibmcognos>
    RequestHeader set X-BI-PATH /ibmcognos/bi/v1
    RequestHeader set CAM-Namespace Ihre_Namespace-ID
</Location>
```

   c) Speichern Sie die Datei `cognos.conf` und starten Sie den Web-Server erneut.

Konfigurieren eines Gateway-Namespace

Wenn IBM Cognos Analytics-Komponenten mehrere Namespaces verwenden bzw. wenn der anonyme Zugriff aktiviert ist und Cognos Analytics-Komponenten einen einzelnen Namespace verwenden, können Sie das Gateway so konfigurieren, dass eine Verbindung zu einem Namespace hergestellt wird.

Benutzer, die bei dem Web-Server angemeldet sind, auf dem sich das Gateway befindet, werden nicht zur Auswahl einer Authentifizierungsquelle aufgefordert. Wenn Sie über zwei Web-Server verfügen, können Sie jeden Web-Server für die Verwendung eines anderen Namespace konfigurieren.

Informationen zu diesem Vorgang

Diese Option kann bei Namespaces verwendet werden, die für Single Sign-on (SSO) konfiguriert sind, und gilt für alle unterstützten Web-Server.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Computer, auf dem das IBM Cognos Analytics-Gateway installiert ist.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Geben Sie im Fenster **Eigenschaften** für die Eigenschaft **Gateway-Namespace** die **Namespace-ID** des Namespace ein, den Sie als **Wert** für diese Eigenschaft verwenden wollen.
4. Klicken Sie im Menü **Datei** auf **Speichern**.
5. Starten Sie den Web-Server erneut.

Gateway testen

Sie können die Installation mithilfe eines Web-Browsers testen.

Vorgehensweise

1. Stellen Sie sicher, dass Ihr Web-Server ausgeführt wird.
2. Öffnen Sie einen Web-Browser.
3. Geben Sie in das Adressfeld den **Gateway-URI** über IBM Cognos Configuration ein. Zum Beispiel

   `http://`*`Hostname:Port`*`/ibmcognos`

   Die Seite **Willkommen** des IBM Cognos Analytics-Portals wird angezeigt.

Kapitel 11. Konfigurieren von optionalen Modellierungskomponenten

Nach erfolgter Installation und Konfiguration der IBM Cognos Analytics-Serverkomponenten können Sie IBM Cognos Framework Manager, die Modellierungskomponente für die Berichterstellung, und IBM Cognos Transformer, das Modellierungstool für die Erstellung von PowerCubes installieren und konfigurieren.

Installieren Sie Framework Manager und Transformer jeweils an einer anderen Position als Cognos Analytics.

IBM Cognos Framework Manager

IBM Cognos Framework Manager ist das Metadatenmodellierungstool für IBM Cognos Analytics.

Framework Manager kann auf demselben Computer wie andere IBM Cognos Analytics-Komponenten installiert werden oder auf einem separaten Computer.

Wenn Sie von einer älteren Version von Framework Manager aktualisiert haben, können Sie dieselben Modelle und Projekte wie in der vorhergehenden Version verwenden. Um vorhandene Projekte zu aktualisieren, müssen Sie sie in der neuen Version von Framework Manager öffnen.

Wenn Sie Framework Manager von einer älteren Version aktualisieren, müssen Sie zuerst die ältere Framework Manager-Version deinstallieren. Weitere Informationen finden Sie in Kapitel 16, „Deinstallieren von IBM Cognos Analytics”, auf Seite 313.

Schließen Sie vor der Installation von Framework Manager alle aktuell ausgeführten Programme, um sicherzustellen, dass das Installationsprogramm alle erforderlichen Dateien auf den Computer kopiert.

Stellen Sie außerdem sicher, dass Sie für den Windows-Computer, auf dem Sie die Installation durchführen, über Administratorberechtigungen verfügen. Wenn Sie nicht über Administrator-Berechtigungen verfügen, bitten Sie Ihren Systemadministrator, Sie zur Administratorgruppe auf Ihrem Computer hinzuzufügen. Für das Konto, das zur Ausführung von Framework Manager verwendet wird, sind außerdem Administratorrechte erforderlich.

Installieren und konfigurieren Sie alle IBM Cognos Analytics-Serverkomponenten, bevor Sie Framework Manager installieren.

Verwenden Sie als Installationsposition ein Verzeichnis, dessen Pfadname ausschließlich ASCII-Zeichen enthält. Einige Server unterstützen in Verzeichnisnamen nur ASCII-Zeichen. Wenn Framework Manager in einem Verzeichnis installiert wird, dessen Pfadname einen Apostroph enthält, lässt sich die Hilfe möglicherweise nicht ordnungsgemäß öffnen.

Die Konfiguration eines externen Quellcodeverwaltungssystems in Framework Manager erleichtert Ihnen die Verwaltung, die Freigabe und den Schutz unterschiedlicher Metadatenversionen. Weitere Informationen finden Sie im Abschnitt über die Verwendung der externen Repository-Steuerung in der Veröffentlichung *IBM Cognos Framework Manager User Guide*.

Systemanforderungen für IBM Cognos Framework Manager

Stellen Sie vor der Installation von IBM Cognos Framework Manager sicher, Windows-Computer die Anforderungen von IBM Cognos Analytics an Software und Hardware erfüllt. Die Hardware-Komponenten, z. B. der Festplattenspeicherplatz, hängen von der Größe Ihres Modells ab.

In der folgenden Tabelle sind die Mindestanforderungen im Hinblick auf Hard- und Software aufgeführt, die zur Ausführung von Framework Manager erfüllt sein müssen.

Tabelle 19. Systemanforderungen für Framework Manager	
Anforderung	**Spezifikation**
Betriebssystem	Windows
RAM	Minimum: 512 MB Optimal: 1 GB
Plattenspeicherplatz	Mindestens erforderlicher Arbeitsspeicher: 500 MB freier Speicherbereich auf dem Laufwerk mit dem von Cognos Analytics verwendeten temporären Verzeichnis.
Datenbank	Wenn Sie den kompatiblen Abfragemodus (Compatible Query Mode, CQM) verwenden, muss die Datenbank-Client-Software auf demselben Computer wie Framework Manager installiert sein. Die Datenbankkonnektivität muss eingerichtet sein.
Internet Explorer 11	Microsoft Internet Explorer 11 muss auf demselben Computer wie Framework Manager installiert sein, selbst wenn Sie diesen Browser nicht verwenden. Internet Explorer 11 ist für die ordnungsgemäße Funktionsweise der Framework Manager-Funktionalität erforderlich. Sie können gleichzeitig andere unterstützte Browser in Verbindung mit Cognos Analytics verwenden.
Sonstige	Microsoft Data Access Component (MDAC) 2.6 oder neuere Versionen zur Verwendung mit Produktbeispielen.

Die Konfiguration eines externen Quellcodeverwaltungssystems in Framework Manager erleichtert Ihnen die Verwaltung, die Freigabe und den Schutz unterschiedlicher Metadatenversionen. Weitere Informationen finden Sie im Abschnitt über die Verwendung der externen Repository-Steuerung im Framework Manager *User Guide*.

Eine aktuelle Liste der Umgebungen, die von IBM Cognos Analytics-Produkten unterstützt werden, finden Sie auf der Seite mit den Kompatibilitätsberichten für IBM Softwareprodukte (www.ibm.com/support/pages/node/735235).

Installieren von IBM Cognos Framework Manager

Für eine vollständige Installation von IBM Cognos Analytics müssen Sie Cognos Framework Manager auf einem Windows-Computer installieren.

Für die Installation muss eine andere Position als die IBM Cognos Analytics-Installationsposition ausgewählt werden.

Vorgehensweise

1. Wechseln Sie zu der Position, an der die Installationsdateien heruntergeladen und extrahiert wurden, und klicken Sie doppelt auf die Datei `installer.exe`.
2. Verweisen Sie auf das entsprechende Repository und wählen Sie **IBM Cognos Analytics-Tools** und **IBM Cognos Framework Manager** aus.
3. Wählen Sie die für die Installation zu verwendende Sprache aus.

   Die von Ihnen ausgewählte Sprache bestimmt die Sprache der Benutzeroberfläche. Es werden alle unterstützten Sprachen installiert. Die Sprache der Benutzeroberfläche kann nach der Installation in eine der installierten Sprachen geändert werden.

4. Folgen Sie den Anweisungen im Installationsassistenten, um die erforderlichen Dateien auf Ihren Computer zu kopieren.
5. Schützen Sie das Installationsverzeichnis vor unbefugten Zugriffen.

Nächste Schritte

Für die Konfiguration werden Standardeinstellungen verwendet. Sie können diese Standardeinstellungen während der Installation oder zu einem späteren Zeitpunkt ändern, um sie für Ihre Umgebung zu optimieren.

Konfigurieren von IBM Cognos Framework Manager

Sie müssen IBM Cognos Framework Manager für die Kommunikation mit IBM Cognos Analytics und den zugehörigen Komponenten konfigurieren.

Vorbereitende Schritte

Installieren und konfigurieren Sie zunächst IBM Cognos Analytics, bevor Sie Framework Manager konfigurieren. Sie müssen zuerst Content Manager installieren und konfigurieren und den **IBM Cognos**-Service auf mindestens einem Content Manager-Computer starten. Dies gewährleistet, dass der Zertifizierungsstellenservice ein Zertifikat für den Framework Manager-Computer ausstellt.

Außerdem müssen Sie die Datenquellen konfigurieren, die Sie in Framework Manager-Projekten verwenden möchten.

Informationen zu diesem Vorgang

Wenn Sie Framework Manager auf demselben Computer wie IBM Cognos Analytics (in einem anderen Verzeichnis) installieren, ist keine Konfiguration erforderlich, wenn die folgenden Bedingungen zutreffen:

- Web-Server ist für die Verwendung der standardmäßigen virtuellen Verzeichnisse konfiguriert.
- Es werden Standardports und -ressourcen sowie kryptografische Standardeinstellungen verwendet.

Wenn Framework Manager außerhalb der Netzfirewall installiert ist, durch die die Komponenten der Anwendungsebene geschützt sind, können bei der Kommunikation mit dem Dispatcher Probleme auftreten. Um solche Probleme zu vermeiden, können Sie Framework Manager entweder mit den Komponenten der Anwendungsebene installieren oder ein Gateway installieren und konfigurieren, das für die Dispatcher-Kommunikation von Framework Manager dediziert ist. Weitere Informationen finden Sie im Abschnitt „Konfigurieren von Framework Manager innerhalb der Netzfirewall” auf Seite 154 oder „Konfigurieren von Framework Manager außerhalb der Netzfirewall” auf Seite 155.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Computer, auf dem Framework Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Geben Sie entsprechende Werte für die folgenden Einstellungen an:

   Gateway-URI
   Standardeinstellung: `http://CA-Server:Port/bi/v1/disp`

   Beispiel: `http://my_ca_server:9300/bi/v1/disp`

   Dieser URI muss stets mit dem URI für Cognos Analytics übereinstimmen.

   Enthält der URI die Angabe **localhost**, ersetzen Sie **localhost** durch einen vollständig qualifizierten Hostnamen oder eine IP-Adresse.

   Dispatcher-URI für externe Anwendungen
   Geben Sie den folgenden Wert ein: `http://ca_server:port/bi/api/soap`

   Beispiel: `http://my_ca_server:9300/bi/api/soap`

Enthält der URI die Angabe **localhost**, ersetzen Sie **localhost** durch einen vollständig qualifizierten Hostnamen oder eine IP-Adresse.

4. Klicken Sie im Menü **Datei** auf **Speichern**.

Ergebnisse

Framework Manager wird für die Kommunikation mit IBM Cognos Analytics konfiguriert.

Konfigurieren von Framework Manager innerhalb der Netzfirewall

Führen Sie die folgenden Schritte aus, um die Kommunikation zwischen Framework Manager und IBM Cognos Analytics-Komponenten einzurichten, wenn Framework Manager sich innerhalb einer Netzfirewall befindet.

Wichtig: Sie müssen vollständig qualifizierte Hostnamen in den Werten für die folgenden Felder von Cognos Configuration angeben. Jeder Wert, den Sie angeben, muss auch im Feld **Subject Alternative Name** > **DNS-Namen** oder im Feld **Subject Alternative Name** > **IP-Adressen** angezeigt werden.

- **Umgebung**
  - **Gateway-URI**
  - **Externer Dispatcher-URI**
  - **Interner Dispatcher-URI**
  - **Dispatcher-URI für externe Anwendungen**
  - **Content Manager-URIs**
- **Umgebung** > **Konfigurationsgruppe**
  - **Gruppenkontakthost**
  - **Host für die Koordination von Mitgliedern**
- **Zugriffsschutz** > **Verschlüsselung** > **Cognos**
  - **Allgemeiner Servername**
  - **Subject Alternative Name** > **DNS-Namen**
  - **Subject Alternative Name** > **IP-Adressen**

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Computer, auf dem Framework Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Geben Sie im Fenster **Eigenschaften** im Feld **Gateway-URI** den entsprechenden Wert ein.

   Verwenden Sie das HTTPS- oder das HTTP-Protokoll, um die Kommunikation mit SSL bzw. ohne SSL auszuwählen.
4. Ändern Sie den Hostnamen im **Gateway-URI** von LOCALHOST in die IP-Adresse oder den Hostnamen des Computers, auf dem die Gateway-Komponente installiert ist.
5. Legen Sie den Wert für den **Dispatcher-URI für externe Anwendungen** fest, indem Sie den URI des Servers eingeben, auf dem die Komponenten der Anwendungsebene installiert sind.

   Dieser Wert ist mit dem Wert der Eigenschaft **Interner Dispatcher-URI** auf dem Computer mit den Komponenten der Anwendungsebene identisch.
6. Klicken Sie im Fenster **Explorer** unter **Verschlüsselung** auf den standardmäßigen Verschlüsselungsprovider **Cognos**.
7. Geben Sie in der Eigenschaftengruppe **Einstellungen für Zertifizierungsstelle** für die Eigenschaft **Kennwort** das Kennwort an, das Sie auf dem standardmäßig aktiven Content Manager-Computer konfiguriert haben.
8. Klicken Sie im Menü **Datei** auf **Speichern**.

Konfigurieren von Framework Manager außerhalb der Netzfirewall

Wenn Framework Manager außerhalb der Netzfirewall installiert ist, können Sie für die Kommunikation mit dem Dispatcher ein dediziertes Gateway installieren und konfigurieren.

Vorgehensweise

1. Richten Sie ein dediziertes Gateway für Framework Manager ein.
2. Öffnen Sie auf dem Gateway-Computer IBM Cognos Configuration und ändern Sie die Eigenschaft **Dispatcher-URIs für Gateway** in den URI, der auf dem Computer mit den Komponenten der Anwendungsebene für **Interner Dispatcher-URI** angegeben ist.
3. Starten Sie IBM Cognos Configuration auf dem Framework Manager-Computer.
4. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
5. Geben Sie im Fenster **Eigenschaften** im Feld **Gateway-URI** den entsprechenden Wert für den Server ein, den Sie als dediziertes Gateway verwenden.
   - Wenn Ihr Web-Server für das ISAPI-Gateway konfiguriert wurde, ersetzen Sie `cognos.cgi` durch `cognosisapi.dll`.
   - Wenn Ihr Web-Server für die Verwendung von Apache-Modulen konfiguriert wurde, verwenden Sie die folgende Syntax:

     `http://`*`Hostname:Port`*`/ibmcognos/cgi-bin/`*`Modulalias`*
6. Ändern Sie den Teil LOCALHOST des **Gateway-URI** entweder in die IP-Adresse oder den Hostnamen des dedizierten Gateway-Servers.
7. Geben Sie im Feld **Dispatcher-URI für externe Anwendungen** den URI ein, der auf dem Server mit den Komponenten der Anwendungsebene als **Interner Dispatcher-URI** angegeben ist.
8. Klicken Sie im Fenster **Explorer** unter **Verschlüsselung** auf den standardmäßigen Verschlüsselungsprovider **Cognos**.
9. Geben Sie in der Eigenschaftengruppe **Einstellungen für Zertifizierungsstelle** für die Eigenschaft **Kennwort** das Kennwort an, das Sie auf dem standardmäßig aktiven Content Manager-Computer konfiguriert haben.
10. Klicken Sie im Menü **Datei** auf **Speichern**.

Ergebnisse

Framework Manager wird für die Kommunikation mit IBM Cognos Analytics und den zugehörigen Komponenten konfiguriert.

Festlegen von Variablen für Datenquellenverbindungen für Framework Manager

Die IBM Cognos Analytics-Modellierungstools erstellen und verwalten Metadaten. In Framework Manager werden Metadaten für die Berichtsfunktionen erstellt und verwaltet. Metadaten werden aus Datenquellen in Umgebungen mit mehreren Plattformen oder Sprachen abgeleitet. Daher müssen Sie mehrere Aspekte berücksichtigen, wenn Sie die Datenquellenumgebung für Framework Manager einrichten. Zumeist hängen diese Aspekte von der anderen Technologie ab, die für die Daten- oder Importquellen verwendet wird.

Wenn Sie ein Upgrade von einer älteren Version von Framework Manager durchgeführt haben, ist es nicht erforderlich, die Datenquellenumgebung einzurichten. Sie müssen die Datenquellenumgebung nur dann einrichten, wenn Sie Framework Manager in einem anderen Verzeichnis als die vorhergehende Version installiert haben.

Benutzer, die mit verschiedenen Sprachen arbeiten, können aus derselben Instanz von IBM Cognos Analytics eine Verbindung zu einer MSAS 2005-Datenquelle herstellen. Modellierer müssen für jede Sprache ein separates Package erstellen. Benutzer können Berichte in einer beliebigen Sprache ausführen.

Weitere Informationen über Datenquellenverbindungen finden Sie im Handbuch IBM Cognos *Verwaltung und Sicherheit*.

Stellen Sie sicher, dass Sie die entsprechenden Schriftarten installieren, um Unterstützung für die gewünschten Zeichensätze und Währungssymbole bereitzustellen. Damit japanische und koreanische Währungssymbole korrekt angezeigt werden, müssen Sie die zusätzlichen Schriftarten vom Supplementary Language Documentation-Datenträger installieren.

Führen Sie die folgenden Schritte an der Position durch, an der Framework Manager installiert ist.

Vorgehensweise

1. Legen Sie Umgebungsvariable zur Unterstützung mehrerer Sprachen fest:
   - Legen Sie für Oracle die Umgebungsvariable **NLS_LANG** (National Language Support) auf allen Computern fest, auf denen Framework Manager und IBM Cognos Analytics-Server installiert sind, indem Sie den folgenden Befehl eingeben:

     ```
     NLS_LANG = Sprache_Gebiet.Zeichensatz
     ```

     Beispiele:

     ```
     NLS_LANG = AMERICAN_AMERICA.UTF8
     ```

     ```
     NLS_LANG = JAPANESE_JAPAN.UTF8
     ```

     Der Wert der Variablen bestimmt das von der Ländereinstellung abhängige Verhalten von IBM Cognos Analytics. Fehlernachrichten, Sortierreihenfolge, Datum, Uhrzeit, Währung, Zahlen und Kalenderkonventionen werden automatisch an die native Sprache und die Ländereinstellung angepasst.
   - Legen Sie für IBM Db2 für die Umgebungsvariable **DB2CODEPAGE** den Wert 1252 fest.

     Weitere Informationen darüber, in welchen Fällen diese optionale Umgebungsvariable zu verwenden ist, finden Sie in der Db2-Dokumentation.

   Für SAP BW sind keine Einstellungen erforderlich. SAP unterstützt nur eine einzelne Codepage auf Nicht-Unicode SAP BW-Systemen.
2. Oracle: Fügen Sie `$ORACLE_HOME/lib` zu der Variablen **LD_LIBRARY_PATH** hinzu.

   Achten Sie beim Einrichten der Pfade zum Laden der Bibliothek darauf, dass sich die 32-Bit-Oracle-Bibliotheken im Bibliothekssuchpfad befinden (normalerweise das Verzeichnis `$ORACLE_HOME/lib` bzw. das Verzeichnis `$ORACLE_HOME/lib32`, wenn Sie einen 64-Bit-Oracle-Client installiert haben).
3. SAP BW: Konfigurieren Sie die folgenden Autorisierungsobjekte, damit das Tool zur Modellierung Metadaten abrufen kann.

   Wenn Standardwerte festgelegt sind, möchten Sie die Werte gegebenenfalls im SAP-System ändern.
   - **S_RFC**

     Legen Sie für das Feld **Activity** den Wert **16** fest.

     Legen Sie für das Feld **Name of RFC to be protected** den Wert **SYST, RSOB, SUGU, RFC1, RS_UNIFICATION, RSAB, SDTX, SU_USER** fest.

     Legen Sie für das Feld **Type of RFC** den Wert **FUGR** fest.
   - **S_TABU_DIS**

     Legen Sie für das Feld **Activity** den Wert **03** fest.

     Legen Sie für das Feld **Authorization Group** den Wert **&NC&** fest.

     Anmerkung: &NC& steht für eine beliebige Tabelle, die über keine Autorisierungsgruppe verfügt. Erstellen Sie aus Sicherheitsgründen eine neue Autorisierungsgruppe und weisen Sie dieser die Tabelle **RSHIEDIR** zu. Mit der neuen Autorisierungsgruppe wird der Benutzerzugriff ausschließlich auf die Tabelle beschränkt, die vom Modellierungstool benötigt wird. Erstellen Sie die Autorisierungsgruppe als Anpassung im SAP-System.
   - **S_USER_GRP**

Legen Sie für das Feld **Activity** den Wert **03, 05** fest.

Setzen Sie das Feld **User group in user master main** auf den Standardwert.

- **S_RS_COMP**

  Setzen Sie das Feld **Activity** auf den Standardwert.

  Setzen Sie das Feld **Info Area** auf den Wert *Technischer Name InfoArea*.

  Setzen Sie das Feld **Info Cube** auf den Wert *Technischer Name InfoCube*.

  Setzen Sie das Feld **Name (ID) of reporting components** auf den Standardwert.

  Setzen Sie das Feld **Type of reporting components** auf den Standardwert.

- **S_RS_COMP1**

  Setzen Sie das Feld **Activity** auf den Standardwert.

  Setzen Sie das Feld **Name (ID) of reporting components** auf den Standardwert.

  Setzen Sie das Feld **Type of reporting components** auf den Standardwert.

  Setzen Sie das Feld **Owner (Person Responsible)** auf den Standardwert.

- **S_RS_HIER**

  Legen Sie für das Feld **Activity** den Wert **71** fest.

  Setzen Sie das Feld **Hierarchy Name** auf den Wert *Hierarchiename*.

  Setzen Sie das Feld **InfoObject** auf den Wert *Technischer Name InfoObject*.

  Setzen Sie das Feld **Version** auf den Wert *Hierarchieversion*.

- **S_RS_ICUBE**

  Legen Sie für das Feld **Activity** den Wert **03** fest.

  Legen Sie für das Feld **InfoCube sub-object** die Werte **DATA** und **DEFINITION** fest.

  Setzen Sie das Feld **Info Area** auf den Wert *Technischer Name InfoArea*.

  Setzen Sie das Feld **InfoCube** auf den Wert *Technischer Name InfoCube*.

Weitere Informationen über SAP BW-Autorisierungsobjekte finden Sie in Transaction SU03.

Testen der Framework Manager-Installation

Sie können Ihre Konfiguration testen, indem Sie die Anwendung starten und ein Projekt erstellen.

Vorgehensweise

Um Framework Manager zu starten, klicken Sie im Menü **Start** auf **Alle Programme** > **IBM Cognos Framework Manager**.

Klicken Sie unter Microsoft Windows 8 oder Windows 2012 Server im Fenster **Start** doppelt auf das **Framework Manager**-Symbol.

Wenn die Version des Modellschemas älter als die derzeit unterstützte Version ist, werden Sie möglicherweise zur Aktualisierung aufgefordert.

Wenn die Seite **Willkommen** in Framework Manager angezeigt wird, war die Installation erfolgreich.

IBM Cognos Transformer

IBM Cognos Transformer ist das Metadatenmodellierungstool für die Erstellung von PowerCubes zur Verwendung mit IBM Cognos-Produkten.

Transformer kann Fachspezialisten, die Modelle entwickeln und PowerCubes für den eigenen Gebrauch erstellen möchten, nun einfacher zugänglich gemacht werden. Beispielsweise können IT-Abteilungen

ihren Fachspezialisten oder Transformer-Modellierern ein webbasiertes, herunterladbares Installationsprogramm in einem gemeinsamen gesicherten Portal zur Verfügung stellen und damit eine einfache Versendung der Installationsdateien gewährleisten.

Transformer besteht aus den folgenden Komponenten:

- Dienstprogramm des UNIX- und Linux-Betriebssystems zum Erstellen von PowerCubes
- IBM Cognos Transformer-Client

  Diese Komponente muss auf einem Windows-Computer installiert werden.

Beide Komponenten müssen an einer anderen Position als IBM Cognos Analytics installiert werden.

Für die Konfiguration werden Standardeinstellungen verwendet. Sie können diese Standardeinstellungen bei Bedarf ändern. Die Einstellungen müssen jedoch mit den Einstellungen für IBM Cognos Analytics übereinstimmen.

Systemanforderungen für Cognos Transformer

Stellen Sie vor der Installation von IBM Cognos Transformer sicher, dass der Computer die Software- und Hardwarevoraussetzungen erfüllt. Die Hardwarevoraussetzungen, z. B. der Festplattenspeicherplatz, hängen von der Größe Ihrer PowerCubes ab.

In der folgenden Tabelle sind die Mindestanforderungen im Hinblick auf Hard- und Software aufgeführt, die zur Ausführung von IBM Cognos Transformer erfüllt sein müssen.

Tabelle 20. Systemanforderungen für Transformer

Anforderung	**Spezifikation**
Betriebssystem	Windows UNIX: IBM AIX Linux
RAM	Minimum: 512 MB Optimal: 4 GB
Plattenspeicherplatz	Minimum: 500 MB freie Festplattenkapazität auf dem Laufwerk, das das temporäre Verzeichnis enthält
Datenquelle	Datenbank-Client-Software ist auf demselben Computer wie IBM Cognos Transformer installiert Datenbankverbindungen eingerichtet
Sonstige	Microsoft Data Access Component (MDAC) 2.6 oder höher zur Verwendung mit Produktbeispielen

Installieren von IBM Cognos Transformer

Installieren Sie IBM Cognos Transformer, wenn Sie planen, PowerCubes zur Verwendung in IBM Cognos-Produkten zu erstellen.

Für die Installation von Transformer muss eine andere Position als die IBM Cognos Analytics-Installationsposition ausgewählt werden.

Die Cognos Analytics-Serverkomponenten müssen vor der Installation von Transformer installiert und konfiguriert werden.

Durch die Sprache, die Sie im Installationsassistenten auswählen, wird die Sprache der Benutzeroberfläche sowohl für den Installationsassistenten als auch für IBM Cognos Transformer bestimmt. Es werden alle verfügbaren Sprachen installiert.

Unter einem UNIX- oder Linux-Betriebssystem ist die Installation von IBM Cognos Transformer erst abgeschlossen, nachdem Sie IBM Cognos Transformer auch auf einem Computer mit einem Microsoft Windows-Betriebssystem installiert haben. Alle Komponenten werden in beiden Umgebungen installiert und Sie verwenden dann die Funktionen und Tools, die für die jeweilige Umgebung geeignet sind. Der IBM Cognos Transformer-Client bietet beispielsweise eine grafische Benutzeroberfläche für die Gestaltung von Modellen auf Windows-Computern. Anschließend erstellen Sie Cubes auf Ihrem UNIX- oder Linux-Computer. Modelle, die eine IQD-Datenquelle enthalten, werden unter Linux nicht unterstützt.

Installieren Sie sie in einem Verzeichnis, dessen Pfadname ausschließlich aus ASCII-Zeichen besteht. Einige Server unterstützen in Verzeichnisnamen nur ASCII-Zeichen.

Schließen Sie vor der Installation von IBM Cognos Transformer alle gegenwärtig aktiven Programme, um sicherzustellen, dass das Installationsprogramm alle erforderlichen Dateien auf den Computer kopiert.

Bei einer Installation unter Windows müssen Sie außerdem sicherstellen, dass Sie für den Windows-Computer, auf dem Sie die Installation durchführen, über Administratorberechtigungen verfügen. Wenn Sie nicht über Administrator-Berechtigungen verfügen, bitten Sie Ihren Systemadministrator, Sie zur Administratorgruppe auf Ihrem Computer hinzuzufügen.

Installieren von IBM Cognos Transformer unter UNIX oder Linux

Führen Sie die folgenden Schritte durch, um IBM Cognos Transformer unter UNIX oder Linux zu installieren.

Vorgehensweise

1. Wechseln Sie an die Speicherposition, an der die Installationsdateien heruntergeladen und extrahiert wurden.
2. Wechseln Sie zum Starten des Installationsassistenten in das Betriebssystemverzeichnis und geben Sie Folgendes ein:

   ```
   ./issetup
   ```
3. Wählen Sie die für die Installation zu verwendende Sprache aus.

   Durch die Sprache, die Sie im Installationsassistenten auswählen, wird die Sprache der Benutzeroberfläche für den Installationsassistenten und für IBM Cognos Transformer festgelegt. Es werden alle verfügbaren Sprachen installiert.
4. Folgen Sie den Anweisungen des Installationsassistenten und kopieren Sie die benötigten Dateien auf den Computer.

   Tipp: Die Series 7 IQD Bridge-Komponenten wird unter Linux nicht unterstützt.
5. Gehen Sie auf der Seite **Fertigstellen** des Installationsassistenten wie folgt vor:
   - Wenn Sie die Protokolldateien anzeigen möchten, klicken Sie für die jeweilige Protokolldatei auf **Ansicht**.
   - Starten Sie IBM Cognos Configuration zu diesem Zeitpunkt nicht. Sie müssen zuerst sicherstellen, dass die Umgebung korrekt eingerichtet ist.

     Sie können Transformer mithilfe von IBM Cognos Configuration zu einem späteren Zeitpunkt konfigurieren, indem Sie `cogconfig.sh` im Verzeichnis *`installationsposition`*`/bin64` eingeben.
   - Klicken Sie auf **Fertigstellen**.

Nächste Schritte

Informationen zur Syntax für UNIX-Befehlszeilenoptionen, die von IBM Cognos Transformer unterstützt werden, finden Sie in der Veröffentlichung *IBM Cognos Transformer UNIX Commands Guide*

im IBM Cognos Analytics Knowledge Center (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html).

Die Man-Page für IBM Cognos Transformer kann unter UNIX durch Eingabe von `cogtr man` im Verzeichnis *`installationsposition`*`/bin64` aufgerufen werden.

Installieren von IBM Cognos Transformer unter Windows

Führen Sie die folgenden Schritte durch, um IBM Cognos Transformer unter Microsoft Windows zu installieren.

Vorgehensweise

1. Wechseln Sie zu der Position, an der die Installationsdateien heruntergeladen und extrahiert wurden, und klicken Sie doppelt auf die Datei `issetup.exe`.
2. Wählen Sie die für die Installation zu verwendende Sprache aus.

   Durch die Sprache, die Sie im Installationsassistenten auswählen, wird die Sprache der Benutzeroberfläche für den Installationsassistenten und für IBM Cognos Transformer festgelegt. Es werden alle verfügbaren Sprachen installiert.
3. Folgen Sie den Anweisungen im Installationsassistenten, um die erforderlichen Dateien auf Ihren Computer zu kopieren.
4. Gehen Sie auf der Seite **Fertigstellen** des Installationsassistenten wie folgt vor:
   - Wenn Sie die Protokolldateien anzeigen möchten, klicken Sie für die jeweilige Protokolldatei auf **Ansicht**.
   - Starten Sie IBM Cognos Configuration zu diesem Zeitpunkt nicht. Sie müssen zuerst sicherstellen, dass die Umgebung korrekt eingerichtet ist.

     IBM Cognos Configuration kann über die Verknüpfung **IBM Cognos Configuration** im Menü **Start** gestartet werden.
   - Klicken Sie auf **Fertigstellen**.

Konfigurieren der Kommunikation zwischen Transformer und Cognos Analytics

Sie müssen IBM Cognos Transformer für die Kommunikation mit IBM Cognos Analytics konfigurieren.

Vorbereitende Schritte

Installieren und konfigurieren Sie alle IBM Cognos Analytics-Komponenten, bevor Sie IBM Cognos Transformer konfigurieren. Sie müssen zuerst Content Manager installieren und konfigurieren und den **IBM Cognos**-Service auf mindestens einem Content Manager-Computer starten, bevor Sie IBM Cognos Transformer konfigurieren. Dies gewährleistet, dass der Zertifizierungsstellenservice ein Zertifikat für den IBM Cognos Transformer-Computer ausstellt.

Stellen Sie zur Unterstützung der Verwendung von IBM Cognos Analytics-Datenquellen (einschließlich Packages und Berichte) in Transformer sicher, dass der Datenbankclient auf dem Computer installiert ist, auf dem Transformer installiert ist.

Wenn sich Transformer außerhalb einer Netzfirewall befindet, durch die die Komponenten der Anwendungsebene geschützt sind, können bei der Kommunikation mit dem Dispatcher Probleme auftreten. Um solche Kommunikationsprobleme zu vermeiden, kann Transformer auf derselben Architekturebene wie die Komponenten der Anwendungsebene installiert werden. Als Alternative können Sie für die Kommunikation mit Transformer ein dediziertes Gateway installieren und konfigurieren. Weitere Informationen finden Sie im Abschnitt „Hinweise zu Firewalls” auf Seite 62.

Wenn Sie ein dediziertes Gateway verwenden, müssen Sie auch den Gateway-Computer konfigurieren. Weitere Informationen finden Sie im Abschnitt Kapitel 10, „Konfigurieren des Gateways”, auf Seite 121.

Informationen zu diesem Vorgang

Die Anweisungen in diesem Thema sind für den Installierer oder Administrator bestimmt. Wenn Sie ein Transformer-Modellierer oder Wirtschaftsinformatiker sind, der Transformer herunterladen und verwenden möchte, ist der Abschnitt „Bereitstellen von IBM Cognos Transformer für Modellierer” auf Seite 166 für Sie von Interesse.

Falls IBM Cognos Analytics in mehreren Pfaden installiert wurde, stellen Sie sicher, dass alle URIs auf die richtige Version von IBM Cognos Analytics verweisen.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Computer, auf dem IBM Cognos Transformer installiert ist.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Geben Sie entsprechende Werte für die folgenden Einstellungen an:

   Gateway-URI
   Standardeinstellung: `http://CA-Server:Port/bi/v1/disp`

   Beispiel: `http://my_ca_server:9300/bi/v1/disp`

   Dieser URI muss stets mit dem URI für Cognos Analytics übereinstimmen.

   Enthält der URI die Angabe **localhost**, ersetzen Sie **localhost** durch einen vollständig qualifizierten Hostnamen oder eine IP-Adresse.

   Dispatcher-URI für externe Anwendungen
   Standardeinstellung: `http://CA-Server:Port/p2pd/servlet/dispatch`

   Beispiel: `http://my_ca_server:9300/p2pd/servlet/dispatch`

   Enthält der URI die Angabe **localhost**, ersetzen Sie **localhost** durch einen vollständig qualifizierten Hostnamen oder eine IP-Adresse.
4. Klicken Sie im Menü **Datei** auf **Speichern**.

Ergebnisse

IBM Cognos Transformer wurde für die Kommunikation mit IBM Cognos Analytics konfiguriert.

Konfigurieren der Kommunikation zwischen Transformer und Cognos Analytics

Sie müssen IBM Cognos Transformer für die Kommunikation mit IBM Cognos Analytics konfigurieren.

Vorbereitende Schritte

Installieren und konfigurieren Sie alle IBM Cognos Analytics-Komponenten, bevor Sie IBM Cognos Transformer konfigurieren. Sie müssen zuerst Content Manager installieren und konfigurieren und den **IBM Cognos**-Service auf mindestens einem Content Manager-Computer starten, bevor Sie IBM Cognos Transformer konfigurieren. Dies gewährleistet, dass der Zertifizierungsstellenservice ein Zertifikat für den IBM Cognos Transformer-Computer ausstellt.

Stellen Sie zur Unterstützung der Verwendung von IBM Cognos Analytics-Datenquellen (einschließlich Packages und Berichte) in Transformer sicher, dass der Datenbankclient auf dem Computer installiert ist, auf dem Transformer installiert ist.

Wenn sich Transformer außerhalb einer Netzfirewall befindet, durch die die Komponenten der Anwendungsebene geschützt sind, können bei der Kommunikation mit dem Dispatcher Probleme auftreten. Um solche Kommunikationsprobleme zu vermeiden, kann Transformer auf derselben Architekturebene wie die Komponenten der Anwendungsebene installiert werden. Als Alternative können Sie für die Kommunikation mit Transformer ein dediziertes Gateway installieren und konfigurieren. Weitere Informationen finden Sie im Abschnitt „Hinweise zu Firewalls” auf Seite 62.

Wenn Sie ein dediziertes Gateway verwenden, müssen Sie auch den Gateway-Computer konfigurieren. Weitere Informationen finden Sie im Abschnitt Kapitel 10, „Konfigurieren des Gateways", auf Seite 121.

Informationen zu diesem Vorgang

Die Anweisungen in diesem Thema sind für den Installierer oder Administrator bestimmt. Wenn Sie ein Transformer-Modellierer oder Wirtschaftsinformatiker sind, der Transformer herunterladen und verwenden möchte, ist der Abschnitt „Bereitstellen von IBM Cognos Transformer für Modellierer" auf Seite 166 für Sie von Interesse.

Falls IBM Cognos Analytics in mehreren Pfaden installiert wurde, stellen Sie sicher, dass alle URIs auf die richtige Version von IBM Cognos Analytics verweisen.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Computer, auf dem IBM Cognos Transformer installiert ist.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Geben Sie entsprechende Werte für die folgenden Einstellungen an:

   Gateway-URI
   Standardeinstellung: `http://`*`CA-Server`*`:`*`Port`*`/bi/v1/disp`

   Beispiel: `http://my_ca_server:`*`9300`*`/bi/v1/disp`

   Dieser URI muss stets mit dem URI für Cognos Analytics übereinstimmen.

   Enthält der URI die Angabe **localhost**, ersetzen Sie **localhost** durch einen vollständig qualifizierten Hostnamen oder eine IP-Adresse.

   Dispatcher-URI für externe Anwendungen
   Standardeinstellung: `http://`*`CA-Server`*`:`*`Port`*`/p2pd/servlet/dispatch`

   Beispiel: `http://my_ca_server:9300/p2pd/servlet/dispatch`

   Enthält der URI die Angabe **localhost**, ersetzen Sie **localhost** durch einen vollständig qualifizierten Hostnamen oder eine IP-Adresse.
4. Klicken Sie im Menü **Datei** auf **Speichern**.

Ergebnisse

IBM Cognos Transformer wurde für die Kommunikation mit IBM Cognos Analytics konfiguriert.

Einrichten von Datenquellen für Transformer

Mit IBM Cognos Transformer werden Metadaten für PowerCubes erstellt und verwaltet.

Metadaten werden aus Datenquellen in Umgebungen mit mehreren Plattformen oder Sprachen abgeleitet. Daher müssen Sie mehrere Aspekte berücksichtigen, wenn Sie die Datenquellenumgebung für IBM Cognos Transformer einrichten. Zumeist hängen diese Aspekte von anderer Technologie ab, die für die Daten- oder Importquellen verwendet wird.

Wenn Benutzer, die mit verschiedenen Sprachen arbeiten, eine Verbindung zu einer Microsoft Analysis Services (MSAS) 2000-Datenquelle herstellen, müssen Sie für jede Sprache eine separate IBM Cognos Analytics-Instanz erstellen.

Benutzer, die mit verschiedenen Sprachen arbeiten, können aus derselben Instanz von IBM Cognos Analytics eine Verbindung zu einer MSAS 2005-Datenquelle herstellen. Modellierer müssen für jede Sprache ein separates Package erstellen. Benutzer können Berichte in einer beliebigen Sprache ausführen.

Weitere Informationen zu Datenquellenverbindungen finden Sie im Handbuch *IBM Cognos AnalyticsVerwaltung und Sicherheit*.

Stellen Sie sicher, dass Sie die entsprechenden Schriftarten installieren, um Unterstützung für die gewünschten Zeichensätze und Währungssymbole bereitzustellen. Damit japanische und koreanische Wäh-

rungssymbole korrekt angezeigt werden, müssen Sie die zusätzlichen Schriftarten vom Supplementary Language Documentation-Datenträger installieren.

Führen Sie die folgenden Schritte aus, um Oracle- oder SAP BW-Datenquellen für IBM Cognos Transformer einzurichten.

Vorgehensweise

1. Legen Sie Umgebungsvariable zur Unterstützung mehrerer Sprachen fest:
   - Legen Sie für Oracle die Umgebungsvariable **NLS_LANG** (National Language Support) auf allen Computern fest, auf denen Framework Manager und IBM Cognos Analytics-Server installiert sind, indem Sie den folgenden Befehl eingeben:

     ```
     NLS_LANG = Sprache_Gebiet.Zeichensatz
     ```

     Beispiele:

     ```
     NLS_LANG = AMERICAN_AMERICA.UTF8
     ```

     ```
     NLS_LANG = JAPANESE_JAPAN.UTF8
     ```

     Der Wert der Variablen bestimmt das von der Ländereinstellung abhängige Verhalten von IBM Cognos Analytics. Fehlernachrichten, Sortierreihenfolge, Datum, Uhrzeit, Währung, Zahlen und Kalenderkonventionen werden automatisch an die native Sprache und die Ländereinstellung angepasst.
   - Legen Sie für IBM Db2 für die Umgebungsvariable **DB2CODEPAGE** den Wert 1252 fest.

     Weitere Informationen darüber, in welchen Fällen diese optionale Umgebungsvariable zu verwenden ist, finden Sie in der Db2-Dokumentation.

   Für SAP BW sind keine Einstellungen erforderlich. SAP unterstützt nur eine einzelne Codepage auf Nicht-Unicode SAP BW-Systemen.
2. Fügen Sie für Oracle $ORACLE_HOME/lib zum Bibliothekspfad hinzu.

   Achten Sie beim Einrichten der Pfade zum Laden der Bibliothek darauf, dass sich die 32-Bit Oracle-Bibliotheken im Bibliothekssuchpfad befinden, das ist meist das $ORACLE_HOME/lib-Verzeichnis bzw. das $ORACLE_HOME/lib32-Verzeichnis, wenn Sie einen 64-Bit Oracle-Client installiert haben.
3. SAP BW: Konfigurieren Sie die folgenden Autorisierungsobjekte, damit das Tool zur Modellierung Metadaten abrufen kann.

   Wenn Standardwerte festgelegt sind, möchten Sie die Werte gegebenenfalls im SAP-System ändern.
   - **S_RFC**

     Legen Sie für das Feld **Activity** den Wert **16** fest.

     Legen Sie für das Feld **Name of RFC to be protected** den Wert **SYST, RSOB, SUGU, RFC1, RS_UNIFICATION, RSAB, SDTX, SU_USER** fest.

     Legen Sie für das Feld **Type of RFC** den Wert **FUGR** fest.
   - **S_TABU_DIS**

     Legen Sie für das Feld **Activity** den Wert **03** fest.

     Legen Sie für das Feld **Authorization Group** den Wert **&NC&** fest.

     Anmerkung: &NC& steht für eine beliebige Tabelle, die über keine Autorisierungsgruppe verfügt. Erstellen Sie aus Sicherheitsgründen eine neue Autorisierungsgruppe und weisen Sie dieser die Tabelle **RSHIEDIR** zu. Mit der neuen Autorisierungsgruppe wird der Benutzerzugriff ausschließlich auf die Tabelle beschränkt, die vom Modellierungstool benötigt wird. Erstellen Sie die Autorisierungsgruppe als Anpassung im SAP-System.
   - **S_USER_GRP**

     Legen Sie für das Feld **Activity** den Wert **03, 05** fest.

     Setzen Sie das Feld **User group in user master main** auf den Standardwert.

- **S_RS_COMP**

  Setzen Sie das Feld **Activity** auf den Standardwert.

  Setzen Sie das Feld **Info Area** auf den Wert *Technischer Name InfoArea*.

  Setzen Sie das Feld **Info Cube** auf den Wert *Technischer Name InfoCube*.

  Setzen Sie das Feld **Name (ID) of reporting components** auf den Standardwert.

  Setzen Sie das Feld **Type of reporting components** auf den Standardwert.
- **S_RS_COMP1**

  Setzen Sie das Feld **Activity** auf den Standardwert.

  Setzen Sie das Feld **Name (ID) of reporting components** auf den Standardwert.

  Setzen Sie das Feld **Type of reporting components** auf den Standardwert.

  Setzen Sie das Feld **Owner (Person Responsible)** auf den Standardwert.
- **S_RS_HIER**

  Legen Sie für das Feld **Activity** den Wert **71** fest.

  Setzen Sie das Feld **Hierarchy Name** auf den Wert *Hierarchiename*.

  Setzen Sie das Feld **InfoObject** auf den Wert *Technischer Name InfoObject*.

  Setzen Sie das Feld **Version** auf den Wert *Hierarchieversion*.
- **S_RS_ICUBE**

  Legen Sie für das Feld **Activity** den Wert **03** fest.

  Legen Sie für das Feld **InfoCube sub-object** die Werte **DATA** und **DEFINITION** fest.

  Setzen Sie das Feld **Info Area** auf den Wert *Technischer Name InfoArea*.

  Setzen Sie das Feld **InfoCube** auf den Wert *Technischer Name InfoCube*.

Weitere Informationen über SAP BW-Autorisierungsobjekte finden Sie in Transaction SU03.

Testen der Transformer-Installation

Sie können Ihre Konfiguration testen, indem Sie die Anwendung starten und ein Modell erstellen.

Vorgehensweise

Klicken Sie zum Starten von IBM Cognos Transformer im Menü **Start** auf 'Programme' und anschließend auf **IBM Cognos Transformer**.

Klicken Sie unter Microsoft Windows 8 oder Windows 2012 Server im Fenster **Start** doppelt auf das **IBM Cognos Transformer**-Symbol.

Zum manuellen Starten von IBM Cognos Transformer klicken Sie im Verzeichnis *installationsposition*\bin doppelt auf die Datei cogtr.exe.

Wenn das Fenster **Transformer** angezeigt wird, war die Installation erfolgreich.

Zusätzliche Konfigurationsaufgaben für Cognos Transformer

Die in diesem Abschnitt aufgeführten Aufgaben sind für Modellierer von Cognos Transformer vorgesehen.

Wenn Sie Modellierern Transformer zur Installation und Verwendung zur Verfügung stellen möchten, führen Sie die folgenden Aufgaben aus:

- Erstellen eines Netzinstallationspfads für Transformer-Modellierer
- Exportieren von Konfigurationsdaten für Transformer-Modellierer
- Bereitstellen von IBM Cognos Analytics Transformer für Modellierer

Erstellen eines Netzinstallationspfads für Transformer-Modellierer

Ihr Unternehmen verfügt möglicherweise über spezialisierte oder erfahrene Benutzer, die PowerCubes erstellen möchten, die anhand einer Kombination aus Unternehmens- und persönlichen Datenquellen modelliert werden. Diese Benutzer möchten möglicherweise eigene Analysen der Daten für Ihre Geschäftssparte oder eine kleine Benutzergruppe durchführen. Der Systemverantwortliche oder Administrator kann eine ausführbare Datei an eine Web- oder LAN-Position herunterladen, an der Modellierer die Datei ausführen können, um den IBM Cognos Transformer-Installationsassistenten auszuführen.

Die Anweisungen in diesem Thema sind für den Installierer oder Administrator bestimmt. Wenn Sie Transformer-Modellierer oder Fachspezialist sind und Transformer herunterladen und verwenden möchten, finden Sie weitere Informationen unter „Bereitstellen von IBM Cognos Transformer für Modellierer" auf Seite 166.

Vorbereitende Schritte

Bevor Sie Transformer-Modellierern die Installationsdatei zugänglich machen, müssen noch Quellen und Berechtigungen eingerichtet werden:

- Die Datenbank-Client-Software ist auf den Transformer-Computern installiert (bzw. steht Modellierern dort für die Installation zur Verfügung), die zum Zugriff auf IBM Cognos Analytics-Datenquellen oder IBM Cognos Series 7 IQD-Datenquellen verwendet werden.
- Modellierer müssen Berechtigungen zum Erstellen von Datenquellen in IBM Cognos Administration besitzen.

  Die Modellierer müssen nicht direkt auf IBM Cognos Administration zugreifen können. Sie können Datenquellen mit Transformer oder Befehlszeilen-Tools erstellen und aktualisieren. Sie können für Modellierer einen gesicherten Ordner in dem Portal zur Verfügung stellen, in dem PowerCube-Packages publiziert werden.
- Die Modellierer müssen auf eine Position zugreifen können, an der der PowerCube nach der Erstellung gespeichert werden kann.

  Der IBM Cognos-Service muss auf diese Position zugreifen können; hierbei kann es sich durchaus auch um ein gesichertes gemeinsam genutztes Verzeichnis in einem LAN handeln.
- Um PowerCubes auf einem spezifischen Transformer-Server zu erstellen, muss der Modellierer über FTP-Berechtigungen für die Übertragung von Modellen und Ausführungsberechtigungen für die Erstellung von Cubes auf dem Server verfügen.

  Der Modellierer kann Modelle übertragen und die Cube-Erstellung mithilfe von Scripts ausführen. Der Modellierer kann auch automatische Methoden verwenden, um PowerCubes zu erstellen. Weitere Informationen finden Sie im Handbuch *Verwaltung und Sicherheit*.

Vorgehensweise

1. Legen Sie den Datenträger für Ihr IBM Cognos Transformer-Modellierungsprodukt ein.
2. Wenn die Seite **Willkommen** des Installationsassistenten angezeigt wird, schließen Sie den Assistenten.
3. Suchen Sie auf dem Datenträger die Datei C8transformerinstall.exe.
4. Kopieren Sie die Datei an eine sichere Speicherposition, auf die die Transformer-Modellierer zugreifen können.

Konfigurationsdaten für Transformer-Modellierer

Soll die Transformer-Installationsdatei den Transformer-Modellierern zugänglich gemacht werden, so benötigen diese die Dispatcher- und Verschlüsselungseinstellungen, um Transformer auf den lokalen Computern zu konfigurieren.

Sie können die Konfiguration von einem Transformer-Computer aus für die Verwendung auf allen anderen Computern exportieren. Die Modellierer können die exportierte Konfigurationsdatei in ihr Transformer-Installationsverzeichnis kopieren und den Transformer-Computer im Hintergrund zu konfigurieren.

Die Anweisungen in diesem Thema sind für den Installierer oder Administrator bestimmt. Wenn Sie ein Transformer-Modellierer oder Wirtschaftsinformatiker sind, der Transformer herunterladen und verwenden möchte, ist der Abschnitt „Bereitstellen von IBM Cognos Transformer für Modellierer” auf Seite 166 für Sie von Interesse.

Wenn Sie die Dateien "coglocale", "cogtr.xml" oder "cs7g.ini" auf dem Transformer-Computer aktualisiert haben, müssen Sie diese Dateien an die Web- oder LAN-Positionen kopieren, damit die Transformer-Modellierer sie sich auf ihren Computer herunterladen können.

Um die Konfiguration zu exportieren, muss der Quellencomputer über dieselben IBM Cognos Analytics-Komponenten verfügen wie die Computer der Transformer-Modellierer („Konfigurieren der Kommunikation zwischen Transformer und Cognos Analytics” auf Seite 160).

Exportieren der Transformer-Konfiguration

Mit IBM Cognos Configuration können Sie die Konfiguration von einem Transformer-Computer für die Verwendung auf allen anderen Transformer-Computern exportieren.

Vorgehensweise

1. Klicken Sie in IBM Cognos Configuration im Menü **Datei** auf **Exportieren als**.
2. Wenn die aktuelle Konfiguration in einen anderen Ordner exportiert werden soll, können Sie diesen im Feld **Suchen in** suchen und öffnen.

   Stellen Sie sicher, dass der Ordner vor nicht autorisiertem oder unerwünschtem Zugriff geschützt ist.
3. Geben Sie im Feld **Dateiname** einen Namen für die Konfigurationsdatei ein.
4. Klicken Sie auf **Speichern**.
5. Ändern Sie den Namen der exportierten Datei in cogstartup.xml.
6. Kopieren Sie die exportierte Datei cogstartup.xml vom Quellencomputer an die Web- oder LAN-Speicherposition, an der sich auch die Transformer-Installationsdatei befindet.
7. Wenn Sie die globale Konfiguration auf dem Quellencomputer geändert haben, kopieren Sie die Datei coglocale.xml vom Quellencomputer an die Web- oder LAN-Speicherposition, an der sich die Transformer-Installationsdatei befindet.

   Der Standardpfad der Datei coglocale.xml ist *installationsposition*/configuration.

Kopieren aktualisierter Transformer-Konfigurationsdateien

Wenn Sie bestimmte Konfigurationsdateien aktualisiert haben, müssen Sie diese an die Position kopieren, an der sich die Transformer-Installationsdateien befinden.

Vorgehensweise

1. Wenn Sie die Datei "cogtr.xml" aktualisiert haben, kopieren Sie sie aus dem Verzeichnis `installationsposition/configuration` an die Web- oder LAN-Position, an der sich auch die Transformer-Installationsdatei befindet.
2. Wenn Sie die Datei "cs7g.ini" aktualisiert haben, kopieren Sie sie aus dem Verzeichnis `installationsposition/CS7Gateways/bin` an die Web- oder LAN-Position, an der sich die Transformer-Installationsdatei befindet.

Bereitstellen von IBM Cognos Transformer für Modellierer

Wenn Sie ein Fachspezialist oder Transformer-Modellierer sind, müssen Sie Transformer bereitstellen, damit Sie PowerCubes erstellen und für ausgewählte Benutzer oder Gruppen publizieren können.

Wenn Sie noch keine Installation abgeschlossen haben, gehen Sie wie folgt vor , um Transformer zu installieren. Um Transformer so zu konfigurieren, dass er mit dem IBM Cognos Analytics-Dispatcher kommunizieren kann, führen Sie die Schritte zum Konfigurieren von Transformer aus.

Stellen Sie zur Unterstützung der Verwendung von IBM Cognos Analytics-Datenquellen (einschließlich Packages und Berichte) in Transformer sicher, dass der Datenbankclient auf dem Transformer-Computer installiert ist.

Installation von Transformer

Führen Sie als Fachspezialist oder Transformer-Modellierer die folgenden Schritte durch, um Transformer vom Web oder von einer durch den Administrator bereitgestellten LAN-Position aus zu installieren.

Vorgehensweise

1. Führen Sie von einem Web- oder LAN-Pfad, den der Administrator zur Verfügung gestellt hat, die Datei C8transformerinstall.exe aus.
2. Folgen Sie den Anweisungen des Installationsassistenten und kopieren Sie die benötigten Dateien auf den Computer.

   Tipp: Die Series 7 IQD Bridge-Komponenten wird unter Linux nicht unterstützt.
3. Klicken Sie auf der Seite **Fertigstellen** des Assistenten auf **Fertigstellen**.

Nächste Schritte

Die Veröffentlichung *IBM Cognos Transformer UNIX Commands Guide* enthält die Syntax für UNIX-Befehlszeilenoptionen, die von Cognos Transformer unterstützt werden. Sie können über das IBM Cognos Analytics Knowledge Center (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0) auf dieses Dokument zugreifen.

Konfigurieren von Transformer

Führen Sie als Fachspezialist oder Transformer-Modellierer zum Konfigurieren von Transformer die folgenden Schritte aus.

Vorgehensweise

1. Wechseln Sie zu dem Web- oder LAN-Pfad, auf dem sich die Transformer-Installationsdatei befindet.
2. Kopieren Sie etwaige .xml-Dateien in das Verzeichnis *Transformer_Position*\configuration, wobei *Transformer_Position* das Installationsverzeichnis von Transformer ist.
3. Kopieren Sie etwaige .ini-Dateien in das Verzeichnis *Transformer_Position*\CS7Gateways\bin.
4. Wechseln Sie in das Verzeichnis *Transformer_Position*\bin.
5. Geben Sie den Konfigurationsbefehl ein:

   ```
   ./cogconfig.bat -s
   ```

   IBM Cognos Configuration wendet die in der lokalen Kopie der Datei cogstartup.xml angegebenen Konfigurationseinstellungen an, verschlüsselt Berechtigungsnachweise, generiert digitale Zertifikate und startet den IBM Cognos-Service.
6. Klicken Sie zum Testen von IBM Cognos Transformer im Menü **Start** auf 'Programme' und anschließend auf **IBM Cognos Transformer**.

   Wenn das Fenster **Transformer** angezeigt wird, war die Installation erfolgreich.
7. Löschen Sie nach der erfolgreichen Installation und Ausführung von Transformer die Installationsdateien, die von der Installationsdatei extrahiert wurden.

Kapitel 12. Konfigurationsoptionen

Nach der erfolgten Installation und Konfiguration von IBM Cognos-Komponenten können Sie die Konfiguration für Ihre Umgebung ändern. Die Standardeigenschaftseinstellungen sind zunächst für die Konfiguration der Komponenten vorgegeben. Sie können diese Standardeinstellungen jedoch ändern, wenn sie unter den gegebenen Bedingungen nicht angemessen sind, oder um sie an Ihre Umgebung anzupassen.

Sie können z. B. Funktionen für IBM Cognos Application Firewall konfigurieren oder festlegen, wie viele Ressourcen IBM Cognos-Komponenten zur Verfügung stehen sollen. Außerdem können Sie IBM Cognos-Inhalte mithilfe eines anderen Portals durch die Konfiguration von Portal Services übermitteln.

Sie können IBM Cognos-Komponenten für die Nutzung anderer Ressourcen, wie z. B. eines Authentifizierungsproviders, konfigurieren und dann die Einzelanmeldung (Single Sign-on) für die Datenbank und die Benutzer aktivieren.

Wenn Sie ein Lastausgleichsschema in Ihrer Umgebung verwenden, können Sie dessen Einstellungen ändern, um die Leistung zu verbessern. Sie können z. B. die Anforderungen auf die verschiedenen Dispatcher verteilen, indem Sie deren Verarbeitungskapazität ändern oder indem Sie die minimale und maximale Anzahl an Prozessen und Verbindungen festlegen. Weitere Informationen zum Anpassen der Serverleistung finden Sie im Handbuch *Verwaltung und Sicherheit*.

Bei allen Microsoft Windows- und den meisten UNIX- und Linux-Installationen erfolgt die Konfiguration der Einstellungen mithilfe von IBM Cognos Configuration. Wenn jedoch die an den UNIX- oder Linux-Computer angeschlossene Konsole, auf der Sie IBM Cognos-Komponenten installieren, keine Java-basierten grafischen Benutzeroberflächen unterstützt, müssen Sie die Datei `cogstartup.xml` im Verzeichnis *`installationsposition`*`/configuration` manuell bearbeiten und IBM Cognos Configuration anschließend im Hintergrundmodus ausführen.

Passen Sie Ihre Konfiguration mithilfe dieser optionalen Konfigurationsaufgaben so an, dass sich IBM Cognos-Komponenten problemlos in Ihre vorhandene Umgebung integrieren lassen.

Starten von IBM Cognos Configuration

Verwenden Sie das Konfigurationstool IBM Cognos Configuration, um IBM Cognos zu konfigurieren oder um die IBM Cognos-Services zu starten und zu stoppen.

Bevor Sie IBM Cognos Configuration starten, müssen Sie sicherstellen, dass die Betriebsumgebung ordnungsgemäß eingerichtet ist. Prüfen Sie beispielsweise, ob alle Variablen definiert wurden.

Sie sollten IBM Cognos Configuration nur von der letzten Seite des Installationsassistenten unter dem Betriebssystem Microsoft Windows, UNIX oder Linux starten, wenn keine zusätzlichen Einrichtungsschritte erforderlich sind. Wenn Sie beispielsweise einen anderen Datenbankserver als Microsoft SQL für den Content Store verwenden, kopieren Sie die JDBC-Treiber vor dem Starten des Konfigurationstools an die richtige Position.

Gehen Sie wie folgt vor, um IBM Cognos Configuration auf einem Windows-Computer zu starten:

- Klicken Sie im Menü **Start** auf **Programme** > **IBM Cognos Configuration**.

Gehen Sie wie folgt vor, um IBM Cognos Configuration auf einem UNIX- oder Linux-Computer zu starten:

- Wechseln Sie in das Verzeichnis *`installationsposition`*`/bin` und geben Sie Folgendes ein:

  ./cogconfig.sh

Kritische Konfigurationsaktionen, die zuerst erledigt werden müssen!

Diese Konfigurationsaktionen sind für den Erfolg der Installation entscheidend. Führen Sie diese Aktionen nach der Installation der Komponenten aus.

Sicherstellen, dass JDBC-Treiber an der richtigen Position sind

Für das Release IBM Cognos Analytics 11.1.x müssen die JDBC-Treiber in das Verzeichnis *Installationsposition*\drivers kopiert werden.

Die Verwendung von *Installationsposition*\webapps\p2pd\WEB-INF\lib für JDBC-Treiber wird nicht unterstützt.

JSQL-Treiber für Microsoft SQL Server durch den Microsoft-JDBC-Treiber ersetzen

Ab IBM Cognos Analytics Version 11.0.5 wurde der JSQL-Treiber für Microsoft SQL Server durch den Microsoft-JDBC-Treiber ersetzt. Sie müssen die erforderliche JAR-Datei herunterladen und in das Verzeichnis *Installationsposition*\drivers platzieren. Weitere Informationen finden Sie in Setup für einen Microsoft SQL Server-Content Store.

Eigenschaft Konfigurationsgruppe angeben

Wenn Sie IBM Cognos Analytics **angepasst** installiert haben, öffnen Sie IBM Cognos Configuration und legen Sie die Eigenschaft **Konfigurationsgruppe** fest. Weitere Informationen finden Sie in Verwalten der Konfigurationsgruppe.

Webbasierte Modellierung aktivieren oder inaktivieren

Standardmäßig werden in IBM Cognos Administration erstellte JDBC-Datenquellen nicht in der **Verwalten** > **Datenserver**-Verwaltungsschnittstelle zur Verwendung in Datenmodulen zugänglich gemacht. Wenn Sie Ihre vorhandenen (aktualisierten) Datenquellenverbindungen zum Erstellen von Datenmodulen verwenden wollen, müssen Sie für diese Verbindungen die webbasierte Modellierung aktivieren.

Einige Datenquellen sind für die Verwendung als Quellen zur Erstellung von Datenmodulen ungeeignet. In diesem Fall können Sie die Verwendung von webbasierter Modellierung für die Datenquellenverbindungen untersagen.

Führen Sie folgende Schritte aus, um die webbasierte Modellierung für Ihre Datenquellenverbindungen zu aktivieren oder zu inaktivieren:

1. Wechseln Sie in IBM Cognos Analytics zu **Verwalten** > **Administrationskonsole**.
2. Wählen Sie in IBM Cognos Administration auf der Registerkarte **Konfiguration** die Option **Datenquellenverbindungen** aus.
3. Suchen Sie die Datenquelle und klicken Sie auf die zugehörige Aktion **Eigenschaften festlegen**.
4. Wählen Sie auf der Registerkarte **Verbindung** das Kontrollkästchen **Webbasierte Modellierung zulassen** aus oder ab.

Ändern der von IBM Cognos Analytics-Komponenten verwendeten Java-Version

Für den Betrieb von IBM Cognos Analytics-Komponenten ist Java Runtime Environment (JRE) erforderlich.

Sie können die Java-Version zum Beispiel ändern, wenn Sie IBMCognos Analytics-Komponenten mit einem Anwendungsserver verwenden möchten, der eine bestimmte JRE-Version voraussetzt, oder Sie bereits eine JRE-Version für andere Anwendungen verwenden. Die Java-Version wird mit der Umgebungsvariablen JAVA_HOME eingestellt.

JAVA_HOME

Die Umgebungsvariable JAVA_HOME müssen Sie festlegen, wenn Sie die eigene Java-Umgebung verwenden möchten.

Stellen Sie sicher, dass die JRE-Version von IBM Cognos-Produkten unterstützt wird.

Wenn Sie unter Microsoft Windows keine JAVA_HOME-Variable festlegen, werden die mit der Installation bereitgestellten JRE-Dateien verwendet.

Lesen Sie die Informationen in IBM Software-Produktkompatibilitätsberichte (www.ibm.com/support/pages/node/735235) um zu prüfen, ob die verwendete JRE-Umgebung unterstützt wird.

Nicht eingeschränkte JCE-Richtliniendatei

JREs enthalten eine eingeschränkte Richtliniendatei, die die Verwendung bestimmter kryptografischer Algorithmen und Cipher Suites vorschreibt. Wenn Sie ein breiteres Spektrum an Verschlüsselungsalgorithmen und Cipher-Suites benötigen, stehen Ihnen nun standardmäßig Richtliniendateien ohne Einschränkungen ('Unlimited') zur Verfügung. Diese befinden sich an den folgenden Speicherpositionen:

- `installationsposition/ibm-jre/jre/lib/security/policy/unlimited/US_export_policy.jar`
- `installtionsposition/ibm-jre/jre/lib/security/policy/unlimited/local_policy.jar`

Darüber hinaus stehen für das von IBM bereitgestellte Java JCE-Richtliniendateien ohne Einschränkungen auch hier zur Verfügung.

Schritte

1. Starten Sie Cognos Configuration.
2. Klicken Sie auf **Datei** > **Exportieren als...** und exportieren Sie die Konfiguration in einen Textdatei wie z. B. `export_cogstartup.xml` im Ordner `configuration`. Beenden Sie Cognos Configuration.
3. Erstellen Sie eine Sicherungskopie der folgenden Dateien und Ordner:
   - **Dateien**
   - *Installationsposition/configuration/cogstartup.xml*
   - *Installationsposition/configuration/caSerial*
   - **Ordner**
   - *Installationsposition/configuration/csk*
   - *Installationsposition/configuration/certs*
4. Entfernen Sie alle Ordner und Dateien, für die Sie eine Sicherungskopie erstellt haben, **mit Ausnahme** des Ordners *Installationsposition*`/configuration/certs/mobile`. Entfernen Sie alle anderen Dateien im Ordner *Installationsposition*`/configuration/certs`.
5. Benennen Sie die Konfigurationssicherungsdatei, die Sie in **Schritt 2** erstellt haben, in `cogstartup.xml` um.
6. Legen Sie für die Systemumgebungsvariable JAVA_HOME die JRE fest, die verwendet werden soll.
7. Starten Sie Cognos Configuration, speichern Sie die Konfiguration und starten Sie den Server erneut. Alternativ dazu können Sie auch die Befehlszeile im Ordner *Installationsposition*`/bin64` aufrufen und den folgenden Befehl ausführen: `cogconfig.bat -s`.

   Dadurch werden die Schlüssel für die neue JRE erneut generiert.

Ändern der Standardkonfigurationseinstellungen

Bei der Installation von IBM Cognos-Komponenten werden Standardkonfigurationseinstellungen verwendet. Wenn Sie diese Standardwerte aus bestimmten Gründen nicht verwenden möchten, z. B. weil ein Port bereits von einem anderen Prozess verwendet wird, verwenden Sie IBM Cognos Configuration zum Ändern der Werte.

Wenn Sie den Wert einer Eigenschaft ändern, müssen Sie die Konfiguration speichern und anschließend den IBM Cognos-Service neu starten, damit die neuen Einstellungen auf Ihren Computer angewendet werden.

Stellen Sie für verteilte Installationen sicher, dass alle Content Manager-Computer konfiguriert sind, bevor Sie die Standardkonfigurationseinstellungen auf anderen IBM Cognos-Computern ändern. Sie können z. B. folgende Aktionen ausführen:

- Ändern eines URI
- Verwalten der Konfigurationsgruppe
- Konfigurieren kryptografischer Einstellungen
- Konfigurieren von IBM Cognos-Komponenten für die Verwendung von IBM Cognos Application Firewall
- Konfigurieren der Eigenschaften temporärer Dateien
- Aktivieren und Inaktivieren von Services
- Konfigurieren von Schriftarten
- Ändern der Standardschriftart für Berichte
- Speichern der Berichtsausgabe in einem Dateisystem
- Ändern der Position der Landkartendiagramme für Reporting
- Ändern der Benachrichtigungsdatenbank

Nach dem Ändern des Standardverhaltens von IBM Cognos-Komponenten zur Anpassung an Ihre IBM Cognos-Umgebung können Sie einen Authentifizierungsprovider konfigurieren und Framework Manager installieren und konfigurieren.

Port- und URI-Einstellungen

In Abhängigkeit von der Umgebung können bestimmte Elemente des URI geändert werden. Ein IBM Cognos-URI beinhaltet die folgenden Elemente:

Weitere Informationen zu Ports sind im folgenden Abschnitt verfügbar: „Überprüfen der Standardporteinstellungen” auf Seite 5

- Bei einem Content Manager-URI, Dispatcher-URI für externe Anwendungen oder Dispatcher-URI:

  ```
  Protokoll://Hostname_oder_IP:Port/Kontext_Root/Alias_Position
  ```

- Bei einem Gateway-URI oder einem Webinhalt-URI:

  ```
  Protokoll://Hostname_oder_IP:Port/Virtuelles_Verzeichnis/Gateway_Anwendung
  ```

  oder

  ```
  Protokoll://Hostname_oder_IP:Port/Kontext_Root/Alias_Position
  ```

  Wichtig: Stellen Sie bei HTTPS/SSL-Konfigurationen sicher, dass Sie den vollständig qualifizierten Hostnamen für URIs verwenden.

  Die Elemente werden in der folgenden Tabelle beschrieben:

Tabelle 21. IBM Cognos-URI-Elemente und -Beschreibungen

Element	Beschreibung
Protokoll	Gibt das Protokoll an, das zum Anfordern oder Übertragen von Informationen verwendet wird. Dabei handelt es sich entweder um HTTP (Hyper Text Transfer Protocol) oder HTTPS (Hyper Text Transfer Protocol Secure). **Beispiel:** http oder https

Tabelle 21. IBM Cognos-URI-Elemente und -Beschreibungen (Forts.)	
Element	**Beschreibung**
Hostname oder IP	Gibt die Identität des Hosts im Netz an. Sie können eine IP-Adresse, einen Computernamen oder einen vollständigen Domänennamen verwenden. Bei verteilten Installationen müssen Sie das URI-Element "localhost" ändern. Stellen Sie in einer gemischten Umgebung mit UNIX- und Microsoft Windows-Servern sicher, dass Hostnamen von allen Servern in der Umgebung in IP-Adressen aufgelöst werden können. **Beispiel:** localhost oder 192.168.0.1 oder [2001:0db8:0000:0000:0000:148:57ab]:80
Port	Gibt den Port an, den das Hostsystem auf Anforderungen überwacht. Der Standardport für die IBM Cognos Analytics-Services ist Port 9300. Der Standardport für einen Web-Server ist Port 80. **Beispiel:** 9300 oder 80
Kontext-Root	Wird vom Anwendungsserver verwendet, um den Kontext der Anwendung festzustellen, damit die Anforderung zur Verarbeitung an die entsprechende Webanwendung geleitet werden kann. **Beispiel:** p2pd
Alias-Pfad	Wird vom Anwendungsserver verwendet, um eine Anforderung innerhalb der Webanwendung an die entsprechende Komponente zu leiten. Der Alias-Pfad darf nicht geändert werden, da die IBM Cognos-Komponenten sonst nicht ordnungsgemäß ausgeführt werden. **Beispiel:** servlet/dispatch
Virtuelles Verzeichnis	Wird vom Web-Server verwendet, um eine physische Position zu einem virtuellen Verzeichnis oder einem Alias zuzuordnen. Das virtuelle Verzeichnis im standardmäßigen Gateway-URI "http://localhost:80/ibmcognos/bi/v1/disp" ist zum Beispiel "ibmcognos/cgi-bin". **Beispiel:** ibmcognos/
Gateway-Anwendung	Gibt den Namen der verwendeten Gateway-Anwendung von Cognos an. Wenn Sie beispielsweise über Common Gateway Interface (CGI) auf IBM Cognos-Komponenten zugreifen, ist die standardmäßige Gateway-Anwendung "cognos.cgi". **Beispiel:** cognos.cgi

Wenn Sie die Zusammenarbeit mit IBM Connections verwenden, stellen Sie sicher, dass Sie bei allen Hostnameneinträgen in IBM Cognos Configuration die vollständige Domäne angeben. Beispiel: Ihr Computer heißt "MeinComputer" und Ihre Domäne lautet **MeineFirma.com**. Geben Sie dann als Wert für "Hostname_oder_IP" den Text **MeinComputer.MeineFirma.com** ein. Die Domäne ist erforderlich, damit IBM Connections den Zugriff ermöglichen kann.

Ändern einer Port- oder URI-Einstellung

Mit der folgenden Prozedur können Sie in IBM Cognos Configuration URI-Eigenschaften ändern.

Wichtig: Sie müssen vollständig qualifizierte Hostnamen in den Werten für die folgenden Felder von Cognos Configuration angeben. Jeder Wert, den Sie angeben, muss auch im Feld **Subject Alternative Name** > **DNS-Namen** oder im Feld **Subject Alternative Name** > **IP-Adressen** angezeigt werden.

- **Umgebung**
  - **Gateway-URI**
  - **Externer Dispatcher-URI**
  - **Interner Dispatcher-URI**
  - **Dispatcher-URI für externe Anwendungen**
  - **Content Manager-URIs**
- **Umgebung** > **Konfigurationsgruppe**
  - **Gruppenkontakthost**
  - **Host für die Koordination von Mitgliedern**
- **Zugriffsschutz** > **Verschlüsselung** > **Cognos**
  - **Allgemeiner Servername**
  - **Subject Alternative Name** > **DNS-Namen**
  - **Subject Alternative Name** > **IP-Adressen**

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Klicken Sie im Fenster **Explorer** auf die entsprechende Gruppe oder Komponente:
   - Um ein Element für den Dispatcher zu ändern, klicken Sie auf **Umgebung**.
   - Um ein Element für den lokalen Protokollserver zu ändern, klicken Sie unter **Umgebung** auf **Protokollieren**.
3. Klicken Sie im Fenster **Eigenschaften** auf das Feld **Wert** neben der URI-Eigenschaft, die Sie ändern möchten.
4. Wählen Sie das Element aus und geben Sie die neue Information ein.
   - Zum Ändern des vom lokalen Dispatcher verwendeten Ports ändern Sie den Wert für die Eigenschaft 'Interner Dispatcher-URI'. Da sich die Änderung auf alle URIs auswirkt, die auf dem lokalen Dispatcher basieren, müssen Sie die URIs aller lokalen Komponenten ändern.
   - Wenn Sie den Dispatcher-Port im Dispatcher-URI ändern, müssen Sie bei der Konfiguration von fernen Computern, die auf Dispatcher-, Content Manager- oder Software Development Kit-Services dieses Systems zugreifen, die neuen Portnummern verwenden.
   - Stellen Sie bei HTTPS/SSL-Konfigurationen sicher, dass Sie den vollständig qualifizierten Hostnamen für URIs verwenden.
5. Klicken Sie im Menü **Datei** auf **Speichern**.

Konfigurationseinstellungen überprüfen

Mit dieser Funktion können Sie Einstellungen in Cognos Configuration überprüfen und Konflikte umgehen.

Wichtig: Sie müssen vollständig qualifizierte Hostnamen in den Werten für die folgenden Felder von Cognos Configuration angeben. Jeder Wert, den Sie angeben, muss auch im Feld **Subject Alternative Name** > **DNS-Namen** oder im Feld **Subject Alternative Name** > **IP-Adressen** angezeigt werden.

- **Umgebung**
  - **Gateway-URI**

  - **Externer Dispatcher-URI**
  - **Interner Dispatcher-URI**
  - **Dispatcher-URI für externe Anwendungen**
  - **Content Manager-URIs**
- **Umgebung** > **Konfigurationsgruppe**
  - **Gruppenkontakthost**
  - **Host für die Koordination von Mitgliedern**
- **Zugriffsschutz** > **Verschlüsselung** > **Cognos**
  - **Allgemeiner Servername**
  - **Subject Alternative Name** > **DNS-Namen**
  - **Subject Alternative Name** > **IP-Adressen**

Vorgehensweise

1. Starten Sie **Cognos Configuration**.
2. Wählen Sie das Aktionselement und dann **Überprüfen** aus.
3. Ohne Starten des Cognos Analytics-Servers können die folgenden Aktionselemente überprüft werden, um die Gültigkeit sicherzustellen.
   - **Umgebung** > **Externer Dispatcher-URI**
   - **Umgebung** > **Interner Dispatcher-URI**
   - **Umgebung** > **Portnummer für Dataset-Service**
   - **Umgebung** > **Protokollierung** > **Portnummer des lokalen Protokollservers**
   - **Umgebung** > **Konfigurationsgruppe** > **Mitgliedersynchronisationsport**
   - **Umgebung** > **Konfigurationsgruppe** > **Mitgliederkoordinationsport**
4. Überprüfen Sie, ob die Einstellungen im Abschnitt **Umgebung** > **Konfigurationsgruppe** richtig konfiguriert sind. Diese Einstellungen müssen so konfiguriert werden, dass sie mit dem aktiven Content Manager-Server übereinstimmen.

Verwalten der Konfigurationsgruppe

Die Konfigurationsgruppe definiert eine Gruppe von Servern, die die Konfiguration gemeinsam nutzen. Dies ist bei Installationen mit mehreren Servern wichtig, damit Konfigurationswerte auch nach Netzpartitionierungen auf allen Knoten verfügbar und konsistent bleiben. Der Kontakthost der Konfigurationsgruppe wird auf derselben Instanz wie der aktive Content Manager ausgeführt.

Informationen zu diesem Vorgang

- Bei einer Installation des Typs **Easy Install** sind diese Werte für Sie festgelegt.
- Bei einer **benutzerdefinierten** Installation werden die Host- und Porteigenschaften während der Installation vorab ausgefüllt. Sie müssen jedoch die im Folgenden aufgeführten Schritte ausführen, um zu überprüfen, ob die vorab eingetragenen Einstellungen für Ihre Umgebung geeignet sind.

Vorgehensweise

1. Starten Sie Cognos Configuration.
2. Klicken Sie im Fenster **Explorer** unter **Lokale Konfiguration** auf **Umgebung**.
3. Klicken Sie auf **Konfigurationsgruppe**.
4. Geben Sie die Werte für **Einstellungen des lokalen Mitglieds** an.
   a) Legen Sie die Werte für den **Mitgliedersynchronisationsport** und den **Mitgliederkoordinationsport** fest.

Wichtig: Diese beiden Ports müssen sowohl für den eingehenden als auch den ausgehenden Datenverkehr geöffnet sein.

Stellen Sie sicher, dass es sich bei den beiden Ports um zwei verschiedene lokale Ports handelt, die nicht verwendet werden. Wenn während der Installation alle Anwendungen auf Ihrem Computer aktiv waren, sollten diese Ports bereits unter Verwendung verfügbarer Ports festgelegt worden sein.

- Der **Mitgliedersynchronisationsport** ist der lokale Port, der für die Netzkommunikation verwendet wird und über den Konfigurationsinformationen zwischen den Servern übertragen und synchronisiert werden. Jede Installation muss mit `MutualAuthSSLHttpEndpoint` in den anderen Installationen kommunizieren können. So müssen beispielsweise alle Firewalls zwischen der Anwendungs- und der Datenebene an diesem Port geöffnet sein. "httpEndpoint" wird speziell für die interne Kommunikation zwischen Cognos Analytics-Instanzen verwendet. Der Standardwert lautet 4300.
- Der **Mitgliederkoordinationsport** ist der lokale Port, der für die Netzkommunikation zur Gruppenkoordination verwendet wird. Dieser Port wird dazu verwendet, eine Gruppe zu erkennen und zu verknüpfen und eine aktuelle Liste der Konfigurationsgruppenmitglieder zu verwalten. In der primären Content Manager-Installation ist der Gruppenkontaktport derselbe Port. Jede Installation muss mit den anderen Installationen über den Gruppenkoordinationsport kommunizieren können, d. h., alle Firewalls zwischen den Installationsebenen müssen für diesen Port geöffnet sein. Der Standardwert lautet 5701.

b) Konfigurieren Sie die Eigenschaft **Host für die Koordination von Mitgliedern**.

Diese Einstellung gibt den lokalen Hostnamen für die Koordination der Netzkommunikation innerhalb der Konfigurationsgruppe an.

Gehen Sie wie folgt vor, wenn Ihr Computer nur über einen einzigen Netzadapter verfügt:

Legen Sie als Wert für **Host für die Koordination von Mitgliedern** den vollständig qualifizierten Domänennamen (FQDN) des lokalen Computers fest.

Gehen Sie wie folgt vor, wenn Ihr Computer über mehrere Netzadapter verfügt:
Entscheiden Sie sich für eine der folgenden Methoden:

- Legen Sie als Wert für **Host für die Koordination von Mitgliedern** eine bestimmte IP-Adresse fest, um sicherzustellen, dass der richtige Adapter vom Produkt verwendet wird.

  ODER

- Verwenden Sie die folgende auf einen Musterabgleich bezogene Methode:

  i) Legen Sie als Wert für **Host für die Koordination von Mitgliedern** den vollständig qualifizierten Domänennamen (FQDN) des lokalen Computers fest.

  ii) Bearbeiten Sie die Datei *installation_location*`/wlp/usr/servers/cognosserver/bootstrap.properties` und fügen Sie den folgenden Eintrag zum Angeben eines Musters hinzu, das dem richtigen Adapter entspricht:

  ```
  com.ibm.bi.jgroups.matchaddress=matched_pattern
  ```

  Dabei kann *matched_pattern* eines von zwei Formaten aufweisen:

  – `match-address:`*IP_address_pattern*

  Dieses Format gibt den richtigen Adapter an, indem die IP-Adresse des Adapters mit einem IP-Adressmuster abgeglichen wird.

  Fügen Sie beispielsweise die folgende Zeile in der Datei `bootstrap.properties` hinzu:

  `com.ibm.bi.jgroups.matchaddress=match-address:10\\..*`, womit eine beliebige IP-Adresse, die mit `10.` beginnt (z. B. `10.1.2.3`), als Entsprechung gewertet wird

  Tipp: Die korrekte Syntax für die Adresse für den Abgleich lautet `match-address:`*n*`\..*` (d. h. unter Verwendung eines einzigen umgekehrten Schrägstrichs). Im

obigen Beispiel wird von Ihnen jedoch die Datei `bootstrap.properties` bearbeitet. In `.properties` -Dateien stellt der umgekehrte Schrägstrich (\) jedoch ein Sonderzeichen dar. Sie müssen deshalb einen zusätzlichen umgekehrten Schrägstrich hinzufügen.

- `match-address:`*`name_pattern`*

  Dieses Format gibt den richtigen Adapter an, indem der Adapternamen mit einem Namensmuster abgeglichen wird.

  Fügen Sie beispielsweise die folgende Zeile in der Datei `bootstrap.properties` hinzu:

  `com.ibm.bi.jgroups.matchaddress=match-interface:eth.*`, womit jeder Adapter als Übereinstimmung gewertet wird, dessen Name mit `eth` beginnt, z. B. `eth2`

Weitere Informationen zu der zuvor beschriebenen Methode für Musterabgleich finden Sie auf den folgenden Websites:

- http://www.jgroups.org/manual/index.html#Transport
- https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html

5. Konfigurieren Sie die Eigenschaften für die **Gruppeneinstellungen**.

   Die drei Eigenschaften für die **Gruppeneinstellungen** definieren die Konfigurationsgruppe, über die die Konfiguration zur gemeinsamen Nutzung zur Verfügung gestellt wird. Sie müssen auf allen Cognos Analytics-Servern in Ihrer verteilten Umgebung dieselben Werte festlegen.

   a) Legen Sie auf dem Computer, auf dem der primäre Content Manager-Server installiert ist, die folgenden Werte fest:

   - **Gruppenname**

     Wählen Sie einen Namen für die Gruppe aus.

   - **Gruppenkontaktport**

     Legen Sie denselben Wert fest, den Sie auch für die Eigenschaft **Mitgliederkoordinationsport** verwendet haben.

   - **Gruppenkontakthost**

     Legen Sie denselben vollständig qualifizierten Domänennamen dieses Computers fest, den Sie auch für die Eigenschaft **Host für die Koordination von Mitgliedern** festgelegt haben.

   b) Legen Sie auf jedem der übrigen Computer in der verteilten Umgebung dieselben Werte fest, die Sie auf dem primären Content Manager-Server verwendet haben:

   - **Gruppenname**

     Geben Sie denselben Namen ein, den Sie auf dem primären Content Manager-Server festgelegt haben.

   - **Gruppenkontaktport**

     Legen Sie denselben Wert fest, den Sie auf dem primären Content Manager-Server angegeben haben.

   - **Gruppenkontakthost**

     Legen Sie denselben Wert fest, den Sie auf dem primären Content Manager-Server angegeben haben.

   Tipp: Die Werte können auf einem Computer, bei dem es sich nicht um den primären Content Manager-Server handelt, auch mit einer anderen Methode festgelegt werden, die die folgenden Schritte umfasst:

   i) Klicken Sie mit der rechten Maustaste auf **Konfigurationsgruppe** und klicken Sie dann auf die Schaltfläche **Abrufen**, um das Dialogfeld**Konfigurationsserver abrufen** zu öffnen.

Falls für den aktiven Content Manager SSL aktiviert ist, können Sie die Eigenschaften der Konfigurationsgruppe abrufen, **nachdem** die Content Manager-URL und andere Eigenschaften korrekt konfiguriert und gespeichert wurden.

ii) Geben Sie die entsprechenden Informationen für den Zugriff auf den aktiven Content Manager-Server ein und klicken Sie anschließend auf **OK**.

Benutzer-ID - Die ID mit Administratorberechtigung auf dem Server.

Kennwort - Das Kennwort für die Benutzer-ID.

Namespace-ID - Der Wert ist in der Ressource **Sicherheit**, **Authentifizierung** verfügbar. Beispiel: `CognosEx`

Cognos Analytics-URL - Die URL, die für die Ausführung von Cognos Analytics verwendet wird. Beispiel: `http://myserver:9300/bi`

6. Speichern Sie die Konfiguration.

Konfigurieren von kryptografischen Einstellungen

IBM Cognos-Komponenten benötigen einen Verschlüsselungsprovider, da sie ansonsten nicht ausgeführt werden können. Wenn Sie den standardmäßigen Verschlüsselungsprovider löschen, müssen Sie stattdessen einen anderen Provider konfigurieren.

Sie können die folgenden kryptografischen Einstellungen konfigurieren:

- allgemeine kryptografische Einstellungen
- Einstellungen für den standardmäßigen Verschlüsselungsprovider

Konfigurieren allgemeiner kryptografischer Einstellungen

In einer verteilten Installation kommunizieren IBM Cognos-Computer mit Content Manager, um eine Vertrauensbasis aufzubauen und die Verschlüsselungsschlüssel von Content Manager zu erhalten.

Wenn Sie die Verschlüsselungsschlüssel in Content Manager ändern, indem Sie beispielsweise Anwendungsserver ändern oder Content Manager neu installieren, müssen Sie die Schlüssel auf den anderen IBM Cognos-Computern löschen. Anschließend müssen Sie die Konfiguration auf jedem Computer speichern, sodass sie die neuen Verschlüsselungsschlüssel von Content Manager erhalten. Darüber hinaus müssen alle IBM Cognos-Komponenten in einer verteilten Installation mit denselben Verschlüsselungsprovider-Einstellungen konfiguriert werden.

Außerdem sollte in einer verteilten Umgebung der Symmetric Key nur auf Computern gespeichert werden, auf denen Content Manager installiert ist.

Sie können die folgenden allgemeinen kryptografischen Einstellungen konfigurieren:

- Einhaltung von Standards

  Gibt an, welche Verschlüsselungsstandards verwendet werden sollen, IBM Cognos oder NIST SP 800-131A.

- Eigenschaften des Common-Symmetric-Keystore (CSK)

  Der CSK wird von IBM Cognos zum Ent- und Verschlüsseln von Daten verwendet.

- SSL-Einstellungen (Einstellungen für Secure Sockets Layer)

  Hierzu gehören Einstellungen für gegenseitige Authentifizierung, Vertraulichkeit und SSL Transport Layer Security.

  Anmerkung: Transport Layer Security besteht aus einem Satz von Verschlüsselungsregeln, der geprüfte Zertifikate und Verschlüsselungsschlüssel verwendet, um die Kommunikation über das Internet zu sichern. TLS ist eine Aktualisierung des SSL-Protokolls. Wählen Sie 1.1, 1.2 oder die Kombinationseinstellung aus.

- Erweiterte Algorithmuseinstellungen

  Dazu zählen Signier- und Hashalgorithmen.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** auf **Verschlüsselung**.
3. Ändern Sie im Fenster **Eigenschaften** die Standardwerte, indem Sie auf das Feld **Wert** klicken und den entsprechenden Wert auswählen:
   - Die Optionen für die Umsetzung der Einhaltung von Standards sind IBM Cognos und NIST SP 800-131A. Durch den ausgewählten Wert kann das Speichern fehlschlagen, wenn bei dem ausgewählten Standard keine anderen Parameter zulässig sind. Sie müssen den ausgewählten Algorithmus oder die Konformität mit dem Standard entsprechend ändern. Möglicherweise müssen Sie die JRE-Standortrichtliniendateien ohne Einschränkungen installieren, um alle unterstützten Algorithmen zu aktivieren. Diese stehen bei IBM zur Verfügung.
   - Wenn Sie auf Computern ohne Content Manager die CSKs nicht lokal speichern möchten, ändern Sie unter **CSK-Einstellungen** die Option **Common Symmetric Key lokal speichern** in **Falsch**.

     Wenn **Common Symmetric Key lokal speichern** auf **Falsch** eingestellt ist, wird der Schlüssel bei Bedarf von Content Manager abgerufen. Die Eigenschaft **Common-Symmetric-Keystore-Verzeichnis** wird ignoriert.
   - Wenn die Identität der Computer an beiden Übertragungsenden überprüft werden soll, ändern Sie unter **SSL-Einstellungen** die Option **Gegenseitige Authentifizierung verwenden** in **Wahr**.

     Ändern Sie nicht die Einstellung **Chiffrieren**.
   - Wenn Sie die Hashalgorithmen ändern möchten, wählen Sie für die Eigenschaft **Hashalgorithmus** einen anderen Wert aus.
4. Klicken Sie im Menü **Datei** auf **Speichern**.
5. Testen Sie den Verschlüsselungsprovider nur auf einem Gateway-Computer. Klicken Sie im Fenster **Explorer** mit der rechten Maustaste auf **Verschlüsselung** und klicken Sie auf **Test**.

   Die IBM Cognos-Komponenten prüfen die Verfügbarkeit des Symmetric Key.

Ergebnisse

Nach der Konfiguration der kryptografischen Einstellungen werden die Kennwörter in Ihrer Konfiguration und sämtliche Daten, die Sie erstellen, verschlüsselt.

Konfigurieren des Standardverschlüsselungsproviders

Sie können für den Standardverschlüsselungsprovider einige kryptografische Einstellungen konfigurieren.

Folgende Einstellungen können konfiguriert werden:

- Algorithmen und Cipher-Suites
- Einstellungen für den Namen der Identität
- Einstellungen für Verschlüsselungs-Keystore

  Zum Schlüsselpaar für die Verschlüsselung gehören der private Schlüssel, der zum Verschlüsseln der Daten verwendet wird, sowie der öffentliche Schlüssel, der zum Entschlüsseln der Daten verwendet wird.
- Einstellungen für Zertifizierungsstelle

  Die Zertifizierungsstelle (Certificate Authority, CA) ist entweder die standardmäßige Zertifizierungsstelle oder eine andere Zertifizierungsstelle.
- Einstellungen für den alternativen Subjektnamen

  Der alternative Subjektname (Subject Alternative Name, SAN) wird zum Überprüfen des Ursprungs eines SSL-Zertifikats verwendet.

Vorgehensweise

1. Wenn Sie eine JRE verwenden, bei der es sich nicht um die mit dem IBM Cognos-Server bereitgestellte JRE handelt, rufen Sie das Verzeichnis *Installationsposition*/ibm-jre/jre/lib/ext auf.
2. Kopieren Sie die Datei bcprov-jdk*Version*.jar in das Verzeichnis *JRE_Position*/lib/ext.
3. Wenn Sie eine andere als die von IBM bereitgestellte JRE verwenden, müssen Sie auch die uneingeschränkte JCE-Richtliniendatei (JCE = Java Cryptograph Extension) für Ihre JRE herunterladen und installieren, um sicherzustellen, dass alle verfügbaren Algorithmen und Cipher Suites in IBM Cognos Configuration angezeigt werden.
4. Starten Sie IBM Cognos Configuration.
5. Klicken Sie im Fenster **Explorer** unter **Sicherheit**: **Verschlüsselung** auf **Cognos**.
6. Legen Sie im Fenster **Eigenschaften** die Eigenschaften wie erforderlich fest.

   Tipp: Detaillierte Informationen zu den einzelnen Eigenschaften finden Sie in der Eigenschaftsbeschreibung in IBM Cognos Configuration, wenn Sie auf die Eigenschaft klicken.

   - Um den Datenschutzalgorithmus zu konfigurieren, klicken Sie unter der betreffenden Eigenschaft (**Datenschutzalgorithmus** oder **PDF-Datenschutzalgorithmus**) auf die Spalte **Wert** und wählen Sie aus der Dropdown-Liste den Algorithmus aus.

     Mit dem Wert eines Datenschutzalgorithmus wird festgelegt, wie Daten von den IBM Cognos-Komponenten verschlüsselt werden. In IBM Cognos Configuration eingegebene Datenbankkennwörter werden beispielsweise beim Speichern der Konfiguration verschlüsselt. Der für die Datenverschlüsselung gewählte Algorithmus muss auch für Daten verfügbar sein, die zu einem späteren Zeitpunkt verschlüsselt werden.

     Wenn Änderungen an der Umgebung vorgenommen werden, kann sich dadurch auch die Verfügbarkeit der Chiffrieralgorithmen ändern. Das ist zum Beispiel dann der Fall, wenn die Java Runtime Environment (JRE) geändert wurde, oder wenn Sie auf dem Computer weitere Verschlüsselungssoftware installiert haben. Daher müssen Sie sicherstellen, dass der zur Verschlüsselung der Daten gewählte **Datenschutzalgorithmus** auch beim Zugriff auf die Daten verfügbar ist.

     JREs enthalten eine eingeschränkte Richtliniendatei, die die Verwendung bestimmter kryptografischer Algorithmen und Cipher Suites vorschreibt. Wenn Sie ein breiteres Spektrum an Verschlüsselungsalgorithmen und Cipher-Suites benötigen, stehen Ihnen nun standardmäßig Richtliniendateien ohne Einschränkungen ('Unlimited') zur Verfügung. Diese befinden sich an den folgenden Speicherpositionen:

     – installationsposition/ibm-jre/jre/lib/security/policy/unlimited/US_export_policy.jar
     – installtionsposition/ibm-jre/jre/lib/security/policy/unlimited/local_policy.jar

     Darüber hinaus stehen für das von IBM bereitgestellte Java JCE-Richtliniendateien ohne Einschränkungen auch hier zur Verfügung.
   - Klicken Sie zum Anpassen der Cipher Suites unter **Unterstützte Cipher Suites** in die Spalte **Wert** und dann auf das Bearbeitungssymbol  .

     Entfernen Sie die Cipher Suites, die nicht zutreffend sind, und verschieben Sie die verbleibenden Cipher Suites in der Liste so nach oben oder unten, das die Cipher Suites im höchsten Bereich in der Liste weiter oben stehen.

     Trennen Sie Cipher Suites im 40- bis 56-Bit-Bereich von Cipher Suites im 128- bis 168-Bit-Bereich.
   - Zum Ändern der Speicherposition der Verschlüsselungsschlüssel müssen Sie unter **Einstellungen für Verschlüsselungsschlüssel** die Option **Encryption-Keystore-Verzeichnis** in die neue Position ändern.
   - Um eine andere Zertifizierungsstelle zu verwenden, ändern Sie unter **Einstellungen für Zertifizierungsstelle** die Option **Zertifizierungsstelle eines anderen Anbieters verwenden** in **Wahr**.

Weitere Informationen finden Sie im Abschnitt „Konfigurieren von Cognos Analytics-Komponenten für die Verwendung einer anderen Zertifizierungsstelle” auf Seite 204.

- Wenn Sie die Konfiguration für HTTPS/SSL ausführen, ändern Sie den allgemeinen Servernamen von CAMUSER in den vollständig qualifizierten Domänenname des Servers.
- Zum Konfigurieren von **Alternativer Subjektname** geben Sie **DNS-Namen**, **IP-Adressen** und **E-Mail-Adressen** (optional) an, die dem Serverzertifikat zugeordnet sind. Die Werte werden den Erweiterungen für den alternativen Subjektnamen im Serverzertifikat hinzugefügt. Sie können für jede Eigenschaft mehrere Werte angeben. Trennen Sie die Werte durch das Leerzeichen voneinander.

7. Klicken Sie im Menü **Datei** auf **Speichern**.

Ergebnisse

Wenn Sie den Server einer anderen Zertifizierungsstelle verwenden, konfigurieren Sie die IBM Cognos-Komponenten für die Verwendung dieser Zertifizierungsstelle. Weitere Informationen finden Sie im Abschnitt „Konfigurieren von Cognos Analytics-Komponenten für die Verwendung einer anderen Zertifizierungsstelle” auf Seite 204.

IBM Cognos Application Firewall

IBM Cognos Application Firewall analysiert und überprüft HTTP- und XML-Anforderungen, bevor diese von IBM Cognos-Servern verarbeitet werden. IBM Cognos Application Firewall kann diese HTTP- und XML-Anforderungen ändern.

Durch IBM Cognos Application Firewall werden die Webprodukte von IBM Cognos vor zerstörerischen Daten geschützt. Pufferüberläufe und websiteübergreifende Scriptangriffe (XSS-Angriffe) - entweder durch die sogenannte "Script Injection" in gültige Seiten oder durch die Umleitung auf eine andere Website - sind die häufigsten Formen zerstörerischer Daten.

Sie können Firewall-Aktivitäten verfolgen, indem Sie die Protokolldatei überprüfen, die abgewiesene Anforderungen enthält. Standardmäßig werden Protokollnachrichten in der Datei *installationsposition*`/logs/cogaudit.log` gespeichert.

Wenn Sie die Zusammenarbeitsfunktionen mit IBM Connections verwenden, müssen Sie bei den Eigenschaften der Cognos Application Firewall unter **Gültige Domänen oder Hosts** den Hostnamen, die Domäne und die Portnummer hinzufügen, unter denen IBM Connections ausgeführt wird.

In einer verteilten Umgebung müssen alle Cognos Application Firewall-Einstellungen aller Computer, auf denen IBM Cognos-Komponenten der Anwendungsebene installiert sind, identisch sein. Wenn Cognos Application Firewall z. B. auf einigen Computern aktiviert und auf anderen Computern inaktiviert ist, können unerwartete Reaktionen und Produktfehler auftreten.

Die folgenden URL-Typen werden bei der Cognos Application Firewall-Überprüfung akzeptiert:

- vollständige (absolute) URLs

  im Format *Protokoll*://*Host*:*Port*/*Pfad*, wobei *Protokoll* http oder https ist und *Host* mit der Liste gültiger Domänen überprüft wird
- URLs relativ zum Web-Installationsverzeichnis

  im Format /*web-installationsverzeichnis*/.*, wobei *web-installationsverzeichnis* das Gateway-Web-Verzeichnis basierend auf dem Alias ibmcognos ist, den Sie auf dem Web-Server konfiguriert haben.

  Zum Beispiel

  /ibmcognos/ps/portal/images/action_delete.gif
- spezielle zulässige URLs, einschließlich folgender (jeweils unter Beachtung der Groß- und Kleinschreibung)

  about:blank

  JavaScript:window.close( )

  JavaScript:parent.close( )

JavaScript:history.back( )

parent.cancelErrorPage( )

doCancel( )

Konfigurieren von IBM Cognos-Komponenten für die Verwendung von IBM Cognos Application Firewall

Mit IBM Cognos Configuration können Sie die Einstellungen für die Unterstützung anderer XSS-Tools ändern und Sie können Host- und Domänennamen der IBM Cognos-Liste gültiger Namen hinzufügen.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration an jeder Installationsposition der Komponenten auf Anwendungsebene.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** auf **IBM Cognos Application Firewall**.
3. Stellen Sie im Fenster **Eigenschaften** die richtigen Werte für die Eigenschaft **Soll die CAF-Überprüfung aktiviert werden?** ein.

   IBM Cognos Application Firewall ist standardmäßig aktiviert.

   Wichtig: IBM Cognos Application Firewall ist eine wichtige Komponente der IBM Cognos-Sicherheit, die dem Schutz gegen unberechtigte Zugriffe dient. Wenn Sie IBM Cognos Application Firewall inaktivieren, ist dieser Schutz nicht mehr vorhanden. Unter normalen Umständen empfiehlt es sich nicht, IBM Cognos Application Firewall zu inaktivieren.
4. Wenn Sie ein anderes XSS-Tool verwenden, das Parameter von GET-Anforderungen auf bestimmte Zeichen überprüft, ändern Sie im Fenster **Eigenschaften** den Wert für die Eigenschaft **Ist die XSS-Überprüfung durch Drittanbieter aktiviert?** in **Wahr**.

   Wenn diese Eigenschaft bei SiteMinder auf **True** gesetzt wird, werden die Standardwerte für **BadURLChars** und **BadCSSChars** durch Cognos Analytics maskiert. Die HTTP-Verben PUT und DELETE werden ebenfalls maskiert.

   Beispiele für **BadURLChars** und **BadCSSChars** sind: eine Tilde (~), ein Punkt (.), ein Punkt und ein Schrägstrich (./), ein Größer-als-Zeichen (>) und mehr. Weitere Informationen finden Sie in der SiteMinder-Dokumentation.
5. Fügen Sie der IBM Cognos-Liste der gültigen Namen Host- und Domänennamen hinzu:
   - Klicken Sie auf den Wert für die Eigenschaft **Gültige Domänen oder Hosts** und dann auf das Bearbeitungssymbol  .
   - Klicken Sie im Dialogfeld **Wert - Gültige Domänen oder Hosts** auf **Hinzufügen**.

     Sie müssen die Domänen aller Hyperlinks mit einschließen, die im Portal hinzugefügt werden. Weitere Informationen finden Sie im Abschnitt über das Erstellen einer URL im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit*.

     Tipp: Wenn Sie Drillthrough-Vorgänge von IBM Cognos Series 7 zu Berichten in IBM Cognos Analytics durchführen wollen, fügen Sie die Hostnamen der IBM Cognos Series 7-Gateway-Server der Liste hinzu.
   - Klicken Sie in die leere Tabellenzeile und geben Sie den Host- oder Domänennamen ein.

     Um eine Domäne und alle ihre Unterdomänen zuzulassen, geben Sie am Anfang des Domänennamens einen Platzhalter ein. Beispiel: `*.mycompany.com`.

     Wenn Sie die Funktionen für die Zusammenarbeit von IBM Connections verwenden, müssen Sie Hostname, Domäne und Portnummer für das IBM WebSphere-Profil hinzufügen, unter dem IBM Connections installiert ist. Beispiel: Wenn Sie IBM Connections auf einem Computer mit der Bezeichnung **MeinServer** installiert haben und Ihre Domäne **MeineFirma.com** lautet, fügen Sie **MeinSer-**

ver.MeineFirma.com:9080 hinzu, wobei 9080 für die Nummer des IBM WebSphere-Ports steht, auf dem IBM Connections ausgeführt wird.

- Wiederholen Sie die vorherigen beiden Punkte für jeden hinzuzufügenden Namen.
- Klicken Sie auf **OK**.

IBM Cognos Application Firewall überprüft Domänen- und Hostnamen, um URLs zu schützen, die erstellt werden. Standardmäßig sieht IBM Cognos Application Firewall Domänennamen, die aus den Umgebungskonfigurationseigenschaften abgeleitet wurden, als sichere Domänennamen an. Das Hinzufügen von Namen zur Liste gültiger Namen ist besonders dann nützlich, wenn Sie mithilfe der Funktionen "Zurück" oder "Abbrechen" Anforderungen an Computer ohne IBM Cognos umleiten müssen oder wenn Sie Drillthrough-Vorgänge zu verschiedenen IBM Cognos-Produktinstallationen durchführen.

6. Speichern Sie die Konfiguration.
7. Starten Sie die Services erneut.

Verschlüsseln der Eigenschaften von temporären Dateien

Temporäre Dateien werden in IBM Cognos Analytics verwendet, um kürzlich angezeigte Berichte und von den Services während der Verarbeitung verwendete Daten zu speichern. Sie können den Pfad der temporären Dateien ändern und ihren Inhalt verschlüsseln lassen.

Standardmäßig speichern IBM Cognos-Komponenten temporäre Dateien im Verzeichnis *installationsposition*\temp, ohne sie zu verschlüsseln.

Für optimale Sicherheit sollten Sie außer für das Servicekonto, mit dem der IBM Cognos-Service gestartet wird, keinerlei Zugriffsberechtigungen für das Verzeichnis temp gewähren. Für das Servicekonto sind Lese- und Schreibberechtigungen erforderlich.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Geben Sie im Fenster **Eigenschaften** den neuen Pfad für die Eigenschaft **Temporäre Dateien - Verzeichnis** an.
4. Wenn der Inhalt der temporären Dateien verschlüsselt werden soll, setzen Sie die Eigenschaft **Verschlüsseln temporärer Dateien** auf **Wahr**.
5. Vergewissern Sie sich, dass das Benutzerkonto, unter dem IBM Cognos Analytics-Komponenten ausgeführt werden, über die entsprechenden Berechtigungen für den Pfad zu den temporären Dateien verfügt. Beispiel:
   - Microsoft Windows: uneingeschränkte Zugriffsberechtigungen
   - UNIX oder Linux: Lese- und Schreibberechtigungen

Aktivieren und inaktivieren von Services

In einer verteilten Installation können Sie bestimmte Arten von Anforderungen an bestimmte Computer senden, indem Sie die installierten Services aktivieren bzw. inaktivieren.

Um beispielsweise einen Computer für die Ausführung und Verteilung von Berichten abzustellen, können Sie den Präsentationsservice auf einem Computer mit Komponenten der Anwendungsebene inaktivieren.

Anmerkung: Die Standardwerte für den Dispatcher- und Präsentationsservice gelten nicht für Computer, auf denen nur Content Manager installiert ist. Bei allen anderen Installationsarten treffen die Werte zu.

Wenn alle Komponenten auf mehreren Computern installiert sind, können Sie bestimmte Services auf einigen Computern inaktivieren, um die gewünschte Verteilung zu erzielen. Anforderungen werden nur an Dispatcher gesendet, auf denen ein bestimmter Service aktiviert ist.

Wird ein Service inaktiviert, kann dieser nichts mehr in den Arbeitsspeicher laden. Inaktivierte Services werden nicht gestartet und beanspruchen daher auch keine Ressourcen. Ein Service wird erst ausgeführt, nachdem er aktiviert wurde.

Wenn Sie den Dispatcher-Service inaktivieren, sind die Dispatcher-bezogenen Services inaktiviert. Nur aktivierte Dispatcher-Services können Anforderungen verarbeiten.

Einschränkung: Beim manuellen Starten von Services muss gegebenenfalls der Service **ApacheDS - cognos** vor dem Service **IBM Cognos** gestartet werden.

Aktivieren und Inaktivieren von Services

Gehen Sie folgendermaßen vor, um ausgewählte Services für Komponenten in einer verteilten Installation zu inaktivieren.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Klicken Sie im Fenster **Explorer** unter **Umgebung** auf **IBM Cognos-Services**.
3. Klicken Sie im Fenster **Eigenschaften** auf den **Wert** neben dem Service, den Sie inaktivieren bzw. aktivieren möchten.

   Standardmäßig sind alle Services aktiviert.
4. Klicken Sie auf den Status der Services:
   - Wenn der Service inaktiviert werden soll, klicken Sie auf **Falsch**.
   - Wenn Sie den Service aktivieren möchten, klicken Sie auf **Wahr**.

   Beim manuellen Starten von Services muss gegebenenfalls der Service **ApacheDS - cognos** vor dem Service **IBM Cognos** gestartet werden.
5. Klicken Sie im Menü **Datei** auf **Speichern**.

Konfigurieren von Abfrageeinstellungen

Um den Datenzugriff zu optimieren, können Sie Parameter konfigurieren, die vom Abfrageservice verwendet werden.

Ändern der Cachegröße dynamischer Abfragen

Wenn der Inhalt eines Benutzers (z. B. ein Dashboard) mehr als 25 Abfragen hat, die gleichzeitig ausgeführt werden sollen, werden einige Abfrageergebnisse möglicherweise nicht geladen. Um dieses Problem zu mildern, können Sie die Werte erhöhen, die dem Parameter `queryReuse` zugeordnet sind.

Informationen zu diesem Vorgang

Die dynamische Abfrage kann die Abfrageausführung verbessern, indem zuvor berechnete Ergebnisse wiederverwendet werden. Wenn Abfragen geplant sind, legt die dynamische Abfrage fest, ob es anwendbare Ergebnisse im Cache gibt, die sie nutzen können. Jede Instanz der dynamischen Abfrage verwaltet einen Cache, der bis zu 250 Einträge aufnehmen kann. Jede Benutzersitzung, die auf diese Instanz zugreift, kann bis zu 25 Einträge in diesem Cache enthalten. Einträge im Cache werden entweder entfernt, weil sie inaktiv sind oder um Speicherplatz für neue Einträge zu schaffen.

Dashboards können zahlreiche Widgets in einer oder mehreren Registerkarten enthalten. Die von diesen Widgets generierten Abfragen können dazu führen, dass Einträge aus dem Cache entfernt werden, um Platz für neue Einträge zu schaffen. Wenn ein Benutzer mit dem Dashboard interagiert, stellt er möglicherweise fest, dass für manche Abfragen mehr Zeit benötigt wird. Dies kann auf die Anzahl der Widgets im Dashboard zurückzuführen sein, die der Benutzer verwendet, und darauf, wie er mit ihnen interagiert.

Tipp: Das Erweitern der Cachegröße erhöht die Speichernutzung und den temporären Plattenspeicherplatz. Bevor Sie die Cachegröße erhöhen, überprüfen Sie, inwieweit Abfragen in Ihre Inhalte integriert sind. Möglicherweise können Ihre Dashboards mit weniger Widgets umgestaltet werden. Oder Sie können

nur selten verwendete Widgets auf eine andere Registerkarte verschieben, damit sie weniger häufig ausgeführt werden.

Vorgehensweise

1. Starten Sie die Administrationskonsole.
2. Führen Sie die Schritte unter "Festlegen der Abfrageserviceeigenschaften" in der Veröffentlichung *Cognos Analytics Administration and Security Guide* aus.
3. Wählen Sie in Schritt **6** der oben beschriebenen Prozedur die Option **Erweiterte Einstellungen** aus.
4. Geben Sie neue Werte für die Parameter **qs.general.queryReuse.size** und **qs.general.queryReuse.data.threshold** ein.
   Beispiel

   Sie möchten die folgenden Änderungen am Abfragecache vornehmen:

   - Erhöhen der maximalen Anzahl von Abfragen pro Benutzer von 25 auf 30.
   - Erhöhen der maximalen Anzahl von Abfragen im globalen Pool auf 350.

   Geben Sie diese *Name*/*Wert*-Paare für **Parameter** und **Wert** ein:

   qs.general.queryReuse.size
   30

   qs.general.queryReuse.data.threshold
   350
5. Klicken Sie im Menü **Aktionen** für **QueryService - *Dispatchername*** auf **Starten**, um den Service erneut zu starten.

Ergebnisse

Der Abfrageservice wird mit den neuen Einstellungen konfiguriert.

Anmerkung: Als Alternative zur Verwendung der Administrationskonsole, die in den vorherigen Schritten beschrieben wurde, können Sie eine Datei `xqe.config.custom.xml` erstellen. Um dieselben Änderungen wie im vorherigen Beispiel vorzunehmen, führen Sie die folgenden Schritte aus:

1. Stoppen Sie den IBM Cognos Analytics-Service.
2. Wechseln Sie in das Verzeichnis *`Installationsposition`*`\configuration`.
3. Wenn die Datei `xqe.config.custom.xml` noch nicht vorhanden ist, kopieren Sie die Datei `xqe.config.xml` und benennen Sie sie in `xqe.config.custom.xml` um.
4. Bearbeiten Sie die Datei `xqe.config.custom.xml`:
   a. Geben Sie den Parameter `queryReuse` und die zugehörigen Werte nach der Zeile `<general>` ein.

```
<queryReuse enabled="true|false" size="Anzahl_der_Abfragen_im_Benutzercache">
   <!-- Aufbewahrung wiederverwendbarer Objekte in Sekunden -->
   <retention maxIdle="Anzahl_Sekunden" maxAge="Anzahl_Sekunden"/>
  <!-- Ergebnissätze, die für wiederverwendbare Objekte aufbewahrt werden. Der Speicher
entspricht dem Maximum pro Ergebnissatz in Megabyte.-->
   <data threshold="Anzahl_der_Abfragen_im_globalen_Cache"/>
</queryReuse>
```

   Beispiel

   Sie möchten die folgenden Änderungen am Abfragecache vornehmen:

   - Erhöhen der maximalen Anzahl von Abfragen pro Benutzer von 25 auf 30.
   - Entfernen Sie die Abfrageergebnisse nach 3600 Sekunden Inaktivität.
   - Erhöhen der maximalen Anzahl von Abfragen im globalen Pool auf 350.

   Fügen Sie die folgenden Zeilen direkt nach der Zeile `<general>` ein:

```
<queryReuse enabled="true" size="30">
   <!-- Aufbewahrung wiederverwendbarer Objekte in Sekunden -->
```

```
   <retention maxIdle="300" maxAge="3600"/>
  <!-- Ergebnissätze, die für wiederverwendbare Objekte aufbewahrt werden. Der Speicher
entspricht dem Maximum pro Ergebnissatz in Megabyte.-->
   <data threshold="350" maxMemory="6"/>
</queryReuse>
```

b. Speichern Sie die Datei `xqe.config.custom.xml`.

5. Starten Sie den IBM Cognos Analytics-Service.

Zurücksetzen auf fehlende Werte in Listenberichten

11.1.7 Die Formateigenschaft `Fehlende Wertzeichen`, die in Framework Manager-Modellen definiert ist, wird jetzt in Listenberichten berücksichtigt.

Informationen zu diesem Vorgang

Wenn in früheren Releases die Formateigenschaft `Fehlende Wertzeichen` für ein Element in einem Framework-Manager-Modell definiert war, wurde es für Kreuztabellenberichte angewendet, aber nicht für Listenberichte. Mit anderen Worten: Nullwerte für das angegebene Modellelement wurden in einem Listenbericht als leer angezeigt und nicht als die in der Formateigenschaft `Fehlende Wertzeichen` definierten Zeichen. Dies war nicht das gewünschte Verhalten und wurde in Release 11.1.7 korrigiert.

Wenn Sie zu dem Verhalten vor Release 11.1.7 zurückkehren möchten, gehen Sie wie folgt vor:

Vorgehensweise

1. Stoppen Sie den IBM Cognos Analytics-Service.
2. Wechseln Sie in das Verzeichnis *Installationsposition*`\configuration`.
3. Wenn die Datei `xqe.config.custom.xml` noch nicht vorhanden ist, kopieren Sie die Datei `xqe.config.xml` und benennen Sie sie in `xqe.config.custom.xml` um.
4. Bearbeiten Sie die Datei `xqe.config.custom.xml`:
   a) Fügen Sie unmittelbar nach der Zeile <queryPlanning> die folgende Zeile hinzu:

```
formatMissingValuesInListReports enabled="false"/>
```

   b) Speichern Sie die Datei `xqe.config.custom.xml`.
5. Starten Sie den IBM Cognos Analytics-Service erneut.

Sicherstellen, dass Stammmitglieder in einer Planning Analytics-Datenquelle mit denen im TM1-Client übereinstimmen

11.1.3 Wenn Sie eine TM1-Datenquelle in Cognos Analytics importieren und den Datenquellentyp als **IBM Planning Analytics** auswählen, kann die Liste der Stammmitglieder in der Metadatenverzeichnisstruktur anders aussehen als die Liste, die im TM1-Client angezeigt wird.

Lösung

Sie können die REST-API `tm1.RootMembers()` aktivieren. Diese REST-API gibt Stammmitglieder von der Planning Analytics-Datenquelle zurück, die mit den vom TM1-Client zurückgegebenen Stammmitgliedern übereinstimmen.

Wichtig: Sie müssen Version 2.0.6 oder höher des Planning Analytics-Servers verwenden.

Führen Sie folgende Schritte aus:

1. Stoppen Sie den IBM Cognos Analytics-Service.
2. Wechseln Sie in das Verzeichnis *Installationsposition*`\configuration`.
3. Wenn die Datei `xqe.config.custom.xml` noch nicht vorhanden ist, kopieren Sie die Datei `xqe.config.xml` und benennen Sie sie in `xqe.config.custom.xml` um.

4. Bearbeiten Sie die Datei `xqe.config.custom.xml`:
   a. Fügen Sie unmittelbar nach der Zeile `<queryExecution>` die folgende Zeile hinzu:

```
<paUseRootMembers enabled="true"/>
```

   b. Speichern Sie die Datei `xqe.config.custom.xml`.
5. Starten Sie den IBM Cognos Analytics-Service.

Füllmitglieder in einem Planning Analytics-Paket inaktivieren

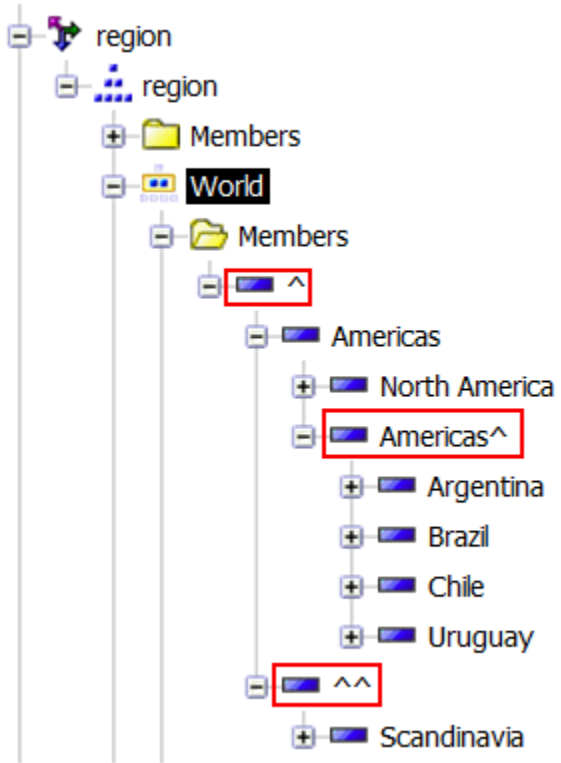
11.1.2 Sie können die automatische Generierung von Füllmitgliedern inaktivieren, sodass ein in Cognos Analytics importiertes Planning Analytics-Paket dieselben Merkmale hat wie im TM1-Client.

In Cognos Analytics werden standardmäßig Füllelemente generiert, um Lücken zu schließen, da der Zugriff vom Stamm der Hierarchie bis zu den Mitgliedern beschränkt ist, deren Daten für den Benutzer sichtbar sind. In IBM Cognos TM1 werden jedoch keine Füllmitglieder generiert.

Beispiel 1: Füllmitglieder aktiviert

Wenn Füllmitglieder aktiviert sind, entspricht die Titelzeile eines Füllmitglieds in der Datenverzeichnisstruktur der Titelzeile des übergeordneten Mitglieds mit angehängtem Winkelzeichen (^). Wenn dem Benutzer kein Zugriff auf ein Stammmitglied erteilt wird, besteht die Titelzeile des Stammmitglieds nur aus einem Winkelzeichen (^).

Eine Metadatenverzeichnisstruktur mit aktivierten Füllmitgliedern wird in der folgenden Abbildung dargestellt:



Ein Diagramm für denselben Cube wird wie folgt angezeigt:

Budget	1 Quarter	2 Quarter	3 Quarter	4 Quarter
*Americas^*				
North America	*825517.05*	*846801.29*	*830379.17*	*868830.05*
Total(children(Am))	**825517.05**	**846801.29**	**830379.17**	**868830.05**

Beispiel 2: Füllmitglieder inaktiviert

Anmerkung: Da der Zugriff auf das Stammmitglied für den Cube in Beispiel 1 eingeschränkt ist, kann der Benutzer, wenn Füllmitglieder inaktiviert sind, keine Mitglieder in der Datenverzeichnisstruktur sehen.

Ein Diagramm von demselben Cube wird wie folgt angezeigt:

Budget	1 Quarter	2 Quarter	3 Quarter	4 Quarter
North America	*825517.05*	*846801.29*	*830379.17*	*868830.05*
Total(children(Am))	**825517.05**	**846801.29**	**830379.17**	**868830.05**

Prozedur

Führen Sie die folgenden Schritte aus, um sicherzustellen, dass eine Datenquelle dieselben Merkmale im TM1-Client und Planning Analytics hat:

1. Stoppen Sie den IBM Cognos Analytics-Service.
2. Wechseln Sie in das Verzeichnis *Installationsposition*\configuration.
3. Wenn die Datei xqe.config.custom.xml noch nicht vorhanden ist, kopieren Sie die Datei xqe.config.xml und benennen Sie sie in xqe.config.custom.xml um.
4. Bearbeiten Sie die Datei xqe.config.custom.xml:
   a. Fügen Sie unmittelbar nach der Zeile <queryExecution> die folgende Zeile hinzu:

```
<!-- Attributwert 'paUseFillerMember enabled' auf 'false' setzen, um Füllmitglied zu inak
tivieren -->
<paUseFillerMember enabled="false"/>
```

   b. Speichern Sie die Datei xqe.config.custom.xml.
5. Starten Sie den IBM Cognos Analytics-Service.

Konfiguration von Schriftarten

IBM Cognos-Produkte verwenden Schriftarten zur Wiedergabe von PDF-Berichten auf dem IBM Cognos-Server. Darüber hinaus werden Schriftarten zur Wiedergabe von Diagrammen in PDF- und HTML-Berichten verwendet.

Eine korrekte Ausgabe ist nur dann gewährleistet, wenn die Schriftarten an der Stelle verfügbar sind, an der der Bericht bzw. das Diagramm ausgegeben werden. Für Diagramme und PDF-Berichte müssen die Schriftarten auf dem IBM Cognos-Server installiert sein. Wenn eine angeforderte Schriftart nicht verfügbar ist, wird sie von den IBM Cognos-Komponenten durch eine andere Schriftart ersetzt.

Da HTML-Berichte in einem Browser ausgegeben werden, müssen die erforderlichen Schriftarten auf dem Computer jedes IBM Cognos-Benutzers installiert sein, der den Bericht aufruft. Wenn eine angeforderte Schriftart nicht verfügbar ist, wird sie durch eine andere Schriftart ersetzt.

Wenn Sie in Ihren Berichten eine neue Schriftart verwenden möchten, gehen Sie anhand der folgenden Prüfliste vor.

__ • Fügen Sie die Schriftart zur Liste der unterstützten Schriftarten hinzu.

__ • Legen Sie den Dateipfad für die neue Schriftart fest.

__ • Ordnen Sie die neue Schriftart dem Namen der physischen Schriftart zu, sofern erforderlich.

Hinweise zur Unterstützung für vereinfachtes Chinesisch

IBM Cognos-Produkte unterstützen den Zeichensatz GB18030-2000, der für die Codierung von Ländereinstellungen mit vereinfachtem Chinesisch verwendet wird.

Bei der Installation auf einem Microsoft Windows-System erfolgt die Unterstützung für den Zeichensatz GB18030-2000 in Form der Schriftart SimSun-18030, die von Microsoft bereitgestellt wird.

Auf anderen Betriebssystemen als Windows müssen Sie eine Schriftart installieren, die GB18030-2000 unterstützt.

Hinzufügen von Schriftarten zur IBM Cognos-Umgebung

Sie können der Liste unterstützter Schriftarten in der IBM Cognos-Umgebung neue Schriftarten hinzufügen, um Berichte mit derzeit nicht verfügbaren Schriftarten zu erstellen. Darüber hinaus können Schriftarten entfernt werden. IBM Cognos-Komponenten verwenden standardmäßig einen globalen Schriftsatz, der auf allen IBM Cognos-Server-Computern verfügbar ist.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf jedem Content Manager-Computer.
2. Klicken Sie im Menü **Aktionen** auf **Globale Konfiguration bearbeiten**.
3. Klicken Sie auf die Registerkarte **Schriftarten**.
4. Klicken Sie auf **Hinzufügen**.

   Tipp: Zum Entfernen einer Schriftart aus der Liste der unterstützten Schriftarten aktivieren Sie das Feld neben dem Namen der Schriftart und klicken Sie anschließend auf **Entfernen**.
5. Geben Sie im Feld **Unterstützter Schriftartenname** den Namen der Schriftart ein und klicken Sie auf **OK**.
6. Klicken Sie im Menü **Datei** auf **Speichern**.

   Die globalen Schriftarten, einschließlich der neu hinzugefügten Schriftarten, müssen auf allen IBM Cognos-Computern in der Umgebung installiert werden.

Ergebnisse

Wenn eine globale Schriftart nicht auf allen IBM Cognos-Computern installiert ist, müssen Sie die globale Schriftart einer installierten, physischen Schriftart zuordnen.

Angeben der Position für verfügbare Schriftarten

Sie müssen das Installationsverzeichnis für alle Schriftarten angeben, einschließlich der Schriftarten, die Sie zur Liste der unterstützten Schriftarten hinzufügen.

Die Liste der Schriftarten umfasst standardmäßig die Schriftarten, die im Verzeichnis *installations-position*\bin\fonts des IBM Cognos-Computers installiert sind. Wenn IBM Cognos-Komponenten auf einem Computer mit einem Microsoft Windows-Betriebssystem installiert sind, verwenden sie darüber hinaus die im Windows-Schriftartverzeichnis installierten Schriftarten.

Sie geben das Schriftartverzeichnis auf allen Computern an, auf denen Komponenten der Anwendungsebene installiert sind.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf allen Computern mit den Komponenten der Anwendungsebene.

2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Legen Sie im Fenster **Eigenschaften** für **Physische Schriftartenverzeichnisse** den Pfad für die Schriftarten fest.

   Wenn mehrere Schriftartenpfade vorhanden sind, trennen Sie die einzelnen Pfade durch ein Semikolon (;) voneinander.

   Wenn Sie einen Anwendungsserver verwenden, bei dem es sich nicht um den mit IBM Cognos Analytics bereitgestellten Anwendungsserver handelt, müssen Sie den vollständig qualifizierten Pfad für die Speicherposition der Schriftarten eingeben. Beispiel: *installationsposition*\bin\fonts.
4. Klicken Sie im Menü **Datei** auf **Speichern**.

Verknüpfen von unterstützten Schriftarten mit installierten Schriftarten

Sie können globale Schriftarten, die nicht auf dem Computer installiert sind, durch physische Schriftarten ersetzen.

Sie können Schriftarten auf allen Computern zuordnen, auf denen die Komponenten der Anwendungsebene installiert sind.

Sie haben beispielsweise der Liste unterstützter Schriftarten eine Schriftart hinzugefügt, die auf dem IBM Cognos-Computer nicht installiert ist. In diesem Fall geben Sie an, welche Schriftart als Ersatz verwendet werden soll.

Wenn Sie Berichte schneller mithilfe der integrierten PDF-Schriftarten drucken möchten, können Sie eine globale Schriftart wie Arial zu einer der integrierten PDF-Schriftarten zuweisen, z. B. Helvetica-PDF, indem Sie die nachfolgenden Schritte befolgen. Außerdem können Sie eine der integrierten PDF-Schriftarten für ein Textobjekt in Reporting oder Query Studio auswählen. Weitere Informationen finden Sie im *Query Studio - Benutzerhandbuch* bzw. im *Reporting - Benutzerhandbuch*.

Wenn Sie der Liste unterstützter Schriftarten eine Schriftart hinzufügen, die auf den IBM Cognos-Computern installiert ist, ist keine Zuordnung erforderlich. Sie müssen jedoch den Pfad der Schriftart angeben.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf allen Computern mit den Komponenten der Anwendungsebene.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Klicken Sie im Fenster **Eigenschaften** neben der Eigenschaft **Physische Schriftartenzuordnungen** in das Feld **Wert** und anschließend auf das Bearbeitungsymbol  .

   Das Dialogfeld **Wert - Physische Schriftartenzuordnungen** wird geöffnet.
4. Klicken Sie auf **Hinzufügen**.

   Tipp: Aktivieren Sie zum Entfernen einer Schriftart das Kontrollkästchen neben der entsprechenden Schriftart und klicken Sie auf **Entfernen**.
5. Geben Sie in das Feld **Globaler Schriftartenname** den Namen der Schriftart ein, die Sie der Liste unterstützter Schriftarten hinzugefügt haben.
6. Klicken Sie auf das Feld **Physischer Schriftartenname**.
7. Wenn Sie den Namen der physischen Schriftart kennen, können Sie diesen direkt eingeben. Andernfalls klicken Sie auf das Bearbeitungsymbol  .

   Klicken Sie im Dialogfeld **Physischer Schriftartenname** auf **Jetzt suchen** und wählen Sie anschließend einen Schriftartnamen aus den Ergebnissen aus.
8. Wiederholen Sie die Schritte 4 bis 7 für alle globalen Schriftarten, die verknüpft werden sollen.
9. Klicken Sie auf **OK**.
10. Klicken Sie im Menü **Datei** auf **Speichern**.

Ergebnisse

Geben Sie nun bei Bedarf den Installationspfad der Schriftarten an.

Verwenden von Systemschriftarten in IBM Cognos Configuration

Sie können IBM Cognos Configuration so konfigurieren, dass es unter Microsoft Windows-Betriebssystemen die Systemschriftarten verwendet.

Anmerkung: Wenn Sie die Einstellungen für die Verwendung der Systemschriftarten aktivieren, können Sie die Schriftarteinstellung innerhalb von IBM Cognos Configuration nicht ändern.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *Installationsposition*/configuration.
2. Öffnen Sie die Datei cogconfig.prefs in einem Texteditor.
3. Fügen Sie die folgende Zeile hinzu:

```
UseSystemDisplaySetting=true
```

4. Speichern Sie die Datei und schließen Sie sie.
5. Starten Sie IBM Cognos Configuration erneut.

Ändern der Standardschriftart für PDF-Berichte

Sie können die Standardschriftart ändern, die IBM Cognos Analytics-Komponenten für PDF-Berichte verwenden. Diese wird angezeigt, sobald Sie einen Bericht öffnen.

Die Standardschriftart wird auf dem Computer geändert, auf dem Content Manager installiert ist. Die Schriftart wird dann als Standardeinstellung auf allen Computern in der Installation übernommen. Sie können die in PDF-Berichten verwendete Schriftart mit IBM Cognos Configuration ändern.

Stellen Sie sicher, dass die Standardschriftart auf allen Computern in Ihrer IBM Cognos-Installation installiert ist.

Um sicherzustellen, dass GB18030-Zeichen in PDF-Berichten korrekt angezeigt werden, legen Sie als Standardschriftart SimSun-GB18030 fest.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf jedem Content Manager-Computer.
2. Klicken Sie im Menü **Aktionen** auf **Globale Konfiguration bearbeiten**.
3. Klicken Sie auf die Registerkarte **Allgemein**.
4. Geben Sie im Feld **Wert** unter **Standardschriftart** die Schriftart ein, die als Standardeinstellung für Berichte verwendet werden soll.
5. Klicken Sie auf **OK**.
6. Klicken Sie im Menü **Datei** auf **Speichern**.
7. Stellen Sie sicher, dass auf allen Computern mit Komponenten der Anwendungsebene unter **Umgebung** im Fenster **Explorer** für die Eigenschaft **Verzeichnis für physische Schriftarten** das Installationsverzeichnis der Standardschriftart angegeben ist oder dass sich die Schriftart im Windows-Schriftartenverzeichnis befindet.

Konfigurieren der in PDF-Berichten eingebetteten Schriftarten

Wenn ein PDF-Bericht in Adobe Reader geöffnet wird, müssen alle im Bericht verwendeten Schriftarten verfügbar sein. Die Schriftarten müssen entweder im Bericht eingebettet oder auf dem Computer des Benutzers installiert sein. Wenn eine Schriftart an keiner der beiden Positionen zur Verfügung steht, versucht Adobe Reader sie mit einer geeigneten Schriftart zu ersetzen. Durch das Ersetzen kann die Darstellung des Berichts geändert werden und einige Zeichen können eventuell nicht angezeigt werden.

Um sicherzustellen, dass PDF-Berichte in Adobe Reader ordnungsgemäß angezeigt werden, bettet IBM Cognos Analytics die erforderlichen Schriftarten standardmäßig in die Berichte ein. Statt alle Zeichen des Schriftartensatzes einzubetten, beschränkt sich IBM Cognos Analytics lediglich auf die im Bericht verwendeten Zeichen (auch Glyphen genannt) und minimiert so die Dateigröße. IBM Cognos Analytics bettet Schriftarten nur ein, wenn diese für das Einbetten lizenziert sind. Die Lizenzinformationen sind in der Schriftart selbst gespeichert und werden von IBM Cognos Analytics gelesen.

Wenn Sie sich sicher sind, dass die in den Berichten verwendeten Schriftarten auf dem Computer des Benutzers vorhanden sind, können Sie die Zahl der eingebetteten Schriftarten beschränken, um die Größe der PDF-Berichte zu reduzieren. Beim Beschränken der Schriftarten legen Sie mithilfe der Schriftarteneinbettungsliste in IBM Cognos Configuration fest, ob eine Schriftart immer oder niemals eingebettet werden soll.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Content Manager-Computer.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Klicken Sie im Fenster **Eigenschaften** unter **Schriftarteinstellungen** auf den Wert für **Schriftarten, die eingebettet werden sollen (Stapelberichtsservice)** oder **Schriftarten, die eingebettet werden sollen (Berichtsservice)** und klicken Sie dann auf das Bearbeitungssymbol  .
4. Wenn Sie nicht das Standardschriftartenverzeichnis verwenden oder einen Pfad zu einem zusätzlichen Verzeichnis hinzufügen möchten, geben Sie den neuen Pfad im Dialogfeld **Schriftarten, die in PDF-Berichte eingebettet werden sollen** in das Feld für die Schriftpfade ein.

   Tipp: Klicken Sie auf **Jetzt suchen**, um eine Liste der verfügbaren Schriftarten in allen angegebenen Pfaden abzurufen.
5. Wenn Sie sicher sind, dass eine Schriftart immer auf den Computern der Benutzer vorhanden ist, markieren Sie den Namen der Schriftart und aktivieren das Kontrollkästchen **Nie**.

   IBM Cognos Analytics bettet die Schriftart nicht in Berichte ein. Adobe Reader übernimmt die Schriftart beim Öffnen des Berichts vom Computer des Benutzers.
6. Wenn Sie nicht sicher sind, ob eine Schriftart immer auf den Computern der Benutzer vorhanden ist, markieren Sie den Namen der Schriftart und aktivieren das Kontrollkästchen **Immer**.

   IBM Cognos Analytics bettet die Schriftart bei allen Berichten ein, die diese Schriftart verwenden. Adobe Reader verwendet die eingebettete Schriftart, wenn der Bericht geöffnet wird.
7. Klicken Sie auf **OK**.

Gespeicherte Berichtsausgabe

Die Berichtsausgabedateien werden standardmäßig im Content Store gespeichert. Sie haben die Möglichkeit, eine Kopie der Berichtsausgabe an einer anderen Dateiposition innerhalb oder außerhalb von IBM Cognos Analytics zu speichern. Wenn Sie sich für diese Möglichkeit entscheiden, wird gleichzeitig eine zugehörige Deskriptordatei mit der Erweiterung "_descr" erstellt. Gespeicherte Dateien werden nicht von IBM Cognos Analytics verwaltet.

Speichern von Berichtsausgaben außerhalb von IBM Cognos Analytics

Wenn Sie eine Dateisystemadresse konfigurieren, die sich außerhalb von IBM Cognos Analytics befindet, können Sie die Berichtsausgabe für externe Anwendungen oder Benutzer freigeben, die keinen Zugriff auf IBM Cognos Analytics haben. Die meisten Berichtsausgabedateien werden auf diese Weise gespeichert.

Um diese Funktion verwenden zu können, müssen Sie zuerst ein Stammverzeichnis in IBM Cognos Configuration konfigurieren. Ein Administrator muss anschließend die Dateiadresse in IBM Cognos Administration festlegen. Weitere Informationen finden Sie im Abschnitt über das Festlegen einer Dateiadresse für außerhalb von IBM Cognos Analytics gespeicherte Berichtsausgaben im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Berichtsausgaben werden immer in das Verzeichnis geschrieben, das für die jeweilige Zustellungsserviceinstanz konfiguriert ist. Um zu vermeiden, dass Berichtsausgaben an mehrere Positionen geschrieben werden, stellen Sie entweder sicher, dass nur eine Instanz des Zustellungsservice ausgeführt wird, oder Sie konfigurieren alle Serviceinstanzen so, dass sie eine gemeinsame Netzdateiposition verwenden. Jeder Dispatcher, der den Zustellungsservice ausführt, muss Zugriff auf das Dateisystem haben oder er muss auf allen Systemen inaktiviert werden, die keine Berichtsausgaben speichern sollen.

Vorgehensweise

1. Erstellen Sie ein Verzeichnis für das Dateisystem.

   Tipp: Stellen Sie sicher, dass auf das Verzeichnis zugegriffen werden kann und es sich nicht im Installationsverzeichnis befindet. In einer verteilten Installation unter Microsoft Windows kann beispielsweise ein Archivordner wie *Servername**Verzeichnis* verwendet werden.
2. Starten Sie IBM Cognos Configuration auf dem Content Manager-Computer.
3. Klicken Sie im Menü **Aktionen** auf **Globale Konfiguration bearbeiten**.
4. Klicken Sie im Fenster **Globale Konfiguration** auf die Registerkarte **Allgemein**.
5. Geben Sie für **Root-Pfad des Dateisystems des Archivverzeichnisses** einen URI ein und halten Sie sich dabei an das folgende Format:

   `file://`*`Verzeichnis`*

   Dabei ist *Verzeichnis* das Verzeichnis, das Sie in Schritt 1 erstellt haben.

   Der Teil file:// des URI ist erforderlich. Es können Windows-UNC-Namen, wie *Servername**Verzeichnis*, verwendet werden. In diesem Fall muss der URI folgendes Format ausweisen:

   `file://\\`*`Servername`*`\`*`Verzeichnis`*

   Tipp: Stellen Sie sicher, dass Sie beim Ausführen von Cognos als Microsoft Windows-Service kein zugeordnetes Laufwerk verwenden.
6. Klicken Sie auf **Test**, um zu prüfen, ob die korrekte Position verwendet wird.
7. Klicken Sie auf **OK**.
8. Klicken Sie im Menü **Datei** auf **Speichern**.

Ergebnisse

Der Administrator muss jetzt die Dateispeicherposition konfigurieren. Entsprechende Informationen finden Sie im Abschnitt über das Festlegen einer Dateiadresse für außerhalb von IBM Cognos Analytics gespeicherte Berichtsausgaben im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Speichern von Berichtsausgaben innerhalb von IBM Cognos Analytics

Wenn Sie eine Dateisystemadresse innerhalb von IBM Cognos Analytics konfigurieren, können Sie die Berichtsausgabe anschließend wiederverwenden. Dies kann auch für Archivierungszwecke nützlich sein, da die im Content Store gespeicherten Dateien je nach den Speicherregeln möglicherweise regelmäßig gelöscht werden.

Um diese Funktion verwenden zu können, müssen Sie zuerst die Eigenschaft **Berichtsausgaben in einem Dateisystem speichern** in IBM Cognos Configuration einstellen. Ein Administrator muss anschließend die Dateiadresse mithilfe des Parameters CM.OutPutLocation in IBM Cognos Administration konfigurieren. Weitere Informationen finden Sie im Abschnitt über das Festlegen einer Dateiadresse für innerhalb von IBM Cognos Analytics gespeicherte Berichtsausgaben im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Berichtsausgaben werden immer in das Verzeichnis geschrieben, das für die jeweilige Zustellungsserviceinstanz konfiguriert ist. Um zu vermeiden, dass Berichtsausgaben an mehrere Positionen geschrieben werden, stellen Sie entweder sicher, dass nur eine Instanz des Zustellungsservice ausgeführt wird, oder Sie konfigurieren alle Serviceinstanzen so, dass sie eine gemeinsame Netzdateiposition verwenden. Jeder

Dispatcher, der den Zustellungsservice ausführt, muss Zugriff auf das Dateisystem haben oder er muss auf allen Systemen inaktiviert werden, die keine Berichtsausgaben speichern sollen.

Damit die Sicherheit der Berichtsausgabe bei Verwendung dieser Funktion bestehen bleibt, muss das Dateisystem über eine Drittanbieterverschlüsselung verfügen.

Vorgehensweise

1. Erstellen Sie ein Verzeichnis für das Dateisystem.

   Tipp: Stellen Sie sicher, dass nur berechtigte Benutzer auf das Verzeichnis zugreifen können.
2. Starten Sie IBM Cognos Configuration auf dem Content Manager-Computer.
3. Klicken Sie im Fenster **Explorer** auf **Datenzugriff** > **Content Manager**.
4. Legen Sie die Eigenschaft **Berichtsausgaben in einem Dateisystem speichern** auf **Wahr** fest.
5. Zum Testen der Verbindung mit dem Verzeichnis für die Berichtsausgabe klicken Sie im Menü **Aktionen** auf **Test**.
6. Klicken Sie im Menü **Datei** auf **Speichern**.

Ergebnisse

Der Administrator muss jetzt die Dateispeicherposition mithilfe des Parameters CM.OutPutLocation konfigurieren. Entsprechende Informationen finden Sie im Abschnitt über das Festlegen einer Dateiadresse für innerhalb von IBM Cognos Analytics gespeicherte Berichtsausgaben im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Ändern des Verzeichnisses für die temporäre Berichtsausgabe

Wenn Benutzer interaktive Berichte ausführen, wird die Berichtsausgabe in Content Manager oder in einem temporären Cache für die Benutzersitzung im lokalen Berichtsdateisystem gespeichert. Sie können das Verzeichnis des temporären Sitzungscache in ein Verzeichnis auf einem fernen Computer ändern, z. B. in ein freigegebenes Verzeichnis auf einem Microsoft Windows-basierten System oder einem Common-Mounted-Verzeichnis auf einem UNIX- oder Linux-basierten System.

Die Speicherposition des temporären Sitzungscaches im Berichtsdateisystem lautet standardmäßig `Installationsposition/temp/session`. Das Verzeichnis `session` wird vom Berichtsserver erstellt, wenn die erste Anforderung einer Benutzersitzung empfangen wird.

Prozedur

1. Starten Sie IBM Cognos Configuration auf den Computern, auf denen Komponenten auf Anwendungsebene installiert sind.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Klicken Sie im Fenster **Eigenschaften** auf den Wert für **Temporäre Dateien - Verzeichnis** und anschließend auf das Bearbeitungssymbol  .
4. Suchen Sie im Dialogfeld **Ordner auswählen** über das Feld **Speichern in** nach dem Computer und dem Verzeichnis und klicken Sie dann auf **Auswählen**.
5. Klicken Sie im Menü **Datei** auf **Speichern**.

   Wenn ein Benutzer eine interaktive Berichtssitzung ausführt, wird die temporäre Berichtsausgabe nun in dem neuen Verzeichnis gespeichert.

Sicherstellen, dass Dateiuploads nicht durch Dateiberechtigungen verhindert werden

Ab Cognos Analytics 11.1.x ist es bei Abfragen mit Datasets erforderlich, dass die Position der temporären Dateien kein UNIX-/Linux-Dateisystem verwendet, das mit der Option NOEXEC angehängt wurde.

Wenn das Dateisystem mit der Option NOEXEC angehängt wurde, verhindert dies die Erstellung und die nachfolgende Abfrage von hochgeladenen Dateien/Datasets.

Position der traditionellen Map Manager-Landkarten für Reporting ändern

IBM Cognos Analytics enthält eine Reihe vordefinierter Landkartendiagramme, die Sie in Reporting verwenden können. Mithilfe von IBM Cognos Configuration können Sie die Speicherposition der Landkartendiagramme ändern.

Anmerkung: Diese Informationen gelten nur für die traditionellen Map Manager-Landkarten, die Sie in Berichten verwenden können.

Landkartendiagramme werden standardmäßig im Verzeichnis `installationsposition/maps` auf dem Computer mit den Komponenten der Anwendungsebene gespeichert.

Weitere Informationen zur Verwendung von Landkartendiagrammen finden Sie im Reporting *Benutzerhandbuch*.

Weitere Informationen zur Verwendung von benutzerdefinierten Landkarten aus anderen Quellen finden Sie im Map Manager *Installation and User Guide*.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Computer mit den Komponenten der Anwendungsebene.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Klicken Sie im Fenster **Eigenschaften** auf den Wert für **Zuordnungsdateiposition**.
4. Klicken Sie auf das Bearbeitungssymbol  .
5. Navigieren Sie im Fenster **Ordner auswählen** zum gewünschten Verzeichnis und klicken Sie dann auf **Auswählen**.
6. Klicken Sie im Menü **Datei** auf **Speichern**.

Ändern der Position von Datendateien

Sie können die Position des Ordners `data` ändern, der von Cognos Analytics-Komponenten erstellte Datendateien enthält.

Die Standardposition für diesen Ordner ist *`installation_location`*`/data`

Wichtig: Der Ordner `data` muss sich lokal auf dem aktiven Content Manager-Computer sowie auf jedem Standby-Content Manager-Computer befinden.

Wenn Sie angeben, dass sich die Datendateien auf einem gemeinsam genutzten Netzlaufwerk befinden, versuchen die aktiven Content Manager-Computer und die Standby-Content Manager-Computer, auf dieselben Suchindexdateien im Ordner `data/search` zuzugreifen. Dies führt dazu, dass Benutzern die folgende Nachricht angezeigt wird:

```
Unable to retrieve activities at this time. (Abrufen von Aktivitäten derzeit
nicht möglich.) ADM-ERR-001
```

Darüber hinaus werden Fehlernachrichten protokolliert und es können Beschädigungen des Index auftreten. Es folgt ein Beispiel für eine protokollierte Fehlernachricht, die durch die Konfiguration des Ordners `data` auf einer gemeinsam genutzten Platte bedingt ist:

```
org.apache.lucene.store.AlreadyClosedException: Already clo-
sed: MMapIndexInput(path="\\myshare\cognos11\data\search\collections\cm\da-
ta\index\_c0d_Lucene50_0.tim") at org.apache.lucene.store.ByteBufferIndexIn-
put.readBytes(ByteBufferIndexInput.java:106) ~[lucene-core-8.2.0.jar:8.2.0
31d7ec7bbfdcd2c4cc61d9d35e962165410b65fe - ivera - 2021-04-19 15:05:56]
```

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Computer mit den Komponenten der Anwendungsebene.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Klicken Sie im Fenster **Eigenschaften** auf den Wert für **Datendateien-Verzeichnis**.
4. Klicken Sie auf das Bearbeitungssymbol  .
5. Navigieren Sie im Fenster **Ordner auswählen** zum gewünschten Verzeichnis und klicken Sie dann auf **Auswählen**.
6. Klicken Sie im Menü **Datei** auf **Speichern**.

Optimieren von WebSphere Liberty Profile

In Produktionsumgebungen können Sie WebSphere Liberty Profile für die maximal zu erwartende Anzahl gleichzeitiger Benutzer optimieren, indem Sie die Werte für **coreThreads** und **maxThreads** in den erweiterten Eigenschaften der Ressourcen anpassen. Mit diesen Werten werden die Kernanzahl und die maximale Anzahl von Steuerprogrammthreads festgelegt.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Klicken Sie im Fenster **Explorer** unter **Umgebung** und **IBM Cognos-Services** auf den Ressourcennamen (der Standardwert lautet **IBM Cognos**).
3. Klicken Sie im Fenster **Eigenschaften** neben **Erweiterte Eigenschaften** in das Feld **Wert** und anschließend auf das Bearbeitungssymbol  .
4. Passen Sie die Parameterwerte nach Bedarf an.

Tabelle 22. Namen und Werte der Serviceressourcenparameter

Parametername	Wert
coreThreads	Die Kernanzahl der Threads, mit denen der WebSphere Liberty Profile-Server gestartet wird. Wenn dieser Wert kleiner 0 ist, wird ein Standardwert verwendet. Dieser Standardwert wird auf der Basis der Anzahl der Hardware-Threads im System berechnet.
maxThreads	Die maximale Anzahl der Threads, die dem WebSphere Liberty Profile-Server zugeordnet werden können.

   Weitere Informationen finden Sie im Knowledge Center für WebSphere Liberty Profile im Abschnitt zum Optimieren des Liberty-Profils (https://www.ibm.com/support/knowledgecenter/en/SSEQTP_liberty/com.ibm.websphere.wlp.doc/ae/twlp_tun.html).
5. Klicken Sie im Menü **Datei** auf **Speichern**.

Aktivieren der Sitzungsreplikation für Content Manager-Bereitschaftsservices

Die Sitzungsreplikationsfunktion ermöglicht eine nahtlose Funktionsübernahme für IBM Cognos Content Manager zwischen einem aktiven Content Manager-Service und einem Content Manager-Bereitschaftsservice.

Wenn die Sitzungsreplikation aktiviert ist, werden Benutzersitzungsdaten zwischen allen Content Manager-Instanzen repliziert. Schlägt der aktive Content Manager fehl, bleiben die Benutzersitzungsdaten erhalten und die Benutzer können die Anwendung ohne Unterbrechung weiterverwenden.

Die Sitzungsreplikation verwendet zwei Ports für die sichere Kommunikation mit den verschiedenen IBM Cognos Content Managers, die innerhalb einer einzelnen Umgebung konfiguriert sind.

Vorgehensweise

1. Starten Sie auf einem Computer, auf dem der IBM Cognos Content Manager installiert ist, IBM Cognos Configuration.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** auf **Replikation**.
3. Geben Sie die folgenden Eigenschaften an:
   a) Legen Sie für die Eigenschaft **Replikation aktivieren** den Wert **Wahr** fest.
   b) Geben Sie im Feld für den Wert **Listener-Portnummer für Peers** eine Portnummer ein.

      Mit dem Wert 0 wird beim Starten des IBM Cognos-Service der erste verfügbare dynamische Port ausgewählt.
   c) Geben Sie im Feld für den Wert **RMI-Replikationportnummer** eine Portnummer ein.

   Anmerkung: Erweiterte Eigenschaften sollten nur unter Anleitung eines Mitarbeiters von IBM #Technical Support verwendet werden.
4. Speichern Sie die Konfiguration und starten Sie den IBM Cognos-Service erneut.
5. Wiederholen Sie die Schritte für jede Content Manager-Instanz in der Umgebung.

   Die Portnummern, die Sie angeben, müssen nicht für jede Content Manager-Instanz identisch sein.

Verwenden eines externen Objektspeichers für Berichtsausgabe und Datasets

Sie können Content Manager so konfigurieren, dass die Berichtsausgabe und die Datasets auf einem lokalen Laufwerk oder in einem gemeinsam genutzten Netzbereich gespeichert werden, indem Sie einen externen Objektspeicher definieren. Die Berichtsausgabe steht in diesem Fall über das Portal und IBM Cognos SDK zur Verfügung, wird aber nicht in der Content Store-Datenbank gespeichert.

Mittels eines externen Objektspeichers für Berichtsausgaben lässt sich die Größe des Content Store reduzieren und die Leistung von Content Manager verbessern.

Vorbereitende Schritte

Führen Sie vor der Erstellung der Verbindung zu einem externen Objektspeicher folgende Aufgaben durch:

- Stellen Sie auf den Content Manager-Computern Zugriff auf die Dateiposition des externen Objektspeichers bereit.
- Erteilen Sie dem Benutzerkonto, unter dem der IBM Cognos-Service ausgeführt wird, Lese- und Schreibzugriff auf die Dateiposition.
- Erstellen Sie den Content Store.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Klicken Sie im Fenster **Explorer** unter **Datenzugriff** > **Content Manager** mit der rechten Maustaste auf den Namen Ihres **Content Store** und wählen Sie **Neue Ressource** > **Externer Objektspeicher** aus.
3. Geben Sie im Fenster **Neue Ressource - Externer Objektspeicher** einen eindeutigen Namen für dieses Dateisystemrepository ein und klicken Sie auf **OK**.

   Sie dürfen nur einen externen Objektspeicher einrichten.

4. Klicken Sie auf den Namen des Repository.
5. Klicken Sie im Fenster **Externer Objektspeicher - Ressourceneigenschaften** in das Wertfeld und geben Sie im daraufhin geöffneten Fenster **URI-Werte** den Pfad zur Dateisystemposition des externen Objektspeichers ein, wobei "file-system-path" der vollständige Pfad zu einer vorhandenen Dateiposition sein muss.

Tabelle 23. Beispiele für URI-Werte	
Dateisystem	**URI-Wert**
Windows	`file:///c:/file-system-path` `file://host/share/file-system-path`
UNIX oder Linux	`file:///file-system-path`

Anmerkung: Relative Pfade wie `file:///../file-system-path` und Laufwerkzuordnungen werden nicht unterstützt.

Bei einer verteilten Installation müssen alle Content Manager Lese- und Schreibzugriff auf die Dateisystemposition haben. Zur Verbesserung der Leistung beim Lesen der Ausgaben sollten die Komponenten der Anwendungsebene, insbesondere der Repository-Service, ebenfalls Lesezugriff auf die Dateisystemposition haben. Andernfalls werden Anforderungen an den aktiven Content Manager weitergeleitet.

6. Starten Sie den IBM Cognos-Service neu.

Überprüfen des Zugriffs auf den externen Objektspeicher

Überprüfen Sie mithilfe von IBM Cognos Configuration, ob IBM Cognos-Komponenten eine Verbindung zum externen Objektspeicher herstellen können.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Klicken Sie unter **Explorer** > **Datenzugriff** mit der rechten Maustaste auf den Namen der Verbindung zu Ihrem externen Objektspeicher.
3. Klicken Sie auf **Testen**.

   IBM Cognos Configuration überprüft den Zugriff auf die Dateiposition des externen Objektspeichers.

   Alternativ können Sie diese Verbindung auch testen, indem Sie mit der rechten Maustaste auf **Lokale Konfiguration** klicken und **Testen** auswählen.

Anpassen des serverseitigen Drucks unter UNIX und Linux

Die Funktionsweise des serverseitigen Drucks des IBM Cognos Analytics-Portals unterscheidet sich je nach Plattform.

Aus diesem Grund können Sie unter UNIX und Linux die Art und Weise, wie das Portal den Berichtsdruck im PDF-Format ausführt, in der Datei *rsprintpdf.sh* anpassen.

Bei Microsoft Windows-Druckservern sollte die Datei *rsprintpdf.sh* nicht konfiguriert werden.

Bei der Ausgabe auf einen UNIX- oder Linux-Druckserver können Probleme auftreten, wenn der Benutzer **Mit Optionen ausführen** auswählt, das **Format** auf PDF setzt, im Abschnitt **Zustellung** die Option **Den Bericht drucken** wählt und dann über **Erweiterte Optionen** weitere Formate wie Querformat, DIN A4-Format oder **Zeit und Modus** zur Ausführung des Berichts auswählt. In diesem Fall kann es passieren, dass die Ausgabe entweder gar nicht generiert wird oder abgeschnitten bzw. falsch ausgerichtet wird.

Vorgehensweise

1. Öffnen Sie die Datei *rsprintpdf.sh* m Verzeichnis *Installationsposition/bin*.
2. Passen Sie den Abschnitt der Datei, der auf die Plattform Ihres Druckservers zutrifft (z. B. AIX oder Linux), in einem Texteditor an.
3. Geben Sie bei der Anpassung die folgenden, auf Ihre Umgebung zutreffenden Informationen ein. Die Informationen werden vom Serverprozess als Befehlszeilenoptionen an das Script *rsprintpdf.sh* übergeben.

Tabelle 24. Anpassungsoptionen für das Drucken von Berichten im PDF-Format

Option	Name	Beschreibung
-p	printer	Gibt die Druckwarteschlange an. Ist diese nicht angegeben, so wird die Standardwarteschlange verwendet.
-o	orientation	Gibt die Seitenausrichtung einer Datei an: Quer- oder Hochformat. Ist diese nicht angegeben, so wird Hochformat verwendet.
-m	media	Gibt das Papierformat der Ausgabe an, zum Beispiel Letter oder A4. Wenn weder Papierformat, noch Höhe oder Breite angegeben sind, wird das Standardpapierfach verwendet.
-h	height	Für benutzerdefinierte Papierformate. Gibt die Höhe der Seite in Punkten an. Dieser Parameter ist nur gültig, wenn auch -w, aber nicht -m angegeben ist.
-w	width	Für benutzerdefinierte Papierformate. Gibt die Breite der Seite in Punkten an. Dieser Parameter ist nur gültig, wenn auch -h, aber nicht -m angegeben ist.
-L	Protokolldatei	Gibt den Pfad zu einer benutzerdefinierten Datei für die Aufzeichnung von Fehlernachrichten an. Der Standardname der Protokolldatei lautet *rsprintpdf.errors.log*.

4. **Tipp**: Erstellen Sie eine Sicherungskopie der bearbeiteten Datei *rsprintpdf.sh* für den Fall, dass diese Datei bei einem späteren Software-Upgrade überschrieben wird.

Ändern der Benachrichtigungsdatenbank

Der Benachrichtigungsserver verwendet standardmäßig dieselbe Datenbank, die Content Manager für den Content Store verwendet. Sie können separate Datenbanken für die Benachrichtigung verwenden, wenn Sie große Mengen an Stapelberichten und -E-Mails ausführen müssen.

Die Verwendung einer separaten Benachrichtigungsdatenbank umfasst die folgenden Schritte:

- Erstellen einer Benachrichtigungsdatenbank.

  Verwenden Sie für IBM Db2, Oracle oder Microsoft SQL Server dieselbe Vorgehensweise wie bei der Erstellung der Content-Store-Datenbank. Gehen Sie anhand der Anweisungen unter „Richtlinien zum Erstellen des Content Store” auf Seite 7 vor.

  Anmerkung: Wenn Sie Db2 verwenden, können Sie kein Script generieren, um die Benachrichtigungsdatenbank auf dieselbe Weise zu generieren wie den Content Store.

  Befolgen Sie für Db2 unter z/OS die Anweisungen im Abschnitt „Empfohlene Einstellungen für die Erstellung einer Benachrichtigungsdatenbank in IBM Db2 unter z/OS ” auf Seite 200.
- Einrichten der Datenbankkonnektivität.

  Sie können dieselbe Vorgehensweise wie beim Einrichten der Verbindung für die Content Store-Datenbank verwenden („Einrichten der Datenbankverbindung für die Content Store-Datenbank” auf Seite 96).
- Ändern der Verbindungseigenschaften für die Benachrichtigungsdatenbank.

Gehen Sie anhand der Anweisungen unter „Ändern der Verbindungseigenschaften für die Benachrichtigungsdatenbank” auf Seite 201 vor.

Empfohlene Einstellungen für die Erstellung einer Benachrichtigungsdatenbank in IBM Db2 unter z/OS

Die Datenbank, die Sie als Benachrichtigungsdatenbank erstellen, muss die angegebenen Konfigurationseinstellungen enthalten.

Um eine erfolgreiche Installation sicherzustellen, gehen Sie bei Erstellung der Benachrichtigungsdatenbank anhand der folgenden Richtlinien vor.

Verwenden Sie die folgende Prüfliste, um die Benachrichtigungsdatenbank in Db2 unter z/OS einzurichten.

__ • Erstellen Sie für die Benachrichtigungsdatenbank eine Datenbankinstanz, eine Speichergruppe und ein Benutzerkonto.

  Ein Benutzer muss über Berechtigungen zum Erstellen und Löschen von Tabellen in der Datenbank verfügen.

  IBM Cognos Analytics verwendet die Berechtigungsnachweise des Benutzerkontos, um mit dem Datenbankserver zu kommunizieren.

__ • Stellen Sie sicher, dass Sie einen Pufferpool mit einer Seitengröße von 32 KB und einen zweiten Pufferpool mit einer Seitengröße von 4 KB für die Datenbankinstanz reservieren.

__ • Administratoren müssen ein Script ausführen, das Tabellenbereiche zur Aufnahme von großen Objekten und anderen Daten erstellt und festlegt, dass die Benachrichtigungsdatenbank die Tabellenbereiche verwenden soll.

  Weitere Informationen zur Ausführung des Scripts finden Sie in „Erstellen von Tabellenbereichen für eine Benachrichtigungsdatenbank für IBM Db2 für z/OS ” auf Seite 200.

__ • Ihr Datenbankadministrator muss die IBM Cognos Analytics-Datenbanken in regelmäßigen Abständen sichern, da diese die IBM Cognos-Daten enthalten.

  Um die Sicherheit und die Integrität der Datenbanken zu gewährleisten, müssen diese vor nicht autorisierten und unerwünschten Zugriffen geschützt werden.

Erstellen von Tabellenbereichen für eine Benachrichtigungsdatenbank für IBM Db2 für z/OS

Wenn Sie Db2 for z/OS verwenden, muss ein Datenbankadministrator Scripts ausführen, um die Tabellenbereiche zu erstellen, die für die Benachrichtigungsdatenbank erforderlich sind. Diese Scripts müssen angepasst werden, d. h. die Platzhalterparameter sind durch solche zu ersetzen, die für Ihre Umgebung geeignet sind.

Stellen Sie sicher, dass Sie die Namenskonventionen für Db2 for z/OS verwenden. Beispielsweise müssen alle Parameternamen mit einem Buchstaben anfangen und dürfen maximal 6 Zeichen lang sein. Weitere Informationen finden Sie im Db2 Knowledge Center.

Vorgehensweise

1. Stellen Sie als Benutzer mit Berechtigungen zum Erstellen und Löschen von Tabellenbereichen sowie zum Ausführen von SQL-Anweisungen eine Verbindung mit der Datenbank her.
2. Wechseln Sie zur Erstellung der Tabellenbereiche mit den Benachrichtigungen in das Verzeichnis *Installationsposition*/configuration/schemas/delivery/zosdb2.
   a) Erstellen Sie eine Sicherungskopie der Scriptdatei NC_TABLESPACES.sql und speichern Sie die Datei an einer anderen Position.
   b) Öffnen Sie die ursprüngliche Scriptdatei NC_TABLESPACES.sql und ersetzen Sie die Platzhalterparameter mithilfe der folgenden Tabelle durch die für Ihre Umgebung geeigneten Parameter.

Tabelle 25. Parameternamen und Beschreibungen für Tabellenbereiche für die Db2-Benachrichtigungsdatenbank unter z/OS

Parametername	Beschreibung
NCCOG	Gibt den Namen der Benachrichtigungsdatenbank an.
DSN8G810	Gibt den Namen der Speichergruppe an.
BP32K	Gibt den Namen des Pufferpools an.

Die Tabelle beschreibt auch Parameter, die noch nicht im Script enthalten sind, möglicherweise aber in Zukunft hinzugefügt werden.

c) Speichern Sie das Script und führen Sie es aus.

Beispiel:

```
db2 -tvf NC_TABLESPACES.sql
```

d) Öffnen Sie die Scriptdatei `NC_CREATE_DB2.sql` und ersetzen Sie den Platzhalterparameter NCCOG durch den Namen der Benachrichtigungsdatenbank.

e) Speichern Sie das Script.

Das Script wird von den Services für die Job- und Zeitplanüberwachung automatisch ausgeführt. Sie können es jedoch auch selbst ausführen.

Ändern der Verbindungseigenschaften für die Benachrichtigungsdatenbank

Nachdem Sie eine separate Benachrichtigungsdatenbank erstellt haben, müssen Sie IBM Cognos-Komponenten für die Verwendung der neuen Datenbank konfigurieren.

Sie müssen alle Content Manager und Komponenten der Anwendungsebene für die Verwendung derselben Benachrichtigungsdatenbank konfigurieren.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration an jeder Position, an der Content Manager oder Komponenten der Anwendungsebene installiert sind.
2. Klicken Sie im Fenster **Explorer** unter **Datenzugriff** auf **Benachrichtigung**.
3. Identifizieren Sie die Datenbank, die für Benachrichtigungen verwendet wird:
   - Klicken Sie im Fenster **Explorer** mit der rechten Maustaste auf **Benachrichtigung** und wählen Sie **Neue Ressource** > **Datenbank**.
   - Geben Sie einen Namen für die Datenbankressource ein.
   - Wählen Sie den Datenbanktyp aus dem Dropdown-Menü aus.
   - Klicken Sie auf **OK**.
4. Geben Sie im Fenster **Eigenschaften** die Werte für die Datenbankressource für Benachrichtigungen ein.
5. Klicken Sie im Menü **Datei** auf **Speichern**.
6. Testen Sie die Benachrichtigung. Klicken Sie im Fenster **Explorer** mit der rechten Maustaste auf **Benachrichtigung** und klicken Sie auf **Test**.

   Dadurch werden die Datenbankverbindung und die E-Mail-Server-Verbindung getestet.

   Wenn Sie die Content Store-Datenbank für die Benachrichtigung verwenden, werden die Zeitpläne in die Tabellen der neuen Benachrichtigungsdatenbank repliziert.

Ergebnisse

Stellen Sie sicher, dass die zur Identifizierung der Benachrichtigungsdatenbankressource verwendeten Werte auf allen Content Manager-Computern und Computern mit Komponenten der Anwendungsebene übereinstimmen. Wenn Sie die Standard-Datenbank für Benachrichtigungen verwenden möchten, müssen Sie die Werte im Fenster **Eigenschaften** nicht anpassen.

Zertifikatsmanagement in Cognos Analytics

IBM Cognos Analytics richtet mithilfe von Zertifikaten eine Basis für die Vertrauenswürdigkeit (Root of Trust, RoT) zwischen den verschiedenen zugehörigen Komponenten ein. Es werden die Zertifikate einer internen Zertifizierungsstelle (Standardeinstellung) oder einer externen Zertifizierungsstelle (Certificate Authority, CA) unterstützt.

Die Verwaltung der Zertifikate erfolgt mithilfe des Befehlszeilentools ThirdPartyCertificateTool.

ThirdPartyCertificateTool – Befehle und Verwendungsbeispiele

Das **ThirdPartyCertificateTool** wird verwendet, um eine Zertifikatssignieranforderung (CSR) zu erstellen, ein Zertifikat oder einen privaten Schlüssel zu importieren und ein Zertifikat zu exportieren.

Dieses Tool kann sowohl mit der internen Zertifizierungsstelle (Standardeinstellung) als auch mit der externen Zertifizierungsstelle (Certificate Authority, CA) verwendet werden.

Das Tool befindet sich im Verzeichnis Cognos Analytics *installationsposition*`/bin`.

Die Abschnitte in diesem Thema liefern Beschreibungen von Befehlen sowie Verwendungsbeispiele für **ThirdPartyCertificateTool**.

Tipp: Dieselben Informationen können unter Angabe des Parameters `-help` in Verbindung mit dem Tool abgerufen werden. Beispiel: `ThirdPartyCertificateTool.bat -help`

ThirdPartyCertificateTool - Befehle

Verwenden Sie die folgenden Befehle, um den Hauptoperationsmodus für das Tool anzugeben.

`-c`
Erstellt eine Zertifikatssignieranforderung (CSR).

`-i`
Importiert ein Zertifikat oder einen privaten Schlüssel.

`-E`
Exportiert ein Zertifikat.

Anmerkung: Wenn die integrierte Cognos-Zertifizierungsstelle (Certificate Authority, CA) verwendet wird, exportiert der Exportbefehl das Zertifikat, das von der lokalen Zertifizierungsinstanz ausgegeben wurde. Möglicherweise handelt es sich dabei nicht um das neueste CA-Zertifikat, falls es über Fernzugriff regeneriert wurde und die beiden lokalen Zertifikate noch gültig sind.

Verwenden Sie die folgenden Befehle, um die Operationsmodifikatoren anzugeben:

`-T`
Mit dem Truststore arbeiten. Verwenden Sie diesen Modifikator nur in Verbindung mit den Befehlen **`-i`** und **`-E`**.

`-e`
Mit Kryptoidentität arbeiten.

Verwenden Sie die folgenden Befehle, um die Informationsflags anzugeben:

`-p`
Keystore-Kennwort. Wenn dieser Befehl nicht vorhanden ist, wird das Standardkennwort verwendet.

`-a`
Schlüsselpaaralgorithmus: entweder **RSA** (Standardeinstellung) oder **ECC**.

-r
CSR- oder Zertifikatsdateiposition (abhängig vom Operationsmodus).

-t
CA-Kettendatei. Dabei kann es sich um PEM, eine binäre PKCS#7 CA-Zertifikatskette oder ein einzelnes CA-Zertifikat im DER-Format handeln.

-d
Der DN (Distinguished Name) des Zertifikats, beispielsweise `CN=produktname, OU= organisationseinheit, O=unternehmen, C=land`.

-w
Das Kennwort für Quelle des privaten Schlüssels (PKCS#8, PKCS#12).

-H
DNS-Namen für SAN (Subject Alternative Name), beispielsweise `DNS_host_1 [DNS_host_n]`.

-I
IP-Adressen (IPv4, IPv6) für SAN (Subject Alternative Name), beispielsweise `IP_address_1 [IP_address_n]`.

-j
Kennwort des Keystores für JRE-Zertifikate. Wenn dieser Befehl nicht enthalten ist, wird das Standardkennwort des Keystores für die JRE-Zertifikate verwendet.

-k
Dateispeicherposition des privaten PKCS#8-Schlüssels.

-K
Dateispeicherposition des privaten PKCS#12-Schlüssels und der Datei der CA-Kette.

-M
E-Mail-Adressen für SAN (Subject Alternative Name), beispielsweise `email_1 [email_n]`.

Verwendungsbeispiele mit ThirdPartyCertificateTool

Dieser Abschnitt enthält Beispiele für Befehle, die Sie mit **ThirdPartyCertificateTool** ausführen können.

Anmerkung: Die Beispiele enthalten den Platzhalter *keystore-kennwort*. Dieses Kennwort muss mit dem **Keystore-Kennwort** übereinstimmen, das in IBM Cognos Configuration unter **Sicherheit** > **Verschlüsselung** > **Cognos** festgelegt ist. Das Standardkennwort für den Keystore lautet `NoPassWordSet`. Falls Sie das Keystore-Standardkennwort geändert haben, müssen Sie das von Ihnen angegebene Kennwort verwenden.

In der folgenden Liste werden die Aufgaben angegeben, die Sie mit **ThirdPartyCertificateTool**in Verbindung mit der zugehörigen Befehlssyntax ausführen können:

- Zertifikatssignieranforderung (CSR) generieren.

```
ThirdPartyCertificateTool.(bat|sh) -c -e
[-p keystore-kennwort] -a schlüsselpaaralgorithmus
-r pfad_zu_zertifikat_oder_csr
-d dn
[-H dns_namen_für_san]
[-I ip-adressen_für_san]
[-M e-mail-adressen_für_san]
```

- Zielverschlüsselungszertifikat importieren.

```
ThirdPartyCertificateTool.(bat|sh) -i -e [-p keystore-kennwort]
-r pfad_zu_zertifikat_oder_csr -t pfad_zu_zertifikatskette
```

- Vertrauenswürdiges Zertifikat importieren.

```
ThirdPartyCertificateTool.(bat|sh) -i -T [-p keystore-kennwort]
-r pfad_zu_zertifikat_oder_csr
```

- Verschlüsselungsschlüssel mithilfe separater Einträge importieren.

```
ThirdPartyCertificateTool.(bat|sh) -i -e [-p keystore-kennwort]
-a schlüsselpaaralgorithmus -r pfad_zu_zertifikat_oder_csr
-t pfad_zu_zertifikatskette
-w kennwort_für_quelle_des_privaten_schlüssels -k pfad_zu_PKCS#8
```

- Verschlüsselungsschlüssel von PKCS#12 importieren.

```
ThirdPartyCertificateTool.(bat|sh) -i -e [-p keystore-kennwort]
-a schlüsselpaaralgorithmus -w kennwort_für_quelle_des_privaten_schlüssels
-K pfad_zu_PKCS#12
```

- CA-Zertifikat exportieren.

```
ThirdPartyCertificateTool.(bat|sh) -E -T [-p keystore-kennwort]
-r pfad_zu_zertifikat_oder_csr
```

Anmerkung: Wenn die integrierte Cognos-Zertifizierungsstelle (Certificate Authority, CA) verwendet wird, bewirkt die Angabe des Exportbefehls -E das Exportieren des Zertifikats, das von der lokalen Zertifizierungsinstanz ausgegeben wurde. Möglicherweise handelt es sich dabei nicht um das neueste CA-Zertifikat, falls es über Fernzugriff regeneriert wurde und die beiden lokalen Zertifikate noch gültig sind.

- Verschlüsselungszertifikat exportieren.

```
ThirdPartyCertificateTool.(bat|sh) -E -e [-p keystore-kennwort]
-r pfad_zu_zertifikat_oder_csr
```

Konfigurieren von Cognos Analytics-Komponenten für die Verwendung einer anderen Zertifizierungsstelle

Sie können IBM Cognos Analytics so konfigurieren, dass ein Zertifikat einer externen Zertifizierungsstelle (Certificate Authority, CA) zum Einrichten einer Vertrauenswürdigkeitsbasis (Root of Trust, RoT) in der Sicherheitsinfrastruktur verwendet wird.

Standardmäßig verwenden die Komponenten von IBM Cognos Analytics zu diesem Zweck ihre eigene Zertifizierungsstelle.

Gehen Sie wie im Folgenden beschrieben vor, um Cognos Analytics für die Verwendung einer anderen Zertifizierungsstelle (Certificate Authority, CA) zu konfigurieren:

1. „Löschen des vorhandenen Keystores” auf Seite 204
2. „Erstellen der Dateien für Zertifikatssignieranforderungen (CSR-Dateien)” auf Seite 205
3. „Importieren der Zertifikate der Zertifizierungsstelle (CA)” auf Seite 206
4. „Aktivieren der externen Zertifizierungsstelle (CA)” auf Seite 207

Eine Änderung der Zertifizierungsstelle wirkt sich auf andere installierte Komponenten von Cognos Analytics aus, z. B. auf Framework Manager und Planning Analytics. Die Vorgehensweise für die Konfiguration einer externen Zertifizierungsstelle für diese Komponenten entspricht der Vorgehensweise bei Cognos Analytics.

Wichtig: Die an dieser Stelle beschriebene Vorgehensweise für die Konfiguration einer externen Zertifizierungsstelle ist nicht für IBM Cognos PowerPlay geeignet. Bei diesem Produkt müssen Sie den für Version 10.2.2 des IBM Cognos Business Intelligence-Produkts beschriebenen Prozess anwenden. Weitere Informationen enthält das Installations- und Konfigurationshandbuch für *IBM Cognos Business Intelligence PowerPlay*, Version 10.2.2.

Löschen des vorhandenen Keystores

Wenn Sie IBM Cognos Analytics zur Verwendung einer externen Zertifizierungsstelle (CA) konfigurieren, müssen Sie mit einem heruntergefahrenen System und einem leeren Schlüsselspeicher beginnen.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration als Administrator.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** > **Verschlüsselung** auf **Cognos**.
3. Klicken Sie unter **Einstellungen für Zertifizierungsstelle** auf die Eigenschaft **Zertifizierungsstelle eines anderen Anbieters verwenden** und stellen Sie sicher, dass für **Wert** die Angabe **Falsch** festgelegt ist.
4. Klicken Sie im Menü **Datei** auf **Speichern**, um die Konfiguration zu speichern.
5. Schließen Sie Cognos Configuration.
6. Wechseln Sie in das Installationsverzeichnis von Cognos Analytics und löschen Sie den gesamten Inhalt aus dem Verzeichnis *install_location*\configuration\certs.

Erstellen der Dateien für Zertifikatssignieranforderungen (CSR-Dateien)

Um ein Zertifikat von einer Zertifizierungsstelle zu erhalten, müssen Sie zunächst Dateien für Zertifikatssignieranforderungen (CSR-Dateien) für den Verschlüsselungsschlüssel aus dem Cognos Analytics-Keystore erstellen. Mithilfe einer solchen Datei generiert die Zertifizierungsstelle ein Verschlüsselungszertifikat und ein Zertifikat einer Zertifizierungsstelle, die Sie dann in Ihren Keystore importieren.

Vorbereitende Schritte

Unter UNIX und Linux müssen Sie vor Verwendung von **ThirdPartyCertificateTool** sicherstellen, dass die Umgebungsvariable JAVA_HOME gesetzt ist.

Bei Installationen unter Microsoft Windows können Sie das Tool wie im nachfolgenden Beispiel veranschaulicht mit dem Befehl `-java:local` ausführen, damit die mit der Installation bereitgestellte JRE verwendet wird: `ThirdPartyCertificateTool.bat -java:local -c -d ...`

Informationen zu diesem Vorgang

Wenn Sie das **Keystore-Kennwort** in IBM Cognos Configuration geändert haben (unter **Verschlüsselung** > **Cognos**), verwenden Sie für *keystore_password* beim Ausführen der nachfolgenden **ThirdPartyCertificateTool**-Befehle das neue Kennwort. Das Standardkennwort lautet **`NoPassWordSet`**.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *installationsposition*\bin und führen Sie das Tool **ThirdPartyCertificateTool** aus.
2. Geben Sie den folgenden Befehl ein, um die Zertifikatssignieranforderung (Certificate Signing Request, CSR) für den Verschlüsselungsschlüssel zu erstellen:
   - Geben Sie unter UNIX oder Linux Folgendes ein:

     ```
     ThirdPartyCertificateTool.sh -c -e -d "CN=EncryptCert,O=MyCompany,C=CA"
     -r encryptRequest.csr -p keystore_password -a RSA
     ```

   - Geben Sie unter Windows Folgendes ein:

     ```
     ThirdPartyCertificateTool.bat -c -e -d "CN=EncryptCert,O=MyCompany,C=CA"
     -r encryptRequest.csr -p keystore_password -a RSA
     ```

   Der Wert für den definierten Namen (Distinguished Name, DN) im Befehl (`"CN=EncryptCert,O=MeineFirma, C = CA"`) stellt eine eindeutige Kennzeichnung für die Cognos Analytics-Installation dar. Die in diesem Parameter verwendeten Attribute spiegeln eine hierarchische Struktur in Ihrem Unternehmen wider.

   Das Kennwort, das Sie für diesen Schlüssel eingeben, muss auch beim Importieren des Zertifikats und ebenfalls in IBM Cognos Configuration verwendet werden.
3. Führen Sie den Befehl aus.

Sie können alle Warnungen in Bezug auf die Protokollierung ignorieren.

Wichtig: Diese Zertifikate müssen von der Zertifizierungsstelle im PEM-Format (ASCII Base-64 verschlüsselt) erstellt werden.

Ergebnisse

Der Befehl generiert die folgenden CSR-Dateien:

- Die Datei `CAMKeystore` im Verzeichnis *`installationsposition`*`\configuration\certs`
- Die Datei `encryptRequest.csr` im Verzeichnis *`installationsposition`*`\bin`

Nächste Schritte

Führen Sie die folgenden Schritte aus, nachdem die CSR-Dateien generiert worden sind:

- Geben Sie die Verschlüsselungsschlüsseldatei `encryptRequest.csr` oder deren Inhalt für die gemeinsame Nutzung mit der externen Zertifizierungsstelle frei.

  Mit diesem Schlüssel erstellt die Zertifizierungsstelle (CA) ein Verschlüsselungsschlüsselzertifikat, ein Stammzertifikat und ein Zwischenzertifikat für die Anforderung und nutzt diese Zertifikate gemeinsam mit Ihrer Organisation.

  Details zum Zertifikatsaustauschprozess zwischen Ihrer Organisation und der externen Zertifizierungsstelle (CA) finden enthält die Dokumentation der entsprechenden CA.
- Kopieren Sie die Zertifikate von der externen Zertifizierungsstelle (CA) in das Installationsverzeichnis von Cognos Analytics, z. B. in *`installationsposition`*`\configuration\bin`.
- Importieren Sie die Zertifikate in Ihren Cognos Analytics-Schlüsselspeicher. Weitere Informationen finden Sie im Abschnitt „Importieren der Zertifikate der Zertifizierungsstelle (CA)" auf Seite 206.

Importieren der Zertifikate der Zertifizierungsstelle (CA)

Sie müssen die Zertifikate von der externen Zertifizierungsstelle (Certificate Authority, CA) in Ihren IBM Cognos Analytics-Keystore importieren.

Der Importvorgang muss auf jedem Computer durchgeführt werden, auf dem die folgenden Cognos Analytics-Komponenten installiert sind: Content Manager, die Komponenten der Anwendungsebene, das Gateway und die Clientkomponenten wie z. B. Framework Manager sowie andere Komponenten, sofern Sie diese verwenden.

Vorbereitende Schritte

Unter UNIX und Linux müssen Sie vor Verwendung von **ThirdPartyCertificateTool** sicherstellen, dass die Umgebungsvariable JAVA_HOME gesetzt ist.

Bei Installationen unter Microsoft Windows können Sie das Tool wie im nachfolgenden Beispiel veranschaulicht mit dem Befehl `-java:local` ausführen, damit die mit der Installation bereitgestellte JRE verwendet wird: `ThirdPartyCertificateTool.bat -java:local -c -d ...`

Informationen zu diesem Vorgang

Wenn Sie das **Keystore-Kennwort** in IBM Cognos Configuration geändert haben (unter **Verschlüsselung** > **Cognos**), verwenden Sie für *keystore_password* beim Ausführen der nachfolgenden **ThirdPartyCertificateTool**-Befehle das neue Kennwort. Das Standardkennwort lautet **`NoPassWordSet`**.

Vorgehensweise

1. Wechseln Sie zu der Speicherposition, an der Sie die Zertifikatsdateien der Zertifizierungsstelle (CA) gespeichert haben, und gehen Sie wie folgt vor:

a) Erstellen Sie eine Kopie des Verschlüsselungszertifikats und benennen Sie sie `encryptCertificate.cer`.

b) Erstellen Sie eine Kopie des Stammzertifikats der Zertifizierungsstelle benennen Sie sie `ca.cer`.

2. Falls die Dateien nicht bereits dort vorhanden sind, kopieren Sie die Dateien `encryptCertificate.cer` und `ca.cer` in das Verzeichnis *installationsposition*`/bin`.
3. Starten Sie aus dem Verzeichnis *installationsposition*`/bin` heraus das Befehlszeilentool **ThirdPartyCertificateTool**.
4. Geben Sie zum Importieren des CA-Stammzertifikats in den Cognos Analytics-Truststore den folgenden Befehl ein:

   - Geben Sie unter UNIX oder Linux Folgendes ein:

     ```
     ThirdPartyCertificateTool.sh -i -T -r ca.cer -p keystore-kennwort
     ```

   - Geben Sie unter Windows Folgendes ein:

     ```
     ThirdPartyCertificateTool.bat -i -T -r ca.cer -p keystore-kennwort
     ```

   Der Befehl liest die Datei `ca.cer` und importiert den Inhalt mit dem angegebenen Kennwort in die Datei `CAMKeystore` im Verzeichnis `certs`.
5. Optional: Falls Sie CA-Zwischenzertifikate verwenden, importieren Sie alle Zwischenzertifikate (Zertifikate einer Intermediate Certificate Authority, ICA-Zertifikate) in den Cognos Analytics-Truststore. Verwenden Sie dazu dieselben Befehle wie in Schritt 4.
6. Importieren Sie das Verschlüsselungszertifikat durch Eingeben des folgenden Befehls in den Cognos Analytics-Verschlüsselungsschlüsselspeicher:

   - Geben Sie unter UNIX oder Linux Folgendes ein:

     ```
     ThirdPartyCertificateTool.sh -i -e -r encryptCertificate.cer -p
     keystore-kennwort -t ca.cer
     ```

   - Geben Sie unter Windows Folgendes ein:

     ```
     ThirdPartyCertificateTool.bat -i -e -r encryptCertificate.cer -p
     keystore-kennwort -t ca.cer
     ```

   Wichtig: Stellen Sie sicher, dass Sie für *keystore-kennwort* dasselbe Kennwort angeben, das Sie eingegeben haben, als Sie in der vorherigen Aufgabe den Verschlüsselungsschlüssel exportiert haben.

   Sie können alle Warnungen in Bezug auf die Protokollierung ignorieren.

Ergebnisse

Der Befehl liest die Dateien `encryptCertificate.cer` und `ca.cer` im Verzeichnis *installationsposition*`\bin` und importiert die Zertifikate aus beiden Dateien unter Verwendung des angegebenen Kennworts in die Datei `CAMKeystore` im Verzeichnis *installationsposition*`/configuration/certs`.

Nächste Schritte

Jetzt können Sie die Cognos Analytics-Komponenten zur Verwendung der CA-Zertifikate konfigurieren. Weitere Informationen finden Sie im Abschnitt „Aktivieren der externen Zertifizierungsstelle (CA)” auf Seite 207.

Aktivieren der externen Zertifizierungsstelle (CA)

Verwenden Sie nach dem Import der Zertifikate der externen Zertifizierungsstelle (Certificate Authority, CA) IBM Cognos Configuration für die Konfiguration der einzelnen Computer, auf denen eine IBM Cognos Analytics-Komponente installiert ist. Diese Computer müssen so konfiguriert werden, dass die externe Zertifizierungsstelle verwendet wird.

Informationen zu diesem Vorgang

Stellen Sie sicher, dass die Keystore-Speicherpositionen und -Kennwörter in IBM Cognos Configuration mit den in das Tool **ThirdPartyCertificateTool** eingegebenen Verzeichnissen und Kennwörtern übereinstimmen.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration als Administrator.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** > **Verschlüsselung** auf **Cognos**.
3. Klicken Sie unter **Einstellungen für Zertifizierungsstelle** auf die Eigenschaft **Zertifizierungsstelle eines anderen Anbieters verwenden** und legen Sie als zugehörigen **Wert** die Angabe **Wahr** fest.
4. Geben Sie für die Eigenschaft **Keystore-Kennwort** das Kennwort ein, das Sie für den Verschlüsselungsschlüssel verwendet haben.
5. Klicken Sie zum Speichern der Konfiguration auf **Datei** > **Speichern**.
6. Starten Sie die IBM Cognos-Services neu.

Konfigurieren des SSL-Protokolls für Cognos Analytics-Komponenten

Sie können das Secure Sockets Layer-Protokoll (SSL) für die Kommunikation zwischen IBM Cognos-Komponenten in Installationen auf einem einzelnen Server und in verteilten Installationen verwenden.

IBM WebSphere Liberty Profile-Connector

Wenn der interne Dispatcher-URI das Präfix 'HTTP' aufweist, der externe Dispatcher-URI jedoch das Präfix 'HTTPS' (oder umgekehrt), sind sowohl die Liberty HTTP/1.1-Anschlüsse mit SSL als auch die Liberty HTTP/1.1-Anschlüsse ohne SSL in der Datei `server.xml` aktiviert.

Wenn die internen und externen Dispatcher-URIs verschiedene Protokolle oder Ports verwenden, kann der interne Dispatcher-Port nur von den Komponenten auf dem lokalen Computer aufgerufen werden. Der interne Dispatcher-URI muss auch den lokalen Host angeben.

Installationen auf einem einzigen Computer

Wenn Sie bei einer Installation auf einem einzigen Computer kein SSL verwenden, müssen Sie den Service anhalten, bevor Sie das Protokoll in 'https' ändern. Nachdem Sie die Konfiguration mit den SSL-Einstellungen gespeichert haben, können Sie den Service neu starten.

Verteilte Installationen

In verteilten Installationen müssen Sie zunächst den Computer, auf dem der standardmäßig aktive Content Manager installiert ist, für die Verwendung des SSL-Protokolls konfigurieren und die Services dann auf diesem Computer starten, bevor Sie die Komponenten der Anwendungsebene und die Gateway-Komponenten für die Verwendung von SSL konfigurieren.

Hinzufügen von Computern zu einer Installation

Wenn Sie einer SSL-fähigen Umgebung einen Computer hinzufügen, werden Sie beim Speichern der Konfiguration aufgefordert, das Zertifikat vorläufig als vertrauenswürdig zu akzeptieren. Indem Sie das vorläufige Zertifikat akzeptieren, kann zwischen dem betreffenden Computer und den vorhandenen Komponenten eine dauerhafte Vertrauensebene hergestellt werden.

Hinzufügen von Komponenten zu einem Computer

Wenn Sie eine Komponente zu einer Installation hinzufügen, die bereits für die Verwendung von SSL konfiguriert wurde, wird die Vertrauensstellung für die SSL-Zertifikate von den vorhandenen Komponen-

ten vorausgesetzt. Wenn Sie die Komponenten auf demselben Computer in einer Umgebung hinzufügen, die bereits für SSL konfiguriert ist, dabei aber eine andere Position wählen, werden Sie beim Speichern der Konfiguration aufgefordert, das Zertifikat vorläufig als vertrauenswürdig zu akzeptieren. Indem Sie das vorläufige Zertifikat akzeptieren, kann zwischen dem betreffenden Computer und den vorhandenen Komponenten eine dauerhafte Vertrauensebene hergestellt werden.

Konfigurieren von SSL für Cognos Analytics-Komponenten

Für IBM Cognos-Komponenten können Sie SSL für interne oder externe Verbindungen oder für beide Verbindungstypen verwenden.

Wenn Sie SSL nur für interne Verbindungen konfigurieren, kommunizieren die IBM Cognos-Komponenten auf dem lokalen Computer mithilfe dieses Protokolls. Der Dispatcher ist für sichere Verbindungen auf einem anderen Port empfangsbereit als für Remote-HTTP-Anforderungen. Sie müssen daher zwei Dispatcher-URIs konfigurieren.

Wenn Sie SSL nur für externe Verbindungen konfigurieren, wird für die Kommunikation von fernen IBM Cognos-Komponenten zum lokalen Computer das SSL-Protokoll verwendet. Sie müssen den Dispatcher so konfigurieren, dass er für sichere Fernanforderungen auf einem anderen Port empfangsbereit ist als für lokale HTTP-Anforderungen. Sie müssen auch die Content Manager-URIs und den Dispatcher-URI für externe Anwendungen konfigurieren, um dasselbe Protokoll und denselben Port zu verwenden wie der externe Dispatcher.

Wenn Sie SSL für alle Verbindungen konfigurieren, kann der Dispatcher denselben Port für interne und externe Verbindungen verwenden. Auf ähnliche Weise kann der Dispatcher denselben Port für die gesamte Kommunikation verwenden, wenn Sie SSL nicht für die lokale oder entfernte Kommunikation verwenden.

Standardmäßig verwenden IBM Cognos Analytics-Komponenten eine interne Zertifizierungsstelle (Certificate Authority, CA), um die Vertrauenswürdigkeitsbasis in der IBM Cognos-Sicherheitsinfrastruktur herzustellen. Dies gilt sowohl für SSL- als auch für Nicht-SSL-Verbindungen. Wenn Sie Zertifikate verwenden möchten, die von einem anderen Service verwaltet werden, lesen Sie die Informationen in „Konfigurieren von Cognos Analytics-Komponenten für die Verwendung einer anderen Zertifizierungsstelle” auf Seite 204.

Wenn Sie ein optionales Gateway (HTTP oder HTTPS) verwenden, müssen Sie den Web-Server so konfigurieren, dass er Cognos Analytics-Zertifikaten vertraut. Weitere Informationen finden Sie im Abschnitt „Kopieren des Cognos Analytics-Zertifikats auf einen anderen Server” auf Seite 211.

In verteilten Installationen müssen Sie zunächst den Computer, auf dem der standardmäßig aktive Content Manager installiert ist, für die Verwendung des SSL-Protokolls konfigurieren und die Services dann auf diesem Computer starten, bevor Sie den Computer der Komponenten der Anwendungsebene konfigurieren.

Wichtig: Sie müssen vollständig qualifizierte Hostnamen in den Werten für die folgenden Felder von Cognos Configuration angeben. Jeder Wert, den Sie angeben, muss auch im Feld **Subject Alternative Name** > **DNS-Namen** oder im Feld **Subject Alternative Name** > **IP-Adressen** angezeigt werden.

- **Umgebung**
  - **Gateway-URI**
  - **Externer Dispatcher-URI**
  - **Interner Dispatcher-URI**
  - **Dispatcher-URI für externe Anwendungen**
  - **Content Manager-URIs**
- **Umgebung** > **Konfigurationsgruppe**
  - **Gruppenkontakthost**
  - **Host für die Koordination von Mitgliedern**
- **Zugriffsschutz** > **Verschlüsselung** > **Cognos**
  - **Allgemeiner Servername**

– **Subject Alternative Name** > **DNS-Namen**
– **Subject Alternative Name** > **IP-Adressen**

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
   - Konfigurieren Sie im Fenster **Umgebung - Gruppeneigenschaften** alle URIs mit dem vollständig qualifizierten Domänennamen des Servers. Beachten Sie die Informationen in der folgenden Tabelle für Ihr SSL-Verbindungsszenario:

SSL-Verbindungsszenario	**Umgebungs-URI-Konfigurationsdetails**
SSL nur für interne Verbindungen	Geben Sie für die Eigenschaft **Interner Dispatcher-URI** den Wert `https` sowie eine Portnummer für die SSL-Kommunikation ein. Belassen Sie für die Eigenschaften **Externer Dispatcher-URI** und **Dispatcher-URI für externe Anwendungen** den Wert `http` als Protokoll und verwenden Sie die Standardportnummer oder eine andere verfügbare Portnummer.
SSL nur für externe Verbindungen	Geben Sie für die Eigenschaften **Externer Dispatcher-URI** und **Dispatcher-URI für externe Anwendungen** den Wert `https` und eine Portnummer für die SSL-Kommunikation ein. Belassen Sie für die Eigenschaft **Interner Dispatcher-URI** den Wert `http` als Protokoll und verwenden Sie die Standardportnummer oder eine andere verfügbare Portnummer. Die Portnummern in den beiden Dispatcher-URIs müssen unterschiedlich sein.
SSL für alle Verbindungen	Geben Sie denselben URI für die Eigenschaften **Interner Dispatcher-URI**, **Externer Dispatcher-URI** und **Dispatcher-URI für externe Anwendungen** an. Geben Sie `https` und eine Portnummer für die SSL-Kommunikation ein. Zusätzlich können Sie für die Eigenschaft **Content Manager-URIs** den Wert `https` und eine Portnummer für die SSL-Kommunikation festlegen.
Gateway, das auf einem separaten Computer installiert ist und SSL für externe Verbindungen verwendet	Starten Sie IBM Cognos Configuration auf dem Gateway-Computer. Geben Sie für die Eigenschaft **Dispatcher-URIs für das Gateway** den Wert `https` und eine Portnummer für die SSL-Kommunikation ein.

3. Klicken Sie im Fenster **Explorer** auf **Umgebung** > **Konfigurationsgruppe**. Führen Sie anschließend im Fenster **Konfigurationsgruppe - Komponenteneigenschaften** die folgenden Schritte aus:
   a) Setzen Sie den **Gruppenkontakthost** auf den vollständig qualifizierten Domänennamen des Computers, auf dem der primäre Content Manager installiert ist.

      Wichtig: Jeder Computer, ob auf der Anwendungsebene oder der Datenebene, muss denselben Wert verwenden, der auf dem primären Content Manager-Computer angegeben ist.

Wenn Sie den primären Knoten für die Konfigurationsgruppe konfigurieren, muss der Wert in diesem Feld mit dem DNS-Namen oder der IP-Adresse übereinstimmen, der bzw. die für den **Subject Alternative Name** in Schritt „4.b" auf Seite 211 angegeben wurde.

b) Legen Sie den **Host für die Koordination von Mitgliedern** auf den vollständig qualifizierten Domänennamen fest, den Sie in Schritt „2" auf Seite 210 festgelegt haben.

4. Klicken Sie im Fenster **Explorer** auf **Zugriffsschutz** > **Verschlüsselung** > **Cognos**. Führen Sie anschließend im Fenster **Cognos - Provider - Ressourceneigenschaften** die folgenden Schritte aus:
   a) Stellen Sie sicher, dass der Wert für den allgemeinen Servernamen der vollständig qualifizierte Domänenname des Servers ist.
   b) Geben Sie unter **Subject Alternative Name** die DNS-Namen, IP-Adressen und E-Mail-Adressen (optional) an, die dem Serverzertifikat zugeordnet sind.

      Wichtig: Die DNS-Namen und IP-Adressen müssen mit dem vollständig qualifizierten Domänennamen in den Umgebungs-URIs in Schritt „2" auf Seite 210 übereinstimmen. Wenn der Server über mehrere DNS-Namen verfügt, müssen Sie die einzelnen Namen, getrennt durch Leerzeichen, eingeben. Wenn der Server über mehrere IP-Adressen verfügt, müssen Sie die einzelnen Namen, getrennt durch Leerzeichen, eingeben.
5. Klicken Sie im Menü **Datei** auf **Speichern**.
6. Starten Sie die Services neu.

   Starten Sie in einer verteilten Umgebung zuerst die Services auf dem Content Manager-Computer und anschließend die Services auf den Computern mit den Komponenten der Anwendungsebene.

Gemeinsame Vertrauenswürdigkeit von Cognos Analytics-Servern und anderen Servern aktivieren

Wenn Sie die Standardzertifizierungsstelle von IBM Cognos verwenden und mit SSL Verbindungen von anderen Servern zu IBM Cognos-Servern herstellen möchten, müssen Sie das IBM Cognos-Zertifikat dem Truststore auf den anderen Servern hinzufügen.

Anmerkung: Wenn Sie mithilfe von Browsern eine Verbindung zu IBM Cognos-Komponenten herstellen, fordern die Browser Benutzer automatisch zur Aktualisierung ihrer Truststores auf.

Wenn Sie möchten, dass die Verbindung zwischen IBM Cognos-Servern und dem anderen Server gegenseitig authentifiziert wird, müssen Sie zusätzlich für die IBM Cognos-Server das Zertifikat von Ihrer Zertifizierungsstelle in den Truststore kopieren.

Wenn Sie IBM Cognos-Komponenten für die Verwendung einer anderen Zertifizierungsstelle (Certificate Authority, CA) konfiguriert haben, müssen Sie keine gemeinsame Vertrauenswürdigkeit zwischen dem IBM Cognos-Server und anderen Servern einrichten.

Kopieren des Cognos Analytics-Zertifikats auf einen anderen Server

Um das IBM Cognos-Zertifikat dem Truststore auf anderen Servern hinzuzufügen, müssen Sie das Zertifikat auf den Server kopieren.

Bei Umgebungen mit mehreren Servern müssen Sie alle Cognos Analytics-Berechtigungszertifikate für jede Installation, die einen aktiven Content Manager enthält, exportieren und sie in Ziel-Web-Server importieren, wofür eine Vertrauensbeziehung erforderlich ist.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *installationsposition*/bin.
2. Extrahieren Sie das IBM Cognos-Zertifikat, indem Sie den folgenden Befehl eingeben:
   - Geben Sie unter UNIX oder Linux Folgendes ein:

     ```
     ThirdPartyCertificateTool.sh -E -T -r Zieldatei -p NoPassWordSet
     ```
   - Geben Sie unter Microsoft Windows Folgendes ein:

```
ThirdPartyCertificateTool.bat -E -T -r Zieldatei -p NoPassWordSet
```

3. Importieren Sie das Zertifikat in den Truststore auf Ihrem Server.

   Informationen zum Aktualisieren des Server-Truststore finden Sie in der Serverdokumentation.

Kopieren des CA-Zertifikats auf Cognos Analytics-Server

Kopieren Sie nach dem Kopieren des IBM Cognos-Zertifikats auf die anderen Server das Zertifikat von der Zertifizierungsstelle auf den IBM Cognos-Server.

Bestimmte Server, denen der IBM Cognos Analytics-Server vertrauen muss, haben Zertifikate, die von einer Intermediate Certificate Authority (ICA) eines anderen Anbieters signiert wurden. Das ICA-Zertifikat kann entweder von einer oder mehreren ICAs oder von der endgültigen Zertifizierungsstelle eines anderen Anbieters signiert werden.

Sie müssen die vollständige Vertrauenswürdigkeitsbasis (Root of Trust) in den Cognos-Keystore importieren, beginnend mit der Stammzertifizierungsstelle, sowie jede ICA, die an der Signatur des Serverzertifikats beteiligt ist, mit dem das CA-Zertifikat eine Vertrauensbasis aufzubauen muss.

Vorgehensweise

1. Kopieren Sie das Zertifikat von Ihrer Zertifizierungsstelle an eine sichere Position auf dem IBM Cognos-Server.

   Stellen Sie sicher, dass das CA-Zertifikat im Base-64-codierten X.509-Format vorliegt.
2. Wechseln Sie in das Verzeichnis *installationsposition*/bin.
3. Importieren Sie das CA-Zertifikat mit folgendem Befehl:
   - Geben Sie unter UNIX oder Linux Folgendes ein:

     ```
     ThirdPartyCertificateTool.sh -T -i -r CA-Zertifikatsdatei -p NoPassWordSet
     ```
   - Geben Sie unter Microsoft Windows Folgendes ein:

     ```
     ThirdPartyCertificateTool.bat -T -i -r CA-Zertifikatsdatei -p NoPassWordSet
     ```

Auswählen und Einstufen von Cipher Suites für SSL

Eine SSL-Verbindung (SSL = Secure Socket Layer) beginnt mit einer Verhandlung, in der der Client und der Server eine Liste der unterstützten Cipher Suites in der Liste der zugehörigen Priorität präsentieren. Durch einen Chiffriersatz wird die Schutzqualität für die Verbindung bestimmt. Er enthält kryptografische, Authentifizierungs-, Hash- und Key Exchange-Algorithmen. Vom SSL-Protokoll wird der Chiffriersatz ausgewählt, der die höchste Priorität hat und sowohl vom Client als auch vom Server unterstützt wird.

Eine Liste unterstützter Cipher Suites für SSL wird bereitgestellt. Sie können die Cipher Suites, die Ihren Anforderungen nicht gerecht werden, löschen und anschließend den verbleibenden Cipher Suites eine Priorität oder Vorgabe zuweisen. Für die Verhandlung zwischen Client und Server werden die ausgewählten Cipher Suites nach Priorität geordnet bereitgestellt. Es muss mindestens einer der ausgewählten Cipher Suites zwischen den Client- und Serverplattformen übereinstimmen.

Die Liste unterstützter Cipher Suites wird auf jedem Computer dynamisch erzeugt und ist von der Java Runtime Environment (JRE) oder davon abhängig, ob auf dem Computer andere kryptografische Software installiert ist. Wenn Sie am Computer Änderungen vornehmen, z. B. die JRE aktualisieren oder Software installieren, durch die die JRE aktualisiert wird, kann sich dies auf die Verfügbarkeit der unterstützten Cipher Suites auf dem Computer auswirken. Falls kein unterstützter Chiffriersatz mehr verfügbar ist, der mit den anderen Computern der Umgebung übereinstimmt, müssen Sie gegebenenfalls die JRE auf dem Computer ändern, um diese an die anderen Computer der Umgebung anzupassen.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Klicken Sie im Fenster **Explorer** auf **Verschlüsselung** > **Cognos**.

3. Klicken Sie im Fenster **Eigenschaften** auf die Spalte **Wert** für die Eigenschaft **Unterstützte Cipher Suites**.
4. Klicken Sie auf das Bearbeitungssymbol  .
   - Klicken Sie zum Verschieben eines Chiffriersatzes in die Liste **Aktuelle Werte** auf das entsprechende Kontrollkästchen in der Liste **Verfügbare Werte** und anschließend auf **Hinzufügen**.
   - Klicken Sie zum vertikalen Verschieben eines Chiffriersatzes innerhalb der Liste **Aktuelle Werte** auf das Kontrollkästchen und anschließend auf den Nach-oben- oder Nach-unten-Pfeil.
   - Um einen Chiffriersatz aus der Liste **Aktuelle Werte** zu entfernen, klicken Sie auf das Kontrollkästchen und klicken Sie dann auf **Entfernen**.
5. Klicken Sie auf **OK**.
6. Klicken Sie im Menü **Datei** auf **Speichern**.

Verwendung des SSL-Protokolls für die Datenbankkommunikation

Für die Kommunikation zwischen IBM Cognos Analytics und Datenbanken, die vom **Content Manager-Service**, **Benachrichtigungsservice**, **Mobile-Service**, **Service für benutzergeführte Aufgaben und Anmerkungsservice**, und **Protokollierungsservice** verwendet werden, können Sie das SSL-Protokoll (SSL = Secure Sockets Layer) aktivieren.

Die Datenbanken müssen bereits für eine Verwendung mit IBM Cognos Analytics konfiguriert sein. Weitere Informationen zum Konfigurieren der unterstützten Datenbanken finden Sie in den Abschnitten „Richtlinien zum Erstellen des Content Store" auf Seite 7, „Ändern der Benachrichtigungsdatenbank" auf Seite 199, „Einrichten einer Datenbank für benutzergeführte Aufgaben und Anmerkungen" auf Seite 249 und „Richtlinien zum Erstellen einer Protokolldatenbank" auf Seite 225.

SSL-Unterstützung ist für alle unterstützten Datenbanken verfügbar, mit Ausnahme von IBM Db2 for z/OS.

Bevor Sie die SSL-Verschlüsselung in IBM Cognos aktivieren können, muss SSL auf dem Datenbankserver aktiviert sein und die Datenbankclients müssen so konfiguriert sein, dass sie SSL-Verbindungen zum Datenbankserver verwenden.

Überprüfen Sie anhand der Dokumentation Ihres Datenbankanbieters, welche SSL-Eigenschaften für die verschiedenen Datenbankversionen anzugeben sind.

Aktivieren von SSL für die Kommunikation mit Db2- und Informix-Datenbanken

Sie können das SSL-Protokoll (SSL = Secure Sockets Layer) für die Kommunikation zwischen IBM Cognos Analytics und IBM Db2- bzw. Informix Dynamic Server-Datenbanken aktivieren.

Folgende Datenbanken können konfiguriert werden: Datenbanken für **Content Manager**, **Benachrichtigungen**, **Mobile**, den **Service für benutzergeführte Aufgaben und Anmerkungsservice** sowie für die **Protokollierung**.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie auf Ihrem Datenbankserver SSL aktivieren, bevor Sie die Schritte in IBM Cognos Configuration ausführen.

Vorgehensweise

1. Führen Sie die in der Dokumentation zur jeweiligen Datenbankversion beschriebenen Schritte aus, um SSL für den Datenbankserver zu aktivieren und das SSL-Zertifikat zu exportieren.
2. Laden Sie die JAR-Dateien für die Richtlinien des Typs 'Unlimited Strength' herunter.

Anmerkung: Neuere Versionen der JRE enthalten die JCE-Dateien standardmäßig. Diese Dateien befinden sich in dem folgenden Verzeichnis: `installationsposition/ibm-jre/jre/lib/security/policy/unlimited/`

Wenn Sie die IBM JRE verwenden möchten, können Sie auch https://public.dhe.ibm.com/ibmdl/export/pub/systems/cloud/runtimes/java/security/jce_policy aufrufen und `jurisdiction_policy_files.zip` herunterladen. Dekomprimieren Sie die Richtliniendateien in das Verzeichnis *installationsposition*`/ibm-jre/jre/lib/security`.

3. Importieren Sie das SSL-Zertifikat auf dem Computer, auf dem Sie das SSL-Protokoll konfigurieren, mit dem Dienstprogramm 'keytool' für die JRE, die Sie für IBM Cognos Analytics verwenden.

   Wenn Sie die JRE verwenden, die mit Cognos Analytics-Installationen unter Microsoft Windows-Betriebssystemen bereitgestellt wird, führen Sie die folgenden Schritte aus:

   a) Wechseln Sie zum Verzeichnis *installationsposition*`/ibm-jre/jre/bin` und führen Sie den folgenden Befehl aus:

   ```
   keytool -import -file Pfad/Dateipfad -keystore Keystore-Name -alias Aliasname
   ```

   Bei *keystorename* handelt es sich um einen Namen für einen neuen Keystore und *aliasname* ist ein Alias, den Sie für das Zertifikat auswählen.

   b) Geben Sie ein Kennwort für den Keystore ein. Wenn Sie das Zertifikat zu einem vorhandenen Keystore hinzufügen möchten, geben Sie das Kennwort für den entsprechenden Keystore ein. Wenn Sie einen neuen Keystore erstellen möchten, geben Sie ein Kennwort für den neuen Keystore ein.

   Wichtig: Das SSL-Zertifikat muss in den Keystore für die JRE importiert werden, die für IBM Cognos Analytics verwendet wird.

4. Bearbeiten Sie die Datei `java.security`, um den SSL-Provider einzufügen.

   a) Wenn Sie die JRE verwenden, die mit IBM Cognos Analytics-Installationen unter Microsoft Windows-Betriebssystemen bereitgestellt wird, wechseln Sie in das Verzeichnis *installationsposition*`/ibm-jre/jre/lib/security`. Navigieren Sie andernfalls zum Verzeichnis `lib/security` für die JRE, die Sie für IBM Cognos Analytics verwenden.

   b) Öffnen Sie die Datei `java.security` in einem Texteditor.

   c) Fügen Sie zur Liste der Provider in der Datei die folgende Zeile hinzu:

   ```
   security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
   ```

   Wichtig: Stellen Sie sicher, dass Sie die Zeile vor `security.provider.2=com.ibm.crypto.provider.IBMJCE` hinzufügen.

   d) Ändern Sie die Zahlen für die nachfolgenden `security.provider`-Einträge so, dass sie nach dem Einschließen von `security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS` in der Liste sequenziell sind.

   e) Suchen Sie nach den folgenden Zeilen in der Datei.

   ```
   ssl.KeyManagerFactory.algorithm=IbmX509
   ssl.TrustManagerFactory.algorithm=PKIX
   ```

   f) Fügen Sie die folgenden Zeilen nach den oben angegebenen Zeilen hinzu.

   ```
   ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
   ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
   ```

   g) Speichern Sie die Datei und schließen Sie sie.

5. Wechseln Sie in das Verzeichnis *Installationsposition*`/bin64` und öffnen Sie die Datei `bootstrap_wlp_`*Betriebssystemversion*`.xml` in einem Texteditor.

   Diese Datei wird verwendet, wenn IBM Cognos Analytics als Service von IBM Cognos Configuration aus gestartet wird.

   a) Fügen Sie die folgenden Zeilen zur Datei hinzu.

```
<param>"-Dcom.ibm.jsse2.usefipsprovider=true"</param>
<param>"-Djavax.net.ssl.trustStore=path/keystorename"</param>
```

Die Angabe *Pfad* steht für den Pfad zum Keystore und *Keystore-Name* ist der Name des Keystores.

b) Speichern Sie die Datei und schließen Sie sie.

6. Wechseln Sie in das Verzeichnis *Installationsposition*/bin64 und öffnen Sie die Datei cogconfig.bat (bzw. 'cogconfig.sh' bei UNIX oder Linux) in einem Texteditor.

a) Suchen Sie nach der folgenden Zeile in der Datei.

Windows:

```
J_OPTS=%DD_OPTS% %J_OPTS% %DEBUG_OPTS%
```

Linux, UNIX:

```
$JAVA_CMD $JAVA_OPTS CRConfig $*
```

b) Fügen Sie die folgenden Zeilen vor den oben angegebenen Zeilen hinzu.

Windows:

```
set J_OPTS=-Dcom.ibm.jsse2.usefipsprovider=true %J_OPTS%
set J_OPTS=-Djavax.net.ssl.trustStore=path/keystorename %J_OPTS%
```

Linux, UNIX:

```
JAVA_OPTS="$JAVA_OPTS -Dcom.ibm.jsse2.usefipsprovider=true $JAVA_OPTS"
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStore=path/keystorename $JAVA_OPTS"
```

Die Angabe *Pfad* steht für den Pfad zum Keystore und *Keystore-Name* ist der Name des Keystores.

c) Speichern Sie die Datei und schließen Sie sie.

7. Starten Sie IBM Cognos Configuration durch Doppelklicken auf die Datei cogconfig, an der Sie in Schritt 6 Änderungen vorgenommen haben.
8. Klicken Sie unter **Datenzugriff** auf den Namen der Datenbank, die Sie konfigurieren möchten. Klicken Sie zum Konfigurieren der Content Store-Datenbank beispielsweise unter **Content Manager** auf den Namen der Datenbank.

   Weitere Datenbanken, die konfiguriert werden können, sind die Datenbanken für **Benachrichtigungen**, für **Mobile**, für den **Service für benutzergeführte Aufgaben und Anmerkungsservice** sowie für **Protokollierung**.

   Tipp: Wenn Sie die Datenbank für **Protokollierung** konfigurieren möchten, rufen Sie **Umgebung** > **Protokollierung** auf.
9. Klicken Sie im Eigenschaftsfenster auf die Eigenschaft **SSL-Verschlüsselung aktiviert** und legen Sie **Wahr** als zugehörigen Wert fest.
10. Testen Sie die Verbindung.
11. Speichern Sie Ihre Konfiguration und starten Sie Ihre IBM Cognos Analytics-Services erneut.

Aktivieren von SSL für die Kommunikation mit Microsoft SQL Server-Datenbanken

Sie können das SSL-Protokoll (Secure Sockets Layer) für die Kommunikation zwischen IBM Cognos Analytics und Microsoft SQL Server-Datenbanken aktivieren.

Folgende Datenbanken können konfiguriert werden: Datenbanken für **Content Manager**, **Benachrichtigungen**, **Mobile**, den **Service für benutzergeführte Aufgaben und Anmerkungsservice** sowie für die **Protokollierung**.

Weitere Informationen zum Konfigurieren von SQL Server für SSL enthält die Dokumentation für Ihre Version von Microsoft SQL Server.

Anmerkung: Microsoft SQL Server verwendet unterschiedliche Namen für die JAR-Treiberdateien, z. B. `sqljdbc4.jar`, `sqljdbc41.jar` und `sqljdbc42.jar`. Offiziell unterstützt `sqljdbc42.jar` die Version JRE8, was der von IBM Cognos Analytics verwendeten Version entspricht.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie auf Ihrem Datenbankserver SSL aktivieren, bevor Sie die Schritte in IBM Cognos Configuration ausführen.

Vorgehensweise

1. Rufen Sie das Stammzertifikat der Zertifizierungsstelle (CA = Certificate Authority) ab, von der Ihr SQL Server-Zertifikat ausgestellt wurde (oder das selbst signierte Serverzertifikat ab, falls das Zertifikat nicht von einer Zertifizierungsstelle ausgestellt wurde) und kopieren Sie das Zertifikat auf den Computer, auf dem Cognos Analytics installiert ist.

   Kopieren Sie zum Beispiel durch Eingabe des folgenden Befehls die Datei `sqlcert.cer` in das Stammverzeichnis `c:\sqlcert.cer`:

   ```
   cd C:\Programme\ibm\cognos\analytics\ibm-jre\jre\lib\security
   ```

   Geben Sie dann den folgenden Befehl ein:

   ```
   C:\Progra~1\ibm\cognos\analytics\ibm-jre\jre\bin\keytool
   -import -trustcacerts -file "c:\sqlcert.cer" -keystore cacerts -alias SQLCert
   ```

2. Bearbeiten Sie die Datei *Installationsposition*`\bin64\bootstrap_wlp_`*Betriebssystem-version*`.xml`, indem Sie nach der Zeile `<param condName="${java_vendor}" condValue="IBM">-Xscmaxaot4m</param>` die folgenden Zeilen hinzufügen:

   Windows:

   ```
   <param>"-Dcom.ibm.jsse2.overrideDefaultTLS=true"</param>
   ```

   Linux, UNIX:

   ```
   <param>-Dcom.ibm.jsse2.overrideDefaultTLS=true</param>
   ```

3. Bearbeiten Sie die Datei *Installationsposition*`\bin64\cogconfig.bat` (Windows) oder die Datei *Installationsposition*`\bin64\cogconfig.sh` (Linux, UNIX), indem Sie nach der Zeile `set J_OPTS=%DD_OPTS% %J_OPTS%` die folgende Zeile hinzufügen:

   Windows:

   ```
   set J_OPTS="-Dcom.ibm.jsse2.overrideDefaultTLS=true" %J_OPTS%
   ```

   Linux, UNIX:

   ```
   JAVA_OPTS=$JAVA_OPTS -Dcom.ibm.jsse2.overrideDefaultTLS=true
   ```

4. Starten Sie IBM Cognos Configuration durch Doppelklicken auf die Datei `cogconfig`, an der Sie in Schritt 3 Änderungen vorgenommen haben.
5. Klicken Sie unter **Datenzugriff** auf den Namen der Datenbank, die Sie konfigurieren möchten. Klicken Sie zum Konfigurieren der Content Store-Datenbank beispielsweise unter **Content Manager** auf den Namen der Datenbank.

   Weitere Datenbanken, die konfiguriert werden können, sind die Datenbanken für **Benachrichtigungen**, für **Mobile**, für den **Service für benutzergeführte Aufgaben und Anmerkungsservice** sowie für **Protokollierung**.

Tipp: Wenn Sie die Datenbank für **Protokollierung** konfigurieren möchten, rufen Sie **Umgebung** > **Protokollierung** auf.

6. Klicken Sie im Eigenschaftsfenster auf die Eigenschaft **SSL-Verschlüsselung aktiviert** und legen Sie **Wahr** als zugehörigen Wert fest.
7. Testen Sie die Verbindung und speichern Sie die Konfiguration.
8. Starten Sie IBM Cognos Analytics. Der vollständige Servername in SQL Server Configuration Manager muss mit dem Namen im Zertifikat übereinstimmen. Er muss zum Beispiel `mycomputer.can-lab.ibm.com` lauten und nicht `localhost`.

Aktivieren von SSL für die Kommunikation mit Oracle-Datenbanken

Sie können das SSL-Protokoll (SSL = Secure Sockets Layer) für die Kommunikation zwischen IBM Cognos Analytics und Oracle-Datenbanken aktivieren.

Folgende Datenbanken können konfiguriert werden: Datenbanken für **Content Manager**, **Benachrichtigungen**, **Mobile**, den **Service für benutzergeführte Aufgaben und Anmerkungsservice** sowie für die **Protokollierung**.

Um Secure Sockets Layer (SSL) mit Oracle-Datenbankverbindungen in IBM Cognos Analyticsverwenden zu können, müssen Sie das SSL-Zertifikat in den Java-Keystore importieren.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie auf Ihrem Datenbankserver SSL aktivieren, bevor Sie die Schritte in IBM Cognos Configuration ausführen.

Tipp: Stellen Sie sicher, dass als Datenbanktyp die Option **Oracle-Datenbank (Erweitert)** und nicht einfach nur **Oracle-Datenbank** angegeben ist.

Vorgehensweise

1. Bearbeiten Sie die Datei `bootstrap_wlp_`*`Betriebssystemversion`*`.xml`.

   Diese Datei wird verwendet, wenn IBM Cognos Analytics als Service von IBM Cognos Configuration aus gestartet wird.

   Tipp: Die Verwendung von doppelten Anführungszeichen in der Datei `bootstrap_wlp_linux38664.xml` verhindert, dass IBM Java gestartet werden kann, und führt dazu, dass der Startvorgang für Cognos blockiert wird und fehlschlägt.

   a) Wechseln Sie in das Verzeichnis *`Installationsposition`*`/bin64` und öffnen Sie die Datei `bootstrap_wlp_`*`Betriebssystemversion`*`.xml` in einem Texteditor.

   b) Fügen Sie unter dem Element <process>, <start>, <spawn> die folgenden Zeilen hinzu:

   ```
   <param>-Doracle.net.ssl_version=Versionsnummer</param>
   <param>-Doracle.net.ssl_client_authentication=false</param>
   <param>-Doracle.net.wallet_location=(SOURCE=(METHOD=file)
   METHOD_DATA=(DIRECTORY=path/client_wallet)))</param>
   ```

   Die Angabe für die *Versionsnummer* muss mit der SSL/TLS-Version Ihrer 'Doracle.net.ssl' übereinstimmen. Beispiel: Wenn die verwendete Version die Versionstufe 1.2 aufweist ist, legen Sie die Version wie folgt fest:

   ```
   <param>-Doracle.net.ssl_version=1.2</param>
   ```

   c) Speichern Sie die Datei und schließen Sie sie.

2. Bearbeiten Sie die Datei `cogconfig`.

   a) Öffnen Sie vom Verzeichnis *`Installationsposition`*`/bin64` aus die Datei `cogconfig.bat` (bzw. `cogconfig.sh` bei UNIX oder Linux) in einem Texteditor.

   b) Fügen Sie die folgenden Zeilen zur Datei hinzu.

```
set J_OPTS=-Doracle.net.ssl_version=Versionsnummer %J_OPTS%
set J_OPTS=-Doracle.net.wallet_location=(SOURCE=(METHOD=file)
(METHOD_DATA=(DIRECTORY=Pfad/Client-Wallet))) %J_OPTS%
set J_OPTS=-Doracle.net.ssl_client_authentication=false %J_OPTS%
```

Die Angabe für *Versionsnummer* von 'Doracle.net.ssl' muss dieselbe wie in Schritt 1b sein.

c) Speichern Sie die Datei und schließen Sie sie.

3. Kopieren Sie die folgenden Oracle-Treiberdateien in das Verzeichnis *Installationsposition*/drivers.
   - jssl-1_1.jar
   - oraclepki.jar
   - osdt_cert.jar
   - osdt_core.jar
4. Starten Sie IBM Cognos Configuration durch Doppelklicken auf die Datei cogconfig, an der Sie in Schritt 2 Änderungen vorgenommen haben.
5. Klicken Sie unter **Datenzugriff** auf den Namen der Datenbank, die Sie konfigurieren möchten. Klicken Sie zum Konfigurieren der Content Store-Datenbank beispielsweise unter **Content Manager** auf den Namen der Datenbank.

   Weitere Datenbanken, die konfiguriert werden können, sind die Datenbanken für **Benachrichtigungen**, für **Mobile**, für den **Service für benutzergeführte Aufgaben und Anmerkungsservice** sowie für **Protokollierung**.

   Tipp: Wenn Sie die Datenbank für **Protokollierung** konfigurieren möchten, rufen Sie **Umgebung** > **Protokollierung** auf.
6. Klicken Sie im Eigenschaftsfenster auf die Eigenschaft **SSL-Verschlüsselung aktiviert** und legen Sie **Wahr** als zugehörigen Wert fest.
7. Testen Sie die Verbindung.
8. Speichern Sie die Konfiguration und starten Sie anschließend die Services neu.

Schützen von JDBC-Datenservern mit SSL

Verwenden Sie die folgende Prozedur, um JDBC-Datenserver mit SSL zu schützen.

Vorgehensweise

1. Stellen Sie sicher, dass der Datenserver für SSL außerhalb der IBM Cognos Analytics-Umgebung konfiguriert ist.
2. Stellen Sie in Cognos Analytics sicher, dass die JDBC-URL- und Verbindungseigenschaften der Datenserververbindung so aktualisiert wurden, dass sie alle erforderlichen Parameter enthalten, die in der Dokumentation des entsprechenden Anbieters für die Aktivierung von SSL über JDBC angegeben sind.
3. Importieren Sie das SSL-Zertifikat bzw. die SSL-Zertifikate in den JRE-Truststore von Cognos Analytics, wie im Abschnitt „Kopieren des CA-Zertifikats auf Cognos Analytics-Server" auf Seite 212 angegeben. Die Zertifikate müssen in das Verzeichnis jre/lib/security/cacerts importiert werden und das Standardkennwort lautet changeit.

Konfigurieren von JDBC-Datenservern für Single Sign-on mit Kerberos

Sie können Single Sign-on (SSO) mit dem Kerberos-Protokoll für JDBC-Datenserververbindungen konfigurieren, die für den dynamischen Abfragemodus (DQM) verwendet werden.

Mit Ausnahme von Microsoft SQL Server wird die SSO-Datenserverauthentifizierung nur für den dynamischen Abfragemodus unterstützt.

Die Unterstützung für eingeschränkte Delegierung (eine Microsoft-Erweiterung für Kerberos) ermöglicht es einem Service, ein Ticket für einen anderen Service im Namen des Benutzers anzufordern, indem der Service sich selbst das Service-Ticket des Benutzers vorlegt. Das Service-Ticket wird entweder vom Benutzer delegiert (Service for User to Proxy - S4U2Proxy) oder vom Service selbst generiert, wenn der Benutzer auf andere Weise authentifiziert wird.

Führen Sie die folgenden Schritte aus, um einen Datenserver für SSO mit Kerberos zu konfigurieren:

- Erstellen Sie eine Kerberos-Initialisierungsdatei.
- Konfigurieren Sie einen SPN (Service Principal Name) für den Datenserver für den dynamischen Abfragemodus.
- Erstellen Sie eine Chiffrierschlüsseldatei.
- Konfigurieren Sie das Kerberos-Anmeldemodul.
- Konfigurieren Sie Datenserververbindungen.

Stellen Sie vor dem Start sicher, dass die folgenden Bedingungen erfüllt sind:

1. Der IBM Cognos-Service ist für Single Sign-on mit einem Microsoft Active Directory-Namespace konfiguriert.
2. Die Datenbank wird für die Verwendung des Kerberos-Protokolls konfiguriert.
3. Die Active Directory-Benutzer sind ebenfalls auf dem Datenbankserver konfiguriert.
4. Wenn SSO mit eingeschränkter Delegierung konfiguriert ist, überprüfen Sie die Treiberdokumentation und vergewissern Sie sich, dass der Treiber eingeschränkte Delegierung unterstützt. Nicht alle Treiber, die die Kerberos-Authentifizierung unterstützen, unterstützen auch eingeschränkte Delegierung.

   Die dynamische Abfrage unterstützt eingeschränkte Kerberos-Delegierung mit den JDBC-Treibern für Netezza und Cloudera Impala. Für diese Funktion sind JDBC-Treiber ab den folgenden Versionen erforderlich, die für den Empfang von GSS-Berechtigungsnachweisen erweitert wurden: Netezza 7.2.0.9-P3 und 7.2.1.3-P3 (weitere Informationen finden Sie unter http://www-01.ibm.com/support/docview.wss?uid=swg21997658) und Cloudera Impala 2.5.36

   IBM Cognos Analytics kann entweder mit einer ORACLE-JRE oder einer IBM JRE verwendet werden. Die für IBM erforderlichen JRE-Versionen finden Sie auf der Seite für unterstützte Umgebungen. Wenn Sie Cognos Analytics mit einer IBM JRE verwenden, muss Cloudera Impala JDBC Version 8.0.3.12 oder eine neuere Version der IBM JRE verwenden. Weitere Informationen finden Sie unter https://developer.ibm.com/javasdk/downloads/sdk8/.

Verwenden der Kerberos-Authentifizierung ohne Single Sign-on

Wenn Sie keinen Active Directory-Namespace konfigurieren, können Sie die Datenquelle dennoch für die Kerberos-Authentifizierung konfigurieren. Der Abfrageservice des dynamischen Abfragemodus interpretiert die von Ihnen angegebenen Berechtigungsnachweise (Benutzername und Kennwort) als Berechtigungsnachweise für das Abrufen eines TGT (Ticket-Granting-Ticket) vom Kerberos Distribution Center (Active Directory oder einer anderen Kerberos-Implementierung). Diese Berechtigungsnachweise können über eine Anmeldung angegeben werden oder vom Benutzer eingegeben werden, wenn dieser zur Angabe der Berechtigungsnachweise aufgefordert wird. In diesem Fall ändern sich die Konfigurationsschritte wie folgt:

- Sie müssen keinen SPN registrieren.
- Sie müssen keine Chiffrierschlüsseldatei erstellen.
- Ein Konfigurieren des Kerberos-Anmeldemoduls ist nicht erforderlich.
- Sie müssen eine Kerberos-Initialisierungsdatei angeben.

Erstellen von Kerberos-Initialisierungsdateien

Sie müssen eine Kerberos-Initialisierungsdatei erstellen und auf allen Computern, auf denen Komponente der Anwendungsebene installiert sind, an einer bestimmten Position speichern. Die Kerberos-Initialisierungsdatei `krb5.conf` wird von der JRE-Implementierung des Kerberos-Protokolls verwendet.

Weitere Informationen zu Kerberos-Initialisierungsdateien finden Sie in der MIT-Kerberos-Dokumentation (web.mit.edu/kerberos/krb5-devel/doc/admin/conf_files/krb5_conf.html).

Vorgehensweise

Kopieren Sie auf allen Computern, auf denen Komponente der Anwendungsebene installiert sind, die Datei `krb5.conf` in das Verzeichnis `JAVA_HOME/lib/security`.

Auf Computern mit UNIX können Sie die Datei `krb5.conf` auch ins Verzeichnis `/etc/krb5` kopieren.

Auf Computern mit Linux können Sie die Datei `krb5.conf` auch ins Verzeichnis `/etc` kopieren.

Auf Computern mit Microsoft Windows kopieren Sie die Datei `krb5.conf` in das Verzeichnis `C:\winnt` und benennen Sie sie in `krb5.ini` um.

Erstellen eines SPN für den Abfrageservice

Sie müssen einen SPN (Service Principal Name) erstellen, den der Abfrageservice verwendet. Dieser SPN muss mit einem Active Directory-Domänenbenutzer konfiguriert werden, der für die Delegierung anerkannt ist.

Für den SPN muss das Format `spn@REALM` verwendet werden. Das Format des spn-Werts ist *Servicename/vollständig qualifizierter Domänenname*. `REALM` ist der Realmname, der in der Kerberos-Initialisierungsdatei konfiguriert ist. Beispiel für den Servicenamen 'dqm': `dqm/myserver.mydomain.com@MYWINDOWSDOMAIN.COM`.

Wenn der Name des Active Directory-Domänenbenutzers 'dqmuser' lautet, verwenden Sie für die Registrierung des SPN den folgenden Befehl:

```
setspn -s dqm/myserver.mydomain.com mywindowsdomain\dqmuser
```

Sie können die Parameter **-L** und **-Q** verwenden, um zu prüfen, ob der SPN ordnungsgemäß erstellt wurde. Beispiel:

```
setspn -L mywindowsdomain\dqmuser
```

```
setspn -Q dqm/myserver.mydomain.com
```

Erstellen einer Chiffrierschlüsseldatei

Nach der Erstellung des SPN (Service Principal Name) müssen Sie eine Chiffrierschlüsseldatei für den Service erstellen. Die Chiffrierschlüsseldatei ermöglicht dem Service eine Anmeldung ohne Kennwort. Wenn das Kennwort des Servicekontos geändert wird, muss die Chiffrierschlüsseldatei erneut erstellt werden.

Vorgehensweise

Verwenden Sie den folgenden Befehl zum Erstellen einer Chiffrierschlüssel:

```
ktpass -out krb5.keytab -princ SPN -mapUser Benutzername -mapOp set -pass Kennwort -pType KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

Zum Beispiel

```
ktpass -out krb5.keytab -princ dqm/meinserver.meinedomain.com@meinewindowsdomäne.com -mapUser dqm-benutzer@meinewindowsdomäne -mapOp set -pass Kennwort -pType KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

Konfigurieren des Kerberos-Anmeldemoduls

Sie müssen das Kerberos-Anmeldemodul konfigurieren, um es dem IBM Cognos-Abfrageservice zu ermöglichen, sich bei der Active Directory-Domäne anzumelden. Um die Anmeldung zu ermöglichen, benötigt das Java Authentication and Authorization Service-Package (JAAS-Package) eine Konfigurationsdatei.

Zur Konfiguration der Anmeldemodule sind zwei Vorgehensweisen möglich.

Konfigurieren des Anmeldemoduls für Kerberos mit Single Sign-on (Active Directory):

1. Wählen Sie in Cognos Configuration den Active Directory-Namespace in **Sicherheit** > **Authentifizierung** aus.
2. Geben Sie in der Eigenschaft **Service Principal Name für DQM** den Wert genau so ein, wie er im Chiffrierschlüssel aufgelistet ist.

   Verwenden Sie den Befehl **`klist -k <keytab file>`**, um den Namen des Prinzipals zu finden.
3. Benennen Sie die Chiffrierschlüsseldatei in `ibmcognosba.keytab` um und speichern Sie sie im Ordner *Installationsposition*`/configuration`.

Cognos Analytics erstellt die erforderliche Anmeldekonfiguration dynamisch.

Eine Konfigurationsdatei muss in der Datei `java.security` im Verzeichnis *JRE_HOME*`/lib/security` enthalten sein. Sie müssen eine Zeile ähnlich der folgenden in die Datei `java.security` einfügen.

```
login.config.url.1=file:///${java.home}/lib/security/jaas.conf
```

JAAS-Konfigurationsbeispiele werden in der IBM Cognos-Installation bereitgestellt. Die Namen der Beispieldateien lauten `jaas-ibm.config` und `jaas-oracle.config`; sie befinden sich im Verzeichnis *Installationsposition*`\configuration`.

In den Beispieldateien müssen Sie die folgenden Werte ersetzen:

- *<Principalname>* ist der SPN, den Sie erstellt haben.
- *<Chiffrierschlüsseldateispezifikation>* ist der Pfad und Dateiname der Chiffrierschlüsseldatei, die Sie erstellt haben.

Wenn Sie keine Datenbankverbindung verwenden, die für die Kerberos-Authentifizierung für die Modellierung konfiguriert ist, können Sie, anstatt die Datei `java.security` zu ändern, die JAAS-Anmeldekonfigurationsdatei als zusätzlichen Startparameter für den Abfrageservice in IBM Cognos Administration angeben. Erweitern Sie in IBM Cognos Administration unter **System** Ihren Server, wählen Sie **Abfrageservice** > **Eigenschaften festlegen** > **Einstellungen** aus und geben Sie den Wert in **Zusätzliche JVM-Argumente für den Abfrageservice** in folgendem Format ein: `-Djava.security.auth.login.config=`*<Konfigurationsdatei>*

Verifizieren der Kerebos-Konfiguration

Wenn Sie die JAAS-Konfiguration (Java Authentication and Authorization Service) und die Chiffrierschlüsseldatei verifizieren möchten, können Sie einen Befehl ausführen, für den Sie den **`java`**-Befehl der JRE nutzen, die von Cognos Analytics verwendet wird.

Vorgehensweise

Führen Sie den folgenden Befehl im Verzeichnis *Installationsposition*`/webapps/p2pd/WEB-INF/lib` aus:

`java -cp xqeService.jar -Dcom.ibm.security.krb5.Krb5Debug=all -Dcom.ibm.security.jgss.debug=all com.cognos.xqe.util.KerberosSSOLoginHelper`

Das Dienstprogramm versucht eine Anmeldung mithilfe der Chiffrierschlüsseldatei und zeigt dabei die Kerberos-Debugausgabe an. Am Ende der Ausgabe wird `Helper login successful` oder `Helper Login failed <error message>` angezeigt.

Verifizieren der JDBC-Treiberfunktionen

Unabhängig davon, ob Single Sign-on konfiguriert ist, ist es für DQM erforderlich, dass der Datenbanktreiber Verbindungen mithilfe eines vorab berechtigten Subjekts herstellen kann. Ein Dienstprogramm, das Teil der IBM Cognos Analytics-Installation ist, bietet Unterstützung beim Testen des Treibers.

Vorbereitende Schritte

Das Dienstprogramm akzeptiert **`url`**, **`uid`** und **`password`** als Parameter. Der Treiber muss im Ordner *`Installationsposition`*`/webapps/p2pd/WEB-INF/lib` installiert werden.

Vorgehensweise

Führen Sie im Ordner *`Installationsposition`*`/webapps/p2pd/WEB-INF/lib` den folgenden Befehl aus, für den Sie den **`java`**-Befehl der von Cognos verwendeten JRE nutzen:

`java -cp xqeService.jar;<driver.jar> com.cognos.xqe.util.KerberosConnectionHelper <Treiberklassenname> <JDBC-URL> <Benutzer> <Kennwort>`

Dabei gilt Folgendes:

- *<driver.jar>* ist die JAR-Datei, die den Treiber enthält. Wenn zu viele JAR-Dateien für den Treiber vorhanden sind, können Sie *"*"* für den Klassenpfadparameter angeben.
- *<Treiberklassenname>* ist der Klassenname, der zum Laden des Treibers verwendet wird.
- *<JDBC-URL>* ist die JDBC-Verbindungs-URL für die Datenquelle, einschließlich der treiberspezifischen Eigenschaften für die Kerberos-Authentifizierung.
- *<Benutzer>* ist der Kerberos-Prinzipal.
- *<Kennwort>* ist das Kennwort des Kerberos-Prinzipals.

Das Dienstprogramm versucht, mithilfe der angegebenen Parameter eine Verbindung zur Datenbank herzustellen, und gibt den Kerberos-Debug-Trace aus.

Konfigurieren von Datenserververbindungen für Single Sign-on mit Kerberos

Orientieren Sie sich an den Richtlinien in diesem Thema, wenn Sie die Datenserververbindungseigenschaften für Single Sign-on (SSO) unter Verwendung von Kerberos konfigurieren.

Vorbereitende Schritte

Um eine Oracle-Datenserververbindung bei Verwendung von SSO mit Kerberos konfigurieren zu können, müssen Sie zunächst die Datei `bootstrap_wlp_`*`os_version`*`.xml` bearbeiten. Weitere Informationen finden Sie im Abschnitt „Bearbeiten der Datei bootstrap_wlp_*.xml für Oracle-Verbindungen mit Kerberos-SSO” auf Seite 223.

Vorgehensweise

1. Suchen Sie die Verbindung unter **Verwalten** > **Datenserververbindungen** oder erstellen Sie sie.
2. Klicken Sie auf die Datenserververbindung, um die zugehörigen Eigenschaften anzuzeigen.
3. Klicken Sie auf der Registerkarte **Einstellungen** unter **Authentifizierungsmethode** auf **Externen Namespace verwenden**und wählen Sie einen Active Directory-Namespace in der Liste aus.
4. Klicken Sie auf **Speichern**.
5. Klicken Sie neben **Verbindungsdetails** auf den Link **Bearbeiten**.
6. Geben Sie im Feld **Verbindungseigenschaften** den Wert `ibmcognos.authentication=java_krb5` ein, und geben Sie anschließend die datenbankspezifische Eigenschaft ein, falls erforderlich.

   Die folgende Tabelle enthält verschiedene Beispiele für Verbindungseigenschaften.

Datenserver	Verbindungseigenschaft
Teradata	ibmcognos.authentication=java_krb5;LOGMECH=KRB5;
SAP_HANA	ibmcognos.authentication=java_krb5;
Microsoft SQL Server	ibmcognos.authentication=java_krb5;authenticationScheme=JavaKerberos;

Wenn IBM Cognos Analytics auf einem Microsoft Windows-Computer installiert ist, ist die Angabe von `ibmcognos.authentication=java_krb5` für Microsoft SQL Server- und Teradata-Datenquellenverbindungen nicht erforderlich.

Anmerkung: Im traditionellen Cognos Administration wird das Feld **Verbindungseigenschaften** mit dem Namen **JDBC-Verbindungsparameter** bezeichnet.

7. Testen Sie die Datenserververbindung.

Bearbeiten der Datei `bootstrap_wlp_*.xml` für Oracle-Verbindungen mit Kerberos-SSO

Um Kerberos Single Sign-on (SSO) mit Oracle-Datenserververbindungen verwenden zu können, müssen Sie die Oracle-JVM-Argumente zur Datei IBM Cognos Analytics `bootstrap_wlp_os_version.xml` hinzufügen, bevor Sie die Verbindung in der Verwaltungsschnittstelle konfigurieren.

Diese Datei wird verwendet, wenn IBM Cognos Analytics als Service von IBM Cognos Configuration aus gestartet wird.

Vorgehensweise

1. Öffnen Sie die Datei `bootstrap_wlp_`*`os_version`*`.xml` im Verzeichnis *`install_location`*`/bin64` in einem Texteditor.

   Der vollständige Dateiname hängt vom Betriebssystem ab. Unter Linux lautet der Dateiname z. B. `bootstrap_wlp_linuxi38664.xml`, unter Windows `bootstrap_wlp_winx64.xml`.

   Tipp: Die Verwendung von doppelten Anführungszeichen in der Datei `bootstrap_wlp_linux38664.xml` verhindert, dass IBM Java gestartet werden kann, und führt dazu, dass der Startvorgang für Cognos blockiert wird und fehlschlägt.
2. Fügen Sie unter den Elementen <process>, <start>, <spawn> die folgenden Zeilen nach den speicherbezogenen <param>-Elementen hinzu:

```
<param>-Djava.security.krb5.conf=/etc/krb5.conf</param>
<param>-Dsun.security.krb5.debug=true</param>
<param>-Doracle.net.kerberos5_mutual_authentication=true</param>
<param>-Doracle.net.authentication_services="(KERBEROS5)"</param>
```

   Die Zeilen müssen genau wie im folgenden Ausschnitt aus der Datei `bootstrap_wlp_*.xml` angeordnet sein:

```
<process name="wlp">
    <start>
        <spawn sync="1" wait_time="5">

         <path>${java_home}/bin/java</path>

        <param condName="${ip_protocol}" condValue="IPv6">-Djava.net.preferIPv6Addres
ses=true</param>
        <param condName="${java_vendor}" condValue="IBM">-Xgcpolicy:gencon</param>
        <param condName="${java_vendor}" condValue="Sun">-XX:MaxNewSize=${dispatcherMaxMemo
ryBy2}m</param>
        <param condName="${java_vendor}" condValue="Sun">-XX:NewSize=${dispatcherMaxMemory
By3}m</param>
        <param condName1="${java_vendor}" condValue1="Sun" condName2="${java_version}" cond
Value2="1.8.0"
             condOp2="lt">-XX:MaxPermSize=128m</param>
```

```
        <param condName="${java_vendor}" condValue="Oracle">-XX:MaxNewSize=${dispatcherMaxMe
moryBy2}m</param>
        <param condName="${java_vendor}" condValue="Oracle">-XX:NewSize=${dispatcherMaxMemo
ryBy3}m</param>
        <param condName1="${java_vendor}" condValue1="Oracle" condName2="${java_version}"
condValue2="1.8.0"
             condOp2="lt">-XX:MaxPermSize=128m</param>
        <param condName="${java_vendor}" condValue="IBM">-Xmso512K</param>

         <!-- sso support -->
      <param>-Djava.security.krb5.conf=/etc/krb5.conf</param>
      <param>-Dsun.security.krb5.debug=true</param>
      <param>-Doracle.net.kerberos5_mutual_authentication=true</param>
      <param>-Doracle.net.authentication_services="(KERBEROS5)"</param>
      <!-- end sso support -->

        <param condName="${ip_protocol}" condValue="IPv4">-Djava.net.prefer
IPv4Stack=true</param>
```

3. Speichern Sie die Datei und schließen Sie sie.
4. Rufen Sie die Cognos Analytics-Verwaltungsschnittstelle auf, um mit der Konfiguration des Oracle-Datenservers für Kerberos-SSO fortzufahren. Weitere Informationen finden Sie im Abschnitt „Konfigurieren von Datenserververbindungen für Single Sign-on mit Kerberos” auf Seite 222.

Konfigurieren eines Repositorys für Protokollnachrichten

Das Business Intelligence Bus-Protokoll schließt die Verarbeitung von Protokollnachrichten ein. Protokollnachrichten sind ein wichtiges Diagnosetool zur Untersuchung des Verhaltens von IBM Cognos Analytics.

Neben Fehlernachrichten enthalten Protokollnachrichten Informationen zum Status von Komponenten und zu einer übergeordneten Ansicht wichtiger Ereignisse. Protokollnachrichten können beispielsweise Informationen zu Versuchen zum Starten und Stoppen von Services, zum Abschluss von Verarbeitungsanforderungen und zu Indikatoren für schwerwiegende Fehler enthalten. Prüfprotokolle, die in einer Protokolldatenbank verfügbar sind, stellen Informationen zur Benutzer-und Berichtsaktivität bereit.

Die IBM Cognos -Services auf jedem Computer senden Informationen zu Fehlern und Ereignissen an einen lokalen Protokollserver. Ein lokaler Protokollserver wird auf jedem IBM Cognos Analytics -Computer, der Content Manager-Komponenten oder Komponenten der Anwendungsebene enthält, in den Ordner *Installationsposition*/logs installiert. Da der Protokollserver einen anderen Port als die anderen IBM Cognos Analytics -Komponenten verwendet, verarbeitet er weiterhin Ereignisse, auch wenn andere Services auf dem lokalen Computer, wie z. B. der Dispatcher, inaktiviert sind.

Der folgende Workflow zeigt die Tasks an, die für die Vorbereitung der Protokollierung erforderlich sind.

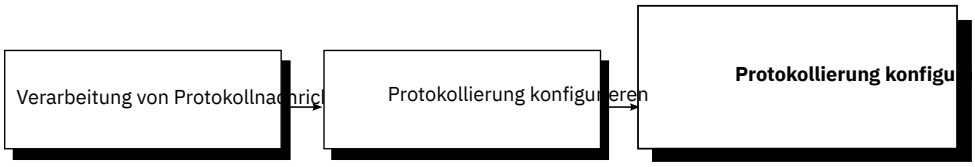


Abbildung 6. Der Workflow für die Implementierung der Protokollierung

- Bestimmen Sie bei der Planung die Protokollierungskonfiguration, die für Ihre Umgebung geeignet ist. Bewerten Sie beispielsweise verschiedene Protokollnachrichtenrepositorys, wie z. B. ferne Protokollserver und Protokolldateien, wie z. B. das UNIX -oder Linux -Systemprotokoll oder das Windows NT -Ereignisprotokoll, zusätzlich zur lokalen Protokolldatei. Sie können auch nur Prüfprotokollinformationen an eine Datenbank senden. Berücksichtigen Sie die Sicherheit, z. B. Methoden, die zum Schützen von Protokolldateien aus Systemfehlern und Benutzermanipulationen verfügbar sind.
- Definieren Sie während der Konfiguration die Starteigenschaften für die Protokollierung, wie z. B. Verbindungseinstellungen für Datenbanken. Sie müssen auch eine Protokollierungsdatenbank erstellen, wenn Sie Prüfprotokolle erfassen möchten. Wenn die Kommunikation zwischen einem lokalen Protokollserver und einem fernen Protokollserver gesichert werden muss, nehmen Sie die entsprechenden Konfigurationsänderungen auf beiden IBM Cognos Analytics -Computern vor. Sie können auch bestimmte Protokollierungsfunktionen aktivieren, wie z. B. die benutzerspezifische Protokollierung.

Informationen zum Konfigurieren der Protokollierung finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

- Geben Sie bei der Konfiguration der Protokollierung die Detaillierungsebene an, die protokolliert werden soll, um Nachrichten auf die Informationen zu fokussieren, die in Ihrer Organisation relevant sind. Prüfberichte können auch für die Verfolgung von Benutzer-und Berichtsaktivitäten eingerichtet werden.

  Informationen zum Einrichten der Protokollierung finden Sie im *IBM Cognos Analytics Administration and Security Guide*.

Informationen zur Verwendung von Protokollnachrichten zum Beheben von Problemen und zum Beheben von Protokollierungsfehlern finden Sie im *Handbuch zur Fehlerbehebung für IBM Cognos Analytics*.

Richtlinien zum Erstellen einer Protokolldatenbank

Sie können eine Datenbank für die Speicherung von Protokollnachrichten erstellen. Die Erstellung einer Protokolldatenbank umfasst die folgenden Schritte:

- Erstellen Sie eine Protokolldatenbank.

  Verwenden Sie für IBM Db2, Oracle oder Microsoft SQL Server dieselbe Vorgehensweise wie bei der Erstellung der Content-Store-Datenbank. Gehen Sie anhand der Anweisungen unter „Richtlinien zum Erstellen des Content Store” auf Seite 7 vor.

  Anmerkung: Wenn Sie Db2 verwenden, können Sie kein Script generieren, um die Benachrichtigungsdatenbank auf dieselbe Weise zu generieren wie den Content Store.

  Befolgen Sie für Db2 unter z/OS die Anweisungen im Abschnitt „Empfohlene Einstellungen für die Erstellung einer Protokolldatenbank für Db2 unter z/OS” auf Seite 225.
- Richten Sie die Datenbankverbindung ein.

  Gehen Sie anhand der Anweisungen unter „Datenbankverbindungen für die Protokolldatenbank” auf Seite 227 vor.
- Geben Sie das Repository für Protokollnachrichten an.

  Gehen Sie anhand der Anweisungen unter „Repositorys für Protokollnachrichten” auf Seite 228 vor.

Empfohlene Einstellungen für die Erstellung einer Protokolldatenbank für Db2 unter z/OS

Die Datenbank muss die angegebenen Konfigurationseinstellungen aufweisen.

Verwenden Sie die folgende Prüfliste, um die Protokolldatenbank für Db2 unter z/OS einzurichten.

__ • Melden Sie sich am z/OS-System als Benutzer an, der über Administratorberechtigung für Db2 unter z/OS verfügt.

__ • Erstellen Sie eine Datenbankinstanz, eine Speichergruppe und ein Benutzerkonto für den Content Store. IBM Cognos verwendet die Berechtigungsnachweise des Benutzerkontos, um mit dem Datenbankserver zu kommunizieren.

__ • Stellen Sie sicher, dass Sie der Datenbankinstanz einen Pufferpool mit einer Seitengröße von 8 KB zuordnen.

__ • Für eine Protokolldatenbank für Db2 unter z/OS müssen Administratoren ein Tabellenbereichsscript zur Erstellung von Tabellenbereichen ausführen, in denen große Objekte und andere Daten für die Protokolldatenbank aufbewahrt werden. Dann müssen sie die Benutzerberechtigungen für die Tabelle gewähren. Weitere Informationen zur Ausführung des Tabellenbereichsscripts finden Sie in „Erstellen von Tabellenbereichen für eine Protokolldatenbank für Db2 on z/OS ” auf Seite 225.

Erstellen von Tabellenbereichen für eine Protokolldatenbank für Db2 on z/OS

Wenn Sie IBM Db2 unter z/OS verwenden, muss ein Datenbankadministrator ein Script ausführen, um die Tabellenbereiche zu erstellen, die für die Protokolldatenbank erforderlich sind. Dieses Script muss

angepasst werden, d. h., die Platzhalterparameter sind durch solche zu ersetzen, die für Ihre Umgebung geeignet sind.

Stellen Sie sicher, dass Sie die Namenskonventionen für Db2 unter z/OS verwenden. Beispielsweise müssen alle Parameternamen mit einem Buchstaben anfangen und dürfen maximal 6 Zeichen lang sein. Weitere Informationen finden Sie im Db2 Knowledge Center.

Vorgehensweise

1. Stellen Sie als Benutzer mit Berechtigungen zum Erstellen und Löschen von Tabellenbereichen sowie zum Ausführen von SQL-Anweisungen eine Verbindung mit der Datenbank her.
2. Wechseln Sie in das Verzeichnis *installationsposition*/configuration/schemas/logging/db2zos.
3. Öffnen Sie die Scriptdatei LS_tablespace_db2z0S.sql und ersetzen Sie die generischen Parameter durch die für Ihre Umgebung geeigneten Parameter mithilfe der folgenden Tabelle.

Tabelle 26. Parameternamen und Beschreibungen von Tabellenbereichen für eine Protokolldatenbank für Db2 unter z/OS

Parametername	**Beschreibung**
IPFSCRIPT_DATABASE	Der Name der Protokolldatenbank.
IPFSCRIPT_STOGROUP	Der Name der Speichergruppe.
IPFSCRIPT_TABLESPACE	Der Name des Tabellenbereichs, in dem die Basistabellen in der Protokolldatenbank enthalten sind. Dieser Tabellenbereich enthält keine Hilfstabellen.
IPFSCRIPT_LS_ID	Die Instanzkennung für die Audit-Datenbank. Dieser Wert darf maximal zwei Zeichen lang sein.
IPFSCRIPT_BP	Der Name des 8-KB-Pufferpools, der für normale Objekte reserviert ist.
IPFSCRIPT_USERNAME	Der Name des Benutzerkontos, das auf die Protokolldatenbank zugreift.

   Die Tabelle führt auch Parameter auf, die zwar noch nicht im Script enthalten sind, aber möglicherweise noch hinzugefügt werden.
4. Speichern Sie das Script und führen Sie es aus.
5. Gewähren Sie die IBM Cognos-Benutzerrechte den Tabellenbereichen, die beim Ausführen der Scriptdatei erstellt wurden:
   - Öffnen Sie die Scriptdatei LS_rightsGrant_db2z0S.sql.
   - Ersetzen Sie die Parameterwerte durch Werte, die für Ihre Umgebung geeignet sind.

     Tipp: Stellen Sie sicher, dass Sie dieselben Werte wie bei der Erstellung der Pufferpools und des Benutzerkontos verwenden.
   - Speichern Sie das Script LS_rightsGrant_db2z0S.sql und führen Sie es aus.

Ergebnisse

Die Protokolldatenbank wurde erstellt.

Datenbankverbindungen für die Protokolldatenbank

Nach dem Erstellen einer Datenbank für Auditprotokolle müssen Sie zusätzliche Schritte zum Einrichten des Datenbankclients ausführen, falls Sie Oracle, IBM Db2 oder Informix Dynamic Server als Datenbankserver verwenden.

In einer verteilten Umgebung können vom lokalen Protokollserver auf einem Computer mit Komponenten der Anwendungsebene Protokollnachrichten an einen einzelnen fernen Protokollserver gesendet werden, der diese dann an die Protokolldatenbank sendet. Bei Oracle und Db2 sind der entsprechende JDBC-Treiber und/oder die entsprechende Datenbank-Client-Software nur auf dem Computer mit den Komponenten der Anwendungsebene mit dem fernen Protokollserver erforderlich, der die Verbindung zur Protokolldatenbank herstellt.

Microsoft SQL Server

Wenn Sie mit einer Microsoft SQL Server-Datenbank arbeiten, wird die Datei `JSQLConnect.jar` standardmäßig am richtigen Ort installiert. Zusätzlich müssen Sie lediglich sicherstellen, dass der Microsoft SQL Server eine TCP/IP-Verbindung verwendet.

Einrichten einer Datenbankverbindung für eine IBM Db2-Protokolldatenbank

Sie müssen auf allen Computern mit Komponenten der Anwendungsebene und Verbindung zur Protokolldatenbank die Datenbank-Client-Software und den JDBC-Treiber einrichten. Sofern Sie für die Protokollnachrichten nicht denselben Datenbanktyp wie für den Content Store verwenden, müssen Sie den JDBC-Treiber auf dem Content Manager-Computer einrichten.

Als Treiberversion muss mindestens JCC 3.7 aus Linux oder UNIX oder Microsoft Windows Version 9.1 Fixpack oder JCC 3.42 aus Linux, UNIX oder Microsoft Windows Version 9.5 Fixpack 2 verwendet werden.

Vorgehensweise

Kopieren Sie die folgenden Dateien vom Verzeichnis *DB2-Installation*`\sqllib\java` in das Verzeichnis *Installationsposition*`\drivers`:

- Die universelle Treiberdatei `db2jcc4.jar`
- Die Lizenzdatei:

  Für Db2 unter Linux, UNIX oder Windows verwenden Sie die Datei `db2jcc_license_cu.jar`.

  Für Db2 unter z/OS verwenden Sie die Datei `db2jcc_license_cisuz.jar`.

  Wenn Sie eine Verbindung mit Db2 unter z/OS herstellen, verwenden Sie die Treiberversion aus Linux, UNIX oder Windows Version 9.1 Fixpack 5 oder Version 9.5 Fixpack 2.

  Tipp: Führen Sie zur Überprüfung der Treiberversion den folgenden Befehl aus:

  ```
  java -cp Pfad\db2jcc4.jar com.ibm.db2.jcc.DB2Jcc -version
  ```

Einrichten einer Datenbankverbindung für eine Oracle-Protokolldatenbank

Sie müssen auf allen Computern mit Komponenten der Anwendungsebene und Verbindung zur Protokolldatenbank den JDBC-Treiber einrichten. Sofern Sie für die Protokollnachrichten nicht denselben Datenbanktyp wie für den Content Store verwenden, müssen Sie den JDBC-Treiber auch auf dem Content Manager-Computer einrichten.

Vorgehensweise

1. Wechseln Sie auf dem Computer, auf dem der Oracle-Client installiert ist, in das Verzeichnis *ORACLE_HOME*`/jdbc/lib`.

2. Kopieren Sie die korrekte Bibliotheksdatei für Ihre Version des Oracle-Clients in das Verzeichnis *Installationsposition*\drivers auf dem Computer, auf dem Content Manager installiert ist und auf dem Benachrichtigungen an eine Oracle-Datenbank gesendet werden.

   Wenn Sie mit Oracle Version 12c Release 2 arbeiten, müssen Sie über die Datei 'ojdbc8.jar' verfügen.

   Wenn Sie mit Oracle Version 12c Release 1 arbeiten, müssen Sie über die Datei 'ojdbc7.jar' verfügen.

   Wenn Sie mit Oracle Version 11g Release 2 arbeiten, müssen Sie über die Datei 'ojdbc6.jar' verfügen.

   Anmerkung: Weitere Informationen finden Sie in den FAQ zu Oracle JDBC.

   Die Dateien sind bei Installation eines Oracle-Clients oder -Servers verfügbar oder können von der Technologie-Website von Oracle heruntergeladen werden.

Einrichten einer Datenbankverbindung für eine Informix-Protokolldatenbank

Sie müssen auf allen Computern mit Komponenten der Anwendungsebene und Verbindung zur Protokolldatenbank den JDBC-Treiber einrichten. Sofern Sie für die Protokollnachrichten nicht denselben Datenbanktyp wie für den Content Store verwenden, müssen Sie den JDBC-Treiber auch auf dem Content Manager-Computer einrichten.

Vorgehensweise

1. Wechseln Sie auf dem Computer, auf dem Informix installiert ist, in das Verzeichnis *Informix_Position*/sqllib/java.
2. Kopieren Sie die folgenden Dateien in das Verzeichnis *Installationsposition*\drivers auf jedem Computer, auf dem Content Manager installiert ist.
   - Die universelle Treiberdatei db2jcc4.jar
   - Die Lizenzdatei db2jcc4_license_cisuz.jar

Repositorys für Protokollnachrichten

Ein lokaler Protokollserver wird automatisch installiert, wenn Sie Content Manager oder die Komponenten der Anwendungsebene installieren. Für die Protokollnachrichten vom lokalen Protokollserver können ein oder mehrere Repositorys angegeben werden.

Senden von Protokollnachrichten an fernen Protokollserver

In einer verteilten Installation können Sie die Protokollserver auf den einzelnen IBM Cognos-Computern so konfigurieren, dass sie Protokollnachrichten an einen einzelnen fernen Protokollserver senden, der als allgemeiner Protokollserver dient. Anschließend können Sie den allgemeinen Protokollserver so konfigurieren, dass er die Protokollnachrichten an eine lokale Datei oder eine Datenbank auf demselben oder einem anderem Computer sendet.

Wenn der ferne Protokollserver nicht mehr verfügbar ist, werden Protokollnachrichten an Wiederherstellungsdateien auf dem lokalen Computer umgeleitet, die im Verzeichnis *installationsposition*/logs/recovery/remote gespeichert sind. Die Dateinamen dieser Wiederherstellungsdateien weisen Zeitmarkeninformationen auf. Die Dateien können nicht wie normale Protokolldateien gelesen werden. Wenn der ferne Protokollserver verfügbar ist, werden alle Protokollinformationen durch einen automatischen Wiederherstellungsprozess auf den fernen Protokollserver verschoben und die lokalen Protokolldateien gelöscht.

Speichern von Protokollnachrichten in einer Datei

Der Protokollserver ist standardmäßig so konfiguriert, dass Protokollnachrichten an die Datei *installationsposition*/logs/cogaudit.log gesendet werden. Wenn die Standardprotokolldatei beim Starten des IBM Cognos-Service nicht vorhanden ist, wird sie automatisch erstellt.

Sie können die Konfiguration aber auch dahingehend ändern, dass die Protokollnachrichten an eine andere Datei gesendet werden. Wenn Sie eine andere Protokolldatei konfigurieren, versucht IBM Cognos beim Start, automatisch diese Datei zusätzlich zu der Standardprotokolldatei zu erstellen. Wenn die Position der konfigurierten Protokolldatei nicht mit dem Verzeichnis *installationsposition*/logs übereinstimmt, müssen Sie vor dem Starten des IBM Cognos-Service sicherstellen, dass der Pfad zu der Protokolldatei auch vorhanden ist. Wenn Sie beispielsweise den Protokollserver so konfigurieren, dass Nachrichten an die Datei "/usr/lpp/logfiles/cognos.log" gesendet werden, versucht IBM Cognos, die Datei cognos.log im Ordner /usr/lpp/logfiles automatisch zu erstellen. Wenn es diesen Ordner nicht gibt, erstellt IBM Cognos die Datei cognos.log nicht und daher können keine Protokollnachrichten in ihr aufgezeichnet werden. Beachten Sie, dass diese Protokollnachrichten auch nicht in der Standardprotokolldatei erfasst werden. Obwohl IBM Cognos automatisch die Standardprotokolldatei erstellt, auch wenn eine andere Protokolldatei konfiguriert wurde, wird diese nicht als Sicherungskopie verwendet.

Speichern von Protokollnachrichten in einer Datenbank

Der Protokollserver kann auch Auditprotokolle an eine Datenbank auf demselben oder einem anderen Computer senden. Auditprotokolle enthalten Informationen zu Benutzer- und Berichtsaktivitäten.

Für die Protokolldatenbank gelten dieselben Anforderungen hinsichtlich Konfiguration und Benutzerkonten wie für die Content Store-Datenbank. Wenn Sie die IBM Cognos-Komponenten so konfiguriert haben, dass Nachrichten an eine Protokolldatenbank gesendet werden, und den IBM Cognos-Service neu starten, erstellen die IBM Cognos-Komponenten die erforderlichen Tabellen und Tabellenfelder. Sie können die Verbindung zur Protokolldatenbank testen, bevor Sie den IBM Cognos-Service neu starten.

Festlegen des Repositorys für Protokollnachrichten für IBM Db2 on UNIX, Linux oder Windows

Sie können einen Repository-Typ für die Protokollnachrichten konfigurieren und dann die Eigenschaften für das spezifische Repository konfigurieren. Sie können auch mehrere Repositorys für Protokollnachrichten konfigurieren.

Vorbereitende Schritte

Stellen Sie vor der Angabe einer Datenbank als Repository sicher, dass Sie folgende Aufgaben ausgeführt haben:

__ • Sie haben die Protokolldatenbank erstellt.

__ • Der Datenbankclient ist eingerichtet.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Computer, auf dem Content Manager oder die Komponenten der Anwendungsebene installiert sind.
2. Klicken Sie im Fenster **Explorer** unter **Umgebung** auf **Protokollierung**.
3. Legen Sie mithilfe der folgenden Tabelle im Fenster **Eigenschaften** die Eigenschaften für den Protokollserver fest.

Tabelle 27. Eigenschaften des Protokollservers	
Aufgabe	**Aktion**
Verwendung von TCP zwischen IBM Cognos-Komponenten auf einem Computer und seinem lokalen Protokollserver	Legen Sie die Eigenschaft **TCP aktivieren** auf **Wahr** fest. Mit UDP ist die Kommunikation schneller und die Gefahr von Verbindungsunterbrechungen geringer als mit TCP. Insgesamt ist aber auch bei einer lokalen TCP-Verbindung die Gefahr von Unterbrechungen gering. Für die Kommunikation zwischen einem lokalen Protokollserver und einem fernen Protokollserver wird grundsätzlich TCP verwendet.
Ändern der Anzahl von Threads, die auf dem lokalen Protokollserver verfügbar sind	Geben Sie für die Eigenschaft **Worker Threads des lokalen Protokollservers** den gewünschten Wert ein. Behalten Sie den Standardwert "10" bei. Der gültige Bereich liegt zwischen 1 und 20. Bei einem sehr hohen Aufkommen von Protokollnachrichten kann es aus Leistungsgründen allerdings sinnvoll sein, weitere Threads zuzuweisen.

4. Klicken Sie im Fenster **Explorer** unter **Umgebung** mit der rechten Maustaste auf **Protokollierung** und klicken Sie dann auf **Neue Ressource** > **Ziel**.
5. Geben Sie in das Feld **Name** einen Namen für das Repository ein.
6. Geben Sie in der Liste **Typ** den Repository-Typ an und klicken Sie auf **OK**.
7. Wenn es sich bei dem Repository um eine Datei handelt, geben Sie im Fenster **Eigenschaften** die entsprechenden Werte für die obligatorischen und optionalen Eigenschaften ein.
8. Wenn es sich bei dem Repository um einen fernen Protokollserver handelt, geben Sie im Fenster **Eigenschaften** die entsprechenden Werte für die obligatorischen und optionalen Eigenschaften ein.

   Wenn die Eigenschaft **Interner Dispatcher-URI** des Repository-Computers für die Verwendung von SSL konfiguriert ist, setzen Sie im Fenster **Eigenschaften** die Eigenschaft **SSL aktivieren** auf **Wahr**.

   Beim anschließenden Konfigurieren des fernen Protokollservers müssen Sie das Repository für die Protokollnachrichten angeben.
9. Wenn es sich bei dem Repository um eine Datenbank handelt, geben Sie im Fenster **Explorer** unter **Protokollierung** den Datenbanktyp und die dazugehörigen Eigenschaften an. Gehen Sie dabei folgendermaßen vor:
   - Klicken Sie mit der rechten Maustaste auf den Datenbanknamen und klicken Sie dann auf **Neue Ressource** > **Datenbank**.
   - Geben Sie in das Feld **Name** einen Namen für das Repository ein.
   - Geben Sie in der Liste **Typ** den Datenbanktyp an und klicken Sie auf **OK**.
   - Geben Sie im Fenster **Eigenschaften** geeignete Werte für die obligatorischen und die optionalen Eigenschaften ein.

     Wenn Sie eine Microsoft SQL Server-Datenbank verwenden, können Sie als Wert für die Eigenschaft **Datenbankserver und Portnummer oder Instanzname** eine Portnummer (z. B. 1433) oder eine benannte Instanz verwenden. Geben Sie die Portnummer an, wenn Sie keine Standardports verwenden. Geben Sie den Instanznamen an, wenn mehrere Instanzen von Microsoft SQL Server vorhanden sind.

     Zum Verbinden mit einer benannten Instanz müssen Sie den Namen der Instanz als JDBC-URL-Eigenschaft oder als Datenquelleneigenschaft angeben. Sie können beispielsweise **localhost\ins-**

tance1 eingeben. Wenn keine Instanznameneigenschaft angegeben wurde, wird eine Verbindung zur Standardinstanz hergestellt.

Beachten Sie, dass die für die benannte Instanz angegebenen Eigenschaften zusammen mit der Benutzer-ID, dem Kennwort und dem Datenbanknamen verwendet werden, um eine JDBC-URL zu erstellen. Beispiel:

jdbc:JSQLConnect://localhost\\instance1/user=sa/*weitere Eigenschaften nach Bedarf*

- Testen Sie die Verbindung zu der neuen Datenbank. Klicken Sie im Fenster **Explorer** unter **Umgebung** mit der rechten Maustaste auf **Protokollierung** und klicken Sie auf **Test**.

  Die IBM Cognos-Komponenten stellen eine Verbindung zur Datenbank her. Wenn mehrere Datenbanken für das Protokollieren von Nachrichten konfiguriert wurden, werden alle Datenbanken von den IBM Cognos-Komponenten getestet.

10. Wiederholen Sie die Schritte 5 bis 10 für jedes Repository, an das der Protokollserver Nachrichten senden soll.
11. Klicken Sie im Menü **Datei** auf **Speichern**.
12. Klicken Sie im Fenster **Explorer** auf **IBM Cognos-Services** > **IBM Cognos**.
13. Klicken Sie im Menü **Datei** auf **Neu starten**.

    Wenn Sie eine Datenbank als Repository ausgewählt haben, erstellen die IBM Cognos-Komponenten die erforderlichen Tabellen und Felder in der von Ihnen erstellten Datenbank.

Ergebnisse

Wenn als Repository ein ferner Protokollserver festgelegt wurde, konfigurieren Sie den Protokollserver und starten Sie ihn. Starten Sie anschließend den IBM Cognos-Service auf dem lokalen Computer neu.

Wenn es sich bei dem Repository um eine Datenbank handelte, können Sie die IBM Cognos-Komponenten zum Ausführen von Protokollberichten von der Datenbank aus verwenden.

Sie haben außerdem die Möglichkeit, eine Protokollebene festzulegen, wodurch die Detailmenge und der Typ der Nachrichten festgelegt wird, die an eine Protokolldatei oder Datenbank gesendet werden. Anweisungen finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Festlegen des Repositorys für Protokollnachrichten für IBM Db2 unter z/OS

Sie können einen Repository-Typ für die Protokollnachrichten konfigurieren und dann die Eigenschaften für das spezifische Repository konfigurieren. Sie können auch mehrere Repositorys für Protokollnachrichten konfigurieren.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Computer, auf dem Content Manager oder die Komponenten der Anwendungsebene installiert sind.
2. Klicken Sie im Fenster **Explorer** unter **Umgebung** auf **Protokollierung**.
3. Legen Sie mithilfe der folgenden Tabelle im Fenster **Eigenschaften** die Eigenschaften für den Protokollserver fest.

Tabelle 28. Eigenschaften des Protokollservers	
Aufgabe	**Aktion**
Verwendung von TCP zwischen IBM Cognos-Komponenten auf einem Computer und seinem lokalen Protokollserver	Legen Sie die Eigenschaft **TCP aktivieren** auf **Wahr** fest. Mit UDP ist die Kommunikation schneller und die Gefahr von Verbindungsunterbrechungen geringer als mit TCP. Für die Kommunikation zwischen einem lokalen Protokollserver und einem fernen Protokollserver wird TCP verwendet.
Ändern der Anzahl von Threads, die auf dem lokalen Protokollserver verfügbar sind	Geben Sie für die Eigenschaft **Worker Threads des lokalen Protokollservers** den gewünschten Wert ein. Behalten Sie den Standardwert "10" bei. Der gültige Bereich liegt zwischen 1 und 20. Bei einem sehr hohen Aufkommen von Protokollnachrichten kann es aus Leistungsgründen allerdings sinnvoll sein, weitere Threads zuzuweisen.

4. Klicken Sie im Fenster **Explorer** unter **Umgebung** mit der rechten Maustaste auf **Protokollierung** und klicken Sie dann auf **Neue Ressource** > **Ziel**.
5. Geben Sie in das Feld **Name** einen Namen für das Repository ein.
6. Klicken Sie in der Liste **Typ** auf **Datenbank** und anschließend auf **OK**.
7. Klicken Sie im Fenster **Explorer** unter **Protokollierung** mit der rechten Maustaste auf den Datenbanknamen. Klicken Sie dann auf **Neue Ressource** > **Datenbank**.
8. Geben Sie in das Feld **Name** einen Namen für das Repository ein.
9. Klicken Sie in der Liste **Typ** auf **DB2-Datenbank** und anschließend auf **OK**.
10. Geben Sie im Fenster **Eigenschaften** Werte für die Felder **Datenbankserver und Portnummer**, **Benutzer-ID und Kennwort** und **Datenbankname** (z/OS) ein.

    Stellen Sie sicher, dass die Benutzer-ID dem Wert entspricht, den Sie in der Scriptdatei LS_tablespace_db2zOS.sql für den Parameter IPFSCRIPT_USERNAME festgelegt haben „Erstellen von Tabellenbereichen für eine Protokolldatenbank für Db2 on z/OS ” auf Seite 225.
11. Klicken Sie im Fenster **Explorer** auf **Lokale Konfiguration**.
12. Klicken Sie im Fenster **Eigenschaften** neben **Erweiterte Eigenschaften** in das Feld **Wert** und klicken Sie dann auf das Bearbeitungssymbol  .
13. Klicken Sie auf **Hinzufügen** und fügen Sie die Namen und Werte der Konfigurationsparameter aus der folgenden Tabelle hinzu:

Tabelle 29. Namen und Werte der Konfigurationsparameter	
Parametername	**Wert**
IPFSCRIPT_CREATE_IN	Die Speicherpositionn der Basistabellen Beispiel: databaseName.baseTablespaceName
IPFSCRIPT_STOGROUP	Der Name der Speichergruppe.
IPFSCRIPT_DATABASE	Der Name der Protokolldatenbank.

Tabelle 29. Namen und Werte der Konfigurationsparameter (Forts.)	
Parametername	**Wert**
IPFSCRIPT_LS_ID	Die Instanzkennung für die Audit-Datenbank. Dieser Wert darf maximal zwei Zeichen lang sein.

14. Klicken Sie im Menü **Datei** auf **Speichern**.
15. Testen Sie die Verbindung zu der neuen Datenbank. Klicken Sie im Fenster **Explorer** unter **Umgebung** mit der rechten Maustaste auf **Protokollierung** und klicken Sie auf **Test**.

    Die IBM Cognos-Komponenten stellen eine Verbindung zur Datenbank her. Wenn mehrere Datenbanken für das Protokollieren von Nachrichten konfiguriert wurden, werden alle Datenbanken von den IBM Cognos-Komponenten getestet.

Festlegen des Repositorys für Protokollnachrichten für Informix

Sie können einen Repository-Typ für die Protokollnachrichten konfigurieren und dann die Eigenschaften für das spezifische Repository konfigurieren. Sie können auch mehrere Repositorys für Protokollnachrichten konfigurieren.

Vorgehensweise

1. Klicken Sie im Fenster **Explorer** unter **Umgebung** auf **Protokollierung**.
2. Legen Sie mithilfe der folgenden Tabelle im Fenster **Eigenschaften** die Eigenschaften für den Protokollserver fest.

Tabelle 30. Eigenschaften des Protokollservers	
Aufgabe	**Aktion**
Verwendung von TCP zwischen IBM Cognos-Komponenten auf einem Computer und seinem lokalen Protokollserver	Legen Sie die Eigenschaft **TCP aktivieren** auf **Wahr** fest. Mit UDP ist die Kommunikation schneller und die Gefahr von Verbindungsunterbrechungen geringer als mit TCP. Für die Kommunikation zwischen einem lokalen Protokollserver und einem fernen Protokollserver wird TCP verwendet.
Ändern der Anzahl von Threads, die auf dem lokalen Protokollserver verfügbar sind	Geben Sie für die Eigenschaft **Worker Threads des lokalen Protokollservers** den gewünschten Wert ein. Behalten Sie den Standardwert "10" bei. Der gültige Bereich liegt zwischen 1 und 20. Bei einem sehr hohen Aufkommen von Protokollnachrichten kann es aus Leistungsgründen allerdings sinnvoll sein, weitere Threads zuzuweisen.

3. Klicken Sie im Fenster **Explorer** unter **Umgebung** mit der rechten Maustaste auf **Protokollierung** und klicken Sie dann auf **Neue Ressource** > **Ziel**.
4. Geben Sie in das Feld **Name** einen Namen für das Repository ein.
5. Klicken Sie in der Liste **Typ** auf **Datenbank** und anschließend auf **OK**.
6. Klicken Sie im Fenster **Explorer** unter **Protokollierung** mit der rechten Maustaste auf den Datenbanknamen. Klicken Sie dann auf **Neue Ressource** > **Datenbank**.
7. Geben Sie in das Feld **Name** einen Namen für das Repository ein.
8. Klicken Sie in der Liste **Typ** auf **Informix Dynamic Server-Datenbank** und anschließend auf **OK**.

9. Geben Sie im Fenster **Eigenschaften** die Werte für die Felder **Datenbankserver und Portnummer**, **Benutzer-ID und Kennwort** und **Datenbankname** ein.
10. Wenn Sie über mehrere Instanzen einer Informix-Protokolldatenbank verfügen, erstellen Sie die erweiterte Eigenschaft IPFSCRIPTIDX und geben Sie das Konto an, unter dem die Instanz ausgeführt wird:
    - Klicken Sie im Fenster **Explorer** auf **Lokale Konfiguration**.
    - Klicken Sie im Fenster **Eigenschaften** auf die Spalte **Wert** für **Erweiterte Eigenschaften** und anschließend auf das Bearbeitungssymbol  .
    - Klicken Sie im Dialogfeld **Wert - Erweiterte Eigenschaften** auf **Hinzufügen**.
    - Geben Sie in der Spalte **Name** den Wert **IPFSCRIPTIDX** ein.
    - Geben Sie in der Spalte **Wert** die Benutzer-ID des Kontos ein, unter dem die Instanz der Protokolldatenbank ausgeführt wird.

      Verwenden Sie für jede Instanz der Informix-Protokolldatenbank ein anderes Benutzerkonto.
    - Wiederholen Sie die Aktion für jede Instanz von IBM Cognos Configuration, die eine Instanz einer Informix-Protokolldatenbank verwendet.
11. Klicken Sie im Menü **Datei** auf **Speichern**.
12. Testen Sie die Verbindung zu der neuen Datenbank. Klicken Sie im Fenster **Explorer** unter **Umgebung** mit der rechten Maustaste auf **Protokollierung** und klicken Sie auf **Test**.

    Die IBM Cognos-Komponenten stellen eine Verbindung zur Datenbank her. Wenn mehrere Datenbanken für das Protokollieren von Nachrichten konfiguriert wurden, werden alle Datenbanken von den IBM Cognos-Komponenten getestet.

Aktivieren der benutzerspezifischen Protokollierung

Beim Diagnostizieren von Problemen können Sie vorübergehend festlegen, dass die Protokollierung anstatt für alle Benutzer gleichzeitig nur für einen oder mehrere bestimmte Benutzer erfolgen soll. Nach Abschluss der Diagnose können Sie mit der normalen Protokollierung fortfahren. Zum Aktivieren der benutzerspezifischen Protokollierung konfigurieren Sie mithilfe von IBM Cognos Configuration Verbindungsinformationen für Java Management Extensions (JMX). JMX ist eine Technologie, die Tools zum Verwalten und Überwachen von Anwendungen und serviceorientierten Netzen bereitstellt. Dann konfigurieren Sie die JMX-Verbindungsinformationen in einer Datei für die Bereitstellungseigenschaften.

Nach dem Aktivieren der benutzerspezifischen Protokollierung für IBM Cognos-Komponenten aktivieren Sie mithilfe des Remoteprozess-Service für JMX die Protokollierung für einen bestimmten Benutzer. Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit* im Abschnitt über die Verwendung der Protokollierung zum Diagnostizieren eines Problems für einen bestimmten Benutzer.

Sie müssen Oracle Java SE Development Kit oder Java Software Development Kit für IBM installieren, um die benutzerspezifische Protokollierung aktivieren zu können.

Konfigurieren von JMX-Verbindungsinformationen mithilfe von IBM Cognos Configuration

Konfigurieren Sie die JMX-Verbindungsinformationen (JMX = Java Management Extensions) in IBM Cognos Configuration, indem Sie einen Cookiewert angeben und dann den Port und die Berechtigungsnachweise für JMX festlegen.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Computern, auf dem Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Konfigurieren Sie im Fenster **Eigenschaften** unter **Dispatcher-Einstellungen** die JMX-Eigenschaften:

- Geben Sie unter **Externer JMX-Port** eine verfügbare Portnummer ein.
- Klicken Sie unter **Externe JMX-Berechtigungsnachweis** in der Spalte **Wert** auf das Bearbeitungssymbol  , geben Sie eine Benutzer-ID und ein Kennwort ein und klicken Sie dann auf **OK**.

  Benutzer-ID und Kennwort sorgen dafür, dass nur autorisierte Benutzer über den Port, der unter **Externer JMX-Port** festgelegt wurde, eine Verbindung zu der Java-Umgebung herstellen können, um die zu protokollierenden Benutzer festzulegen.

4. Speichern Sie die Konfiguration.

Konfigurieren von JMX-Verbindungsinformationen in einer Datei für die Bereitstellungseigenschaften

Geben Sie den JMX-Port in der Datei für die Bereitstellungseigenschaften (p2pd) an, damit die JMX-Einstellungen (JMX = Java Management Extensions) auf Ihrem Anwendungsserver unterstützt werden.

Vorgehensweise

1. Öffnen Sie im Texteditor die Datei p2pd.deploy_defaults.properties, die im Verzeichnis *installationsposition*/webapps/p2pd/WEB-INF gespeichert ist.
2. Kommentieren Sie die Zeile `rmiregistryport` aus und legen Sie den Wert auf den **externen JMX-Port** fest, den Sie in IBM Cognos Configuration konfiguriert haben.
3. Speichern Sie die Datei p2pd.deploy_defaults.properties.
4. Starten Sie die Services für IBM Cognos neu.

Ergebnisse

IBM Cognos unterstützt jetzt die Protokollierung für einen oder mehrere bestimmte Benutzer. Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit* im Abschnitt über die Verwendung der Protokollierung zum Diagnostizieren eines Problems für einen bestimmten Benutzer.

Ändern globaler Einstellungen

Die IBM Cognos-Komponenten stellen standardmäßig sicher, dass für alle Ländereinstellungen, die aus unterschiedlichen Quellen stammen und in verschiedenen Formaten vorliegen können, ein normalisiertes Format verwendet wird. Dies bedeutet, dass alle erweiterten Ländereinstellungen den Einstellungen für eine Sprache und einen regionalen Code entsprechen. Jeder Computer verfügt über eine standardmäßige Systemländereinstellung und eine Benutzerländereinstellung pro Benutzer. Die Benutzerländereinstellungen müssen nicht mit der standardmäßigen Systemländereinstellung übereinstimmen. Wenn Sie globale Einstellungen auf einem Content Manager-Computer ändern, müssen die gleichen Änderungen auch auf den anderen Content Manager-Computern vorgenommen werden.

Sie ändern die globalen Einstellungen aus folgenden Gründen:

- Zum Anpassen der Sprachunterstützung für die Benutzeroberfläche
- Zum Anpassen der Währungsunterstützung
- Zum Anpassen der Unterstützung von Inhaltsländereinstellungen
- Zum Zuordnen der in der Benutzeroberfläche des Produkts verwendeten Sprache
- Zum Zuordnen von Ländereinstellungen für Inhalte
- Zum Hinzufügen von Schriftarten zu Ihrer IBM Cognos-Umgebung
- Zum Anpassen der Standardzeitzone
- Zum Ändern der Codierung für E-Mail-Nachrichten
- Zum Anpassen von Cookieeinstellungen

Anpassen der Sprachunterstützung an die Benutzeroberfläche

Verwenden Sie die Tabelle PRODUKT-GEBIETSSCHEMA, um die Sprachunterstützung für die Benutzeroberfläche hinzuzufügen oder zu entfernen. Wenn Sie beispielsweise keine englische Benutzeroberfläche benötigen, können Sie diese Sprache aus der Liste löschen.

Eine Änderung der Benutzeroberflächensprache des Produkts hat keinerlei Auswirkungen auf die Daten.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie die entsprechenden Schriftarten installieren, um Unterstützung für die gewünschten Zeichensätze und Währungssymbole bereitzustellen. Damit japanische und koreanische Währungssymbole korrekt angezeigt werden, müssen Sie die zusätzlichen Schriftarten vom Supplementary Language Documentation-Datenträger installieren.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf jedem Content Manager-Computer.
2. Klicken Sie im Menü **Aktionen** auf **Globale Konfiguration bearbeiten**.
3. Klicken Sie auf die Registerkarte **Produktländereinstellungen**.

   Alle unterstützten Ländereinstellungen werden angezeigt.
4. Klicken Sie auf **Hinzufügen**.

   Tipp: Aktivieren Sie zum Entfernen der Unterstützung das Kontrollkästchen neben **Unterstützte Ländereinstellung** und klicken Sie anschließend auf **Entfernen**.
5. Geben Sie in die zweite Spalte die Sprachkomponente der Ländereinstellung ein.
6. Wiederholen Sie die Schritte 3 bis 5, um die Unterstützung für eine weitere Sprache hinzuzufügen.
7. Klicken Sie auf **OK**.
8. Klicken Sie im Menü **Datei** auf **Speichern**.

Anpassen der Währungsunterstützung

Wenn Sie zusätzliche Währungen benötigen oder vorhandene Währungen aus der Benutzeroberfläche entfernen möchten, können Sie die Liste der unterstützten Währungen in der Tabelle "Währungen" aktualisieren. Wenn Sie japanische oder koreanische Währungen verwenden, müssen Sie die Unterstützung konfigurieren, damit das japanische Yen-Zeichen und das koreanische Won-Zeichen korrekt dargestellt werden.

Standardmäßig zeigen IBM Cognos-Komponenten nur eine Teilmenge der unterstützten Währungen in der Benutzeroberfläche an. Währungen werden durch entsprechenden ISO 4217-Code gekennzeichnet. Die vollständige Liste der unterstützten Währungen, die hinzugefügt werden können, befindet sich in der Datei "i18n_res.xml" im Verzeichnis *installationsverzeichnis*/bin.

Wenn Sie der IBM Cognos-Umgebung Währungen hinzufügen, ist damit nicht garantiert, dass Ihr Computer über eine Schriftart mit den zur Anzeige der Währung erforderlichen Schriftzeichen verfügt. Stellen Sie sicher, dass Sie die entsprechenden Schriftarten zur Unterstützung der gewünschten Währungssymbole installieren. Um beispielsweise das indische Währungssymbol (Rupie) korrekt anzuzeigen, müssen Sie eine Schriftart mit diesem Zeichen installieren. Damit japanische und koreanische Währungssymbole korrekt angezeigt werden, müssen Sie die zusätzlichen Schriftarten vom Datenträger "Supplementary Language Documentation" installieren.

Hinzufügen von Währungen zur Benutzeroberfläche

Sie können der Benutzeroberfläche unterstützte und nicht unterstützte Währungen hinzufügen. Unterstützte Währungen werden in IBM Cognos Configuration hinzugefügt. Nicht unterstützte Währungen werden der Datei 'i18n_res.xml' hinzugefügt, die mit IBM Cognos geliefert wird.

Wenn Sie einen Währungscode hinzufügen, der von IBM Cognos nicht unterstützt wird, müssen Sie ihn manuell der Datei "i18n_res.xml" im Verzeichnis '*installationsposition*/bin' hinzufügen. Kopieren Sie diese Datei auf alle IBM Cognos-Computer Ihrer Installation.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf jedem Content Manager-Computer.
2. Klicken Sie im Menü **Aktionen** auf **Globale Konfiguration bearbeiten**.
3. Klicken Sie auf die Registerkarte **Währungen**.
4. Klicken Sie auf **Hinzufügen**.

   Tipp: Aktivieren Sie zum Entfernen der Unterstützung das Kontrollkästchen neben dem unterstützten Element und klicken Sie auf **Entfernen**.
5. Geben Sie in die zweite Spalte einen geeigneten Wert ein.

   Der hinzugefügte Wert muss mit ISO 4217-Codes für die Darstellung von Währungen und Formaten übereinstimmen. Normalerweise fügen Sie einen dreistelligen alphabetischen Code als Wert ein. Die ersten beiden Zeichen sind Buchstaben, die dem ISO 3166-Länder- oder Regionscode entsprechen, in dem bzw. der die Währung verwendet wird. Der dritte Buchstabe kennzeichnet den ersten Buchstaben der Währung.
6. Wiederholen Sie die Schritte 3 bis 5, um andere Arten der Unterstützung hinzuzufügen.
7. Klicken Sie im Menü **Datei** auf **Speichern**.

Anpassen der Unterstützung von Inhaltsländereinstellungen

Damit Berichte, Daten oder Metadaten tatsächlich in der bevorzugten Sprache des Benutzers oder in der Sprache einer spezifischen Region angezeigt werden, können Sie der Tabelle mit den Ländereinstellungen für Inhalte partielle Ländereinstellungen (Sprache) oder vollständige Ländereinstellungen (Sprache-Region) hinzufügen. Auf diese Weise werden Inhalte, der in verschiedenen Sprachen oder Ländereinstellungen verfügbar sind, basierend auf der Benutzerländereinstellung für Benutzer wiedergegeben. Die im Portal verwendete Produktländereinstellung wird bei bestimmten Inhalten standardmäßig von der Ländereinstellung für Inhalte überschrieben.

Beim Anzeigen von Berichten in Thailändisch werden Ziffern nicht unterstützt.

Vorbereitende Schritte

Wenn eine Ländereinstellung nicht benötigt wird, können Sie sie aus der Liste entfernen. Die Liste muss mindestens eine Ländereinstellung für Inhalte enthalten, damit die Komponenten der Anwendungsebene ordnungsgemäß funktionieren.

Wenn Sie der IBM Cognos-Umgebung unvollständige Ländereinstellungen (Sprachen) hinzufügen, ist nicht garantiert, dass Ihr Computer über eine Schriftart verfügt, um Webseiten in Ihren bevorzugten Sprachen anzuzeigen. Stellen Sie sicher, dass Sie die entsprechenden Schriftarten installieren, um Unterstützung für die gewünschten Zeichensätze und Währungssymbole bereitzustellen. Damit japanische und koreanische Währungssymbole korrekt angezeigt werden, müssen Sie die zusätzlichen Schriftarten vom Supplementary Language Documentation-Datenträger installieren.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf jedem Content Manager-Computer.
2. Klicken Sie im Menü **Aktionen** auf **Globale Konfiguration bearbeiten**.
3. Klicken Sie auf die Registerkarte **Inhaltsländereinstellungen**.

   Alle unterstützten Ländereinstellungen werden angezeigt.
4. Klicken Sie auf **Hinzufügen**.

   Tipp: Aktivieren Sie zum Entfernen der Unterstützung das Kontrollkästchen neben dem unterstützten Element und klicken Sie auf **Entfernen**.

5. Geben Sie in die zweite Spalte einen geeigneten Wert ein.
   - Geben Sie eine Einstellung für eine partielle Ländereinstellung (Sprache) ein, um Sprachunterstützung für Berichtsdaten und Metadaten hinzuzufügen.
   - Geben Sie Einstellungen für eine vollständige Ländereinstellung (Sprache-Region) ein, um die für eine Region spezifische Unterstützung hinzuzufügen.
6. Wiederholen Sie die Schritte 3 bis 5 für jede zusätzliche Ländereinstellung, die unterstützt werden soll.
7. Klicken Sie im Menü **Datei** auf **Speichern**.

Inhaltsländereinstellungen

In der Tabelle "Inhaltsländereinstellungszuordnungen" können Sie Benutzerländereinstellungen mit einer vollständigen (Sprache-Region) oder partiellen (Sprache) Ländereinstellung zuordnen. Darüber hinaus besteht die Möglichkeit, die bevorzugte Sprache eines Benutzers einer anderen Sprache zuzuordnen. Auf diese Weise werden Inhalte, die in der bevorzugten Sprache nicht verfügbar sind, in der anderen Sprache angezeigt.

Ist beispielsweise ein Bericht oder eine Scorecard in der bevorzugten Sprache Vietnamesisch nicht verfügbar, liegt jedoch in den Sprachen Französisch und Deutsch vor, so können Sie in der Tabelle "Inhaltsländereinstellungszuordnungen" die bevorzugte Sprache (Vietnamesisch) in eine andere Sprache (Französisch oder Deutsch) ändern. Der Bericht oder die Scorecard wird daraufhin in der zugeordneten Sprache angezeigt.

Die Tabelle "Inhaltsländereinstellungszuordnungen" beinhaltet standardmäßig Ländereinstellungen ohne Region. Auf diese Weise können Sie nur die Sprachkomponente der Ländereinstellung verwenden, um Ländereinstellungen festzulegen, und es werden immer die korrekten Informationen angezeigt. Die Daten in einer mehrsprachigen Datenbank stehen beispielsweise in unterschiedlichen Sprachen, wie Französisch (fr), Spanisch (es) und Englisch (en), und nicht in unterschiedlichen Ländereinstellungen, wie Englisch-Kanada (en-ca), Englisch-USA (en-us) oder Französisch-Frankreich (fr-fr), zur Verfügung.

Die folgenden Beispiele erläutern die Methode, mit der IBM Cognos BI-Komponenten den Bericht bzw. die Scorecard ermitteln, der bzw. die einem Benutzer bei Verfügbarkeit von mehreren Sprachversionen angezeigt wird.

Beispiel 1

Ein Bericht steht in Content Manager in zwei Ländereinstellungen zur Verfügung, z.B. en-us (Englisch-USA) und fr-fr (Französisch-Frankreich), die Ländereinstellung des Benutzers ist jedoch auf fr-ca (Französisch-Kanada) festgelegt. IBM Cognos verwendet die Ländereinstellungszuordnung, um zu ermitteln, welcher Bericht dem Benutzer angezeigt wird.

IBM Cognos überprüft zunächst, ob der Bericht in Content Manager für die Ländereinstellung des Benutzers verfügbar ist. Wenn dies nicht der Fall ist, ordnet IBM Cognos die Ländereinstellung des Benutzers einer normalisierten Ländereinstellung zu, die auf der Registerkarte "Inhaltsländereinstellungszuordnungen" konfiguriert ist. Da die Ländereinstellung des Benutzers fr-ca lautet, wird sie der Ländereinstellung fr zugeordnet. IBM Cognos kann anhand dieser Zuordnung überprüfen, ob der Bericht in fr verfügbar ist. Im vorliegenden Fall ist der Bericht nur in en-us und fr-fr, nicht aber in fr verfügbar.

Als Nächstes ordnet IBM Cognos allen verfügbaren Berichten eine normalisierte Ländereinstellung zu. Auf diese Weise wird en-us zu en und fr-fr zu fr.

Da sowohl die Berichts- als auch die Benutzerländereinstellung dem Wert fr zugeordnet sind, wird der Bericht für den Benutzer mit der Ländereinstellung fr-ca mit der Ländereinstellung fr-fr gespeichert.

Beispiel 2

Die Ländereinstellung des Benutzers und die Berichtsländereinstellungen sind derselben Sprache zugeordnet. IBM Cognos entscheidet, welche Ländereinstellung verwendet wird. Wenn die Ländereinstellung eines Benutzers beispielsweise en-ca (Englisch-Kanada) lautet und die Berichte in en-us (Englisch-USA) sowie en-gb (Englisch-Großbritannien) zur Verfügung stehen, ordnet IBM Cognos jede Ländereinstellung

dem Wert en zu. Der Bericht wird dem Benutzer mit denjenigen Ländereinstellungen angezeigt, die IBM Cognos auswählt.

Beispiel 3

Der Bericht und die Benutzerländereinstellungen sind keiner gemeinsamen Sprache zugeordnet. IBM Cognos wählt die Sprache aus. In diesem Fall müssen Sie eine Zuordnung konfigurieren. Wenn ein Bericht beispielsweise in en-us (Englisch-USA) und fr-fr (Französisch-Frankreich) zur Verfügung steht, als Ländereinstellung des Benutzers jedoch es-es (Spanisch-Spanien) festgelegt ist, wählt IBM Cognos die Sprache aus.

Verknüpfen von Inhaltsländereinstellungen

In der Tabelle "Inhaltsländereinstellungszuordnungen" können Sie Benutzerländereinstellungen mit einer vollständigen (Sprache-Region) oder partiellen (Sprache) Ländereinstellung zuordnen. Darüber hinaus besteht die Möglichkeit, die bevorzugte Sprache eines Benutzers einer anderen Sprache zuzuordnen. Auf diese Weise werden Inhalte, die in der bevorzugten Sprache nicht verfügbar sind, in der anderen Sprache angezeigt.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf jedem Content Manager-Computer.
2. Klicken Sie im Menü **Aktionen** auf **Globale Konfiguration bearbeiten**.
3. Klicken Sie auf die Registerkarte **Inhaltsländereinstellungszuordnungen**.
4. Klicken Sie auf **Hinzufügen**.
5. Geben Sie in das Feld **Schlüssel** die Benutzerländereinstellung ein:
   - Um zu gewährleisten, dass in allen Regionen für eine Benutzerländereinstellung Inhalte in einer bestimmten Sprache angezeigt werden, geben Sie die Sprachkomponente der Ländereinstellung, gefolgt von einem Bindestrich (-) und einem Platzhalterzeichen (*) ein.

     Geben Sie beispielsweise **de-*** ein.
   - Um zu gewährleisten, dass für eine Benutzerländereinstellung (Sprache-Region) Inhalte in einer bestimmten Sprache angezeigt werden, geben Sie die vollständige Ländereinstellung ein.

     Geben Sie beispielsweise **de-de** ein.
   - Um eine bevorzugte Sprache mit einer anderen Sprache zu verknüpfen, geben Sie die Komponente der Ländereinstellung für die bevorzugte Sprache ein.

     Geben Sie beispielsweise **zh** ein.

   Tipp: Wenn Sie für eine Reihe von Schlüsseln eine Ländereinstellung festlegen möchten, fügen Sie das Platzhalterzeichen (*) zum Wert unter **Schlüssel** hinzu und geben Sie die Ländereinstellung dann in das Feld **Ländereinstellungszuordnung** ein. Beispiel: Wenn alle Schlüssel für Deutsch beispielsweise die deutsche Ländereinstellung verwenden sollen, geben Sie **de*** im Feld **Schlüssel** und in das Feld **Ländereinstellungszuordnung** den entsprechenden Wert ein.
6. Geben Sie in das Feld **Ländereinstellungszuordnung** die Sprachkomponente der Ländereinstellung ein.

   Für die Benutzerländereinstellungen, die im Feld **Schlüssel** angegeben wurden, wird der Inhalt in dieser Sprache angezeigt.
7. Wiederholen Sie die Schritte 3 bis 5 für weitere Zuordnungen.
8. Klicken Sie auf **OK**.
9. Klicken Sie im Menü **Datei** auf **Speichern**.

Verknüpfen einer Produktländereinstellung

Verwenden Sie die Tabelle "Produktländereinstellungszuordnungen", um die für die Benutzeroberfläche verwendete Sprache anzugeben, wenn die Sprache in der Ländereinstellung des Benutzers nicht zur Verfügung steht.

Sie können gewährleisten, dass alle Regionen für eine Ländereinstellung die gleiche Sprache verwenden oder dass eine spezifische vollständige Ländereinstellung (Sprache-Region) eine bestimmte Sprache verwendet.

Die Benutzeroberfläche des Produkts wird standardmäßig in der Sprache angezeigt, die in den Spracheinstellungen der Benutzerländereinstellung angegeben ist.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf jedem Content Manager-Computer.
2. Klicken Sie im Menü **Aktionen** auf **Globale Konfiguration bearbeiten**.
3. Klicken Sie auf die Registerkarte **Produktländereinstellungszuordnungen**.
4. Klicken Sie auf **Hinzufügen**.
5. Geben Sie in das Feld **Schlüssel** die Benutzerländereinstellung ein:
   - Um zu gewährleisten, dass in allen Regionen für eine Ländereinstellung die Benutzeroberfläche in einer bestimmten Sprache angezeigt wird, geben Sie die Sprachkomponente der Ländereinstellung, gefolgt von einem Bindestrich (-) und einem Platzhalterzeichen (*) ein.

     Geben Sie beispielsweise **es-*** ein.
   - Um zu gewährleisten, dass für eine vollständige Ländereinstellung (Sprache-Region) die Benutzeroberfläche in einer bestimmten Sprache angezeigt wird, geben Sie die vollständige Ländereinstellung ein.

     Geben Sie beispielsweise **es-es** ein.
   - Um eine bevorzugte Sprache mit einer anderen Sprache zu verknüpfen, geben Sie die Komponente der Ländereinstellung für die bevorzugte Sprache ein.

     Geben Sie beispielsweise **zh** ein.

   Tipp: Um die standardmäßig zu verwendende Ländereinstellung anzugeben, geben Sie im Feld **Schlüssel** ein Platzhalterzeichen (*) als Wert ein. Geben Sie anschließend im Feld **Ländereinstellungszuordnung** die Ländereinstellung ein.
6. Geben Sie in das Feld **Ländereinstellungszuordnung** die Sprachkomponente der Ländereinstellung ein.

   Für die Benutzerländereinstellungen, die im Feld **Schlüssel** angegeben wurden, wird der Inhalt in dieser Sprache angezeigt.
7. Wiederholen Sie die Schritte 3 bis 5 für weitere Zuordnungen.
8. Klicken Sie auf **OK**.
9. Klicken Sie im Menü **Datei** auf **Speichern**.

Anpassen der Zeitzone für den Server

Sie können die von Content Manager verwendete Zeitzone anpassen, indem Sie eine andere Zeitzone für den Server in IBM Cognos Configuration auswählen.

Bei UNIX-Installationen, die keine Java-basierte grafische Benutzeroberfläche unterstützen, können Sie die Liste der zulässigen Zeitzonen anzeigen, indem Sie IBM Cognos Configuration auf dem Windows-Computer öffnen, auf dem Framework Manager installiert ist.

Standardmäßig verwendet Content Manager die Zeitzone des Betriebssystems. Alle geplanten Aktivitäten in IBM Cognos werden mithilfe dieser Zeitzone festgelegt. Zusätzlich wird diese Zeitzone von Benutzern

in Portal verwendet, um die Standardzeitzone einzustellen. Weitere Informationen zum Einstellen von Benutzervorgaben in Portal finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Klicken Sie im Menü **Aktionen** auf **Globale Konfiguration bearbeiten**.
3. Klicken Sie im Fenster **Globale Konfiguration** auf die Registerkarte **Allgemein**.
4. Klicken Sie für die **Server-Zeitzone** auf die Spalte **Wert** und wählen Sie eine andere Zeitzone aus der Liste aus.
5. Klicken Sie im Menü **Datei** auf **Speichern**.

Codierung für E-Mail-Nachrichten

Standardmäßig wird von IBM Cognos-Komponenten in E-Mails UTF-8-Codierung verwendet. Dieser Wert legt die Standardcodierung fest, die vom Zustellungsservice in dieser Instanz für alle E-Mail-Nachrichten verwendet wird. Wenn Sie ältere E-Mail-Clients verwenden oder E-Mail-Nachrichten von IBM Cognos an Mobiltelefone und PDAs senden, wird UTF-8 möglicherweise nicht erkannt. In diesem Fall können Sie für die E-Mail-Codierung einen anderen Wert festlegen, der von allen E-Mail-Clients unterstützt wird (z. B. ISO-8859-1, Shift-JIS). Jede Instanz von IBM Cognos, für die ein Zustellungsservice verfügbar ist, muss geändert werden.

Die angegebene Codierung wirkt sich auf die gesamte Nachricht einschließlich Betreff, Anhänge, Namen der Anhänge und Textkörper im Klartext- oder HTML-Format aus.

Die Codierungswerte finden Sie in der folgenden Tabelle:

Tabelle 31. Unterstützte Codierungswerte

Zeichensatz	**Unterstützter Codierungswert**
UTF-8	utf-8
Westeuropäisch (ISO 8859-1)	iso-8859-1
Westeuropäisch (ISO 8859-15)	iso-8859-15
Westeuropäisch (Windows-1252)	windows-1252
Mittel- und Osteuropäisch (ISO 8859-2)	iso-8859-2
Mittel- und Osteuropäisch (Windows-1250)	windows-1250
Kyrillisch (ISO 8859-5)	iso-8859-5
Kyrillisch (Windows-1251)	windows-1251
Türkisch (ISO 8859-9)	iso-8859-9
Türkisch (Windows-1254)	windows-1254
Griechisch (ISO 8859-7)	iso-8859-7
Griechisch (Windows-1253)	windows-1253
Japanisch (EUC-JP)	euc-jp

Tabelle 31. Unterstützte Codierungswerte (Forts.)	
Zeichensatz	**Unterstützter Codierungswert**
Japanisch (ISO-2022-JP)	iso-2202-jp
Japanisch (Shift-JIS)	shift_jis
Traditionelles Chinesisch (Big5)	big5
Vereinfachtes Chinesisch (GB-2312)	gb2312
Koreanisch (EUC-KR)	euc-kr
Koreanisch (ISO 2022-KR)	ISO 2022-KR
Koreanisch (KSC-5601)	ksc_5601
Thailändisch (Windows-874)	windows-874
Thailändisch (TIS-620)	tis-620

Ändern der Codierung für E-Mail-Nachrichten

Sie können die E-Mail-Codierung in einen Wert ändern, der von allen E-Mail-Clients unterstützt wird.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Klicken Sie im Menü **Aktionen** auf **Globale Konfiguration bearbeiten**.
3. Klicken Sie im Fenster **Globale Konfiguration** auf die Registerkarte **Allgemein**.
4. Klicken Sie für die Eigenschaft **E-Mail-Codierung** auf die Spalte **Wert**.
5. Wechseln Sie mit dem Bildlauf zur gewünschten Einstellung und klicken Sie auf diese Einstellung.
6. Klicken Sie im Menü **Datei** auf **Speichern**.

Anpassen von Cookieeinstellungen

Je nach den Anforderungen Ihrer IBM Cognos-Umgebung müssen die die Einstellungen, die von IBM Cognos-Komponenten verwendet werden, unter Umständen geändert werden. Zum Anpassen der Cookiedomäne, des Pfads und des Sicherheitsflags können Sie IBM Cognos Configuration verwenden.

IBM Cognos-Komponenten ermitteln die Cookiedomäne anhand der vom Client übermittelten HTTP-Anforderung. Der Client ist dabei normalerweise ein Web-Browser. Bei den meisten Netzkommunikationen passieren HTTP-Anforderungen auf dem Weg vom Browser zu den IBM Cognos-Komponenten zwischengeschaltete Instanzen wie beispielsweise Proxy-Server oder Firewalls. Einige zwischengeschaltete Instanzen verändern die Informationen, die die IBM Cognos-Komponenten zur Berechnung der Cookiedomäne verwenden. Die IBM Cognos-Komponenten können dann keine Cookies festlegen. Dieses Problem äußert sich normalerweise dadurch, dass Benutzer wiederholt aufgefordert werden, sich anzumelden. Konfigurieren Sie die Cookiedomäne, um dieses Problem zu vermeiden.

Verwenden Sie beim Festlegen des korrekten Wertes für die Cookiedomäne das Format und den Wert, durch die die breiteste Abdeckung für den Host gewährleistet wird (wie nachfolgend angegeben).

- Verwenden Sie für den Wert für die Domäne den Computer- oder Servernamen. Geben Sie diesen Namen ohne Punkte an. Beispiel: `meineFirma`

- Der Wert für die Domäne kann auch ein Suffix enthalten. Zu den Suffixen gehören .com, .edu, .gov, .int, .mil, .net oder .org. Einen Punkt als Präfix hinzufügen. Beispiel: `.meineFirma.com`.
- Es können weitere Ebenen in einem Domänenwert verwendet werden. Dabei sollte der Punkt des Präfix mit eingeschlossen werden. Beispiel: `.accounts.meineFirma.com`.
- Ein Wert für den Pfad kann Cookies weiter begrenzen. Der allgemeinste Pfad ist `/`. Der Pfad `/payables` beschränkt den Cookie auf alle Pfade, die mit "payable" beginnen (und alle Unterverzeichnisse). Der Pfad `/payables/` beschränkt den Cookie auf das Verzeichnis "payables" (und alle Unterverzeichnisse).

Darüber hinaus können Administratoren zu Sicherheitszwecken das Attribut HTTPOnly so einstellen, dass Scripts während einer Benutzersitzung das CAM-Passport-Cookie nicht über den Web-Browser lesen oder bearbeiten können. Weitere Informationen zu diesem Attribut finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf jedem Content Manager-Computer.
2. Klicken Sie im Menü **Aktionen** auf **Globale Konfiguration bearbeiten**.
3. Klicken Sie auf die Registerkarte **Allgemein**.
4. Klicken Sie unter **Cookieeinstellungen** auf die Spalte **Wert** für jede Eigenschaft, die geändert werden soll, und geben Sie den neuen Wert an.

   Wenn Sie die Eigenschaft **Domäne** leer lassen, leitet der Dispatcher die Domäne vom Hostnamen der Anforderung ab.
5. Klicken Sie auf **OK**.

Ändern der IP-Adressversion

IBM Cognos-Produkte unterstützen zwei IP-Adressversionen: IPv4 und IPv6. IPv4 verwendet 32-Bit-IP-Adressen und IPv6 128-Bit-IP-Adressen.

Beispiel:

- IPv4: 192.168.0.1:80
- IPv6: [2001:0db8:0000:0000:0000:148:57ab]:80

In IBM Cognos Configuration können Sie mithilfe der Eigenschaft **IP-Version für die Auflösung des Hostnamens** auswählen, ob IPv4 oder IPv6 für die IBM Cognos-Kommunikation verwendet wird. Standardmäßig wird IPv4 verwendet.

Die Einstellung gilt nur für den Computer, auf dem sie vorgenommen wird. Wenn Sie **IPv4-Adressen verwenden** auswählen, werden alle abgehenden IBM Cognos-Verbindungen auf diesem Computer mit IPv4 hergestellt und der Dispatcher akzeptiert nur eingehende IPv4-Verbindungen. Wenn Sie **IPv6-Adressen verwenden** auswählen, werden alle abgehenden IBM Cognos-Verbindungen auf diesem Computer mit IPv6 hergestellt und der Dispatcher akzeptiert eingehende IPv4- und IPv6-Verbindungen.

IPv4-Clients können mit Dispatcher-Computern kommunizieren, die für IPv6 konfiguriert sind.

Im URI festgelegte Hostnamen werden anhand des Werts der Eigenschaft **IP-Version für die Auflösung des Hostnamens** aufgelöst. Wenn ein URI mit einer numerischen IPv4-Adresse angegeben wird, besitzt diese Vorrang vor dieser Einstellung und die Kommunikation erfolgt mit IPv4.

Damit IBM Cognos Configuration in den lokalen URI-Eigenschaften IPv6-Adressen akzeptiert, müssen Sie IBM Cognos Configuration mit der Option -ipv6 starten. Sie können die Option jedes Mal angeben, wenn Sie IBM Cognos Configuration über die Befehlszeile starten.

Unter Windows können Sie die Option permanent festlegen, indem Sie sie zum Direktaufruf für das Startmenü hinzufügen.

Festlegen der IP-Version

Verwenden Sie IBM Cognos Configuration, um die IP-Version auszuwählen.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Klicken Sie für **IP-Version für die Auflösung des Hostnamens** auf das Feld **Wert** und klicken Sie auf **IPv4-Adressen verwenden** oder **IPv6-Adressen verwenden**.
4. Klicken Sie im Menü **Datei** auf **Speichern**.
5. Schließen Sie IBM Cognos Configuration.

Manuelles Konfigurieren von IBM Cognos Configuration zum Starten mit der Option IPv6

Sie können IBM Cognos Configuration manuell so konfigurieren, dass die Option IPv6 verwendet wird. Legen Sie dazu die Option im Startbefehl fest.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *installationsposition*/bin oder *installationsposition*/bin64.
2. Starten Sie IBM Cognos Configuration mit der IPv6-Option. Gehen Sie dabei je nach Betriebssystem folgendermaßen vor:
   - Geben Sie unter Windows Folgendes ein:

     ```
     cogconfig.bat -ipv6
     ```
   - Geben Sie unter UNIX oder Linux Folgendes ein:

     ```
     ./cogconfig.sh -ipv6
     ```
3. Bearbeiten Sie die URI-Eigenschaften, die das IPv6-Format verwenden, legen Sie die Werte fest und klicken Sie dann im Menü **Datei** auf **Speichern**.

Konfigurieren von IBM Cognos Configuration, sodass es unter Windows immer mit der Option IPv6 gestartet wird

Sie können IBM Cognos Configuration so konfigurieren, dass unter einem Microsoft Windows- Betriebssystem stets die Option IPv6 verwendet wird. Legen Sie die Option dazu in der Startmenüverknüpfung fest.

Vorgehensweise

1. Klicken Sie im Menü **Start** mit der rechten Maustaste auf **IBM Cognos Configuration** und wählen Sie **Eigenschaften** aus.
2. Geben Sie auf der Registerkarte **Verknüpfung** im Feld **Ziel** Folgendes ein:

   ```
   "install_location\bin\cogconfigw.exe -ipv6"
   ```
3. Klicken Sie auf **OK**.

Konfigurieren des Collaboration Discovery-URI

Sie können IBM Cognos Analytics und IBM Cognos Workspace für die Verwendung von IBM Connections für die bereichsübergreifende Entscheidungsfindung konfigurieren. Die Integration mit IBM Connections ermöglicht es Geschäftsbenutzern, beim Erstellen oder Anzeigen von Berichten, der Durchführung von Analyse-oder Überwachungsarbeitsbereichen zusammenzuarbeiten. Users have access to IBM Connecti-

ons activities from within IBM Cognos Workspace and to the IBM Connections homepage from within IBM Cognos Analytics and IBM Cognos Workspace.

Der Collaboration-Erkennungs-URI gibt den IBM Connections-Server an, der als Collaboration-Provider verwendet werden soll. Wenn eine URI angegeben wird, wird die Unterstützung für Onlinezusammenarbeit zu IBM Cognos Analytics wie folgt hinzugefügt:

- Ein Link wird zur Begrüßungsseite des IBM Cognos Analytics-Portals hinzugefügt. Wenn der Benutzer Zugriff auf die Homepage von IBM Connections hat, wird der Link **Zugriff auf mein soziales Netzwerk** genannt und verknüpft den Benutzer mit der Homepage. Wenn der Benutzer Zugriff auf die IBM -Verbindungsaktivitäten hat, nicht aber die Homepage, wird der Link **Eigene Aktivitäten** genannt und verknüpft den Benutzer mit der Seite 'Aktivitäten'.
- Ein Link zur Homepage von IBM Connections wird zum Startmenü im Portal hinzugefügt.
- Ein Link zur Homepage von IBM Connections wird zum Menü 'Aktionen' im Arbeitsbereich ' IBM Cognos ' hinzugefügt.
- Die Menüschaltfläche **Zusammenarbeiten** wird in der Arbeitsbereichsanwendungsleiste in IBM Cognos Workspace hinzugefügt. Dies ermöglicht dem Benutzer, eine Arbeitsbereichsaktivität in IBM Connections zu erstellen oder anzuzeigen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Dispatcher und Services** , um die Liste der Disponenten anzuzeigen.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche Eigenschaften festlegen-Konfiguration.
3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Geben Sie für die Kategorie **Umwelt** , **URI der Collaboration-Erkennung**, den URI wie folgt an:

   `http://`*`Servername`*`:`*`Portnummer`*`/activities/serviceconfigs`

   Beispiel: `http://`*`Servername`*`: 9080/activities/serviceconfigs`

   Dabei steht *`Servername`* für den Servernamen, in dem IBM Connections installiert ist.
5. Klicken Sie auf **OK**.

Konfigurieren von IBM Cognos Workspace

IBM Cognos Workspace ist in IBM Cognos Analytics Server enthalten. Das Produkt umfasst dynamische und anpassbare Funktionen, mit denen Sie schnell und einfach interaktive Arbeitsbereiche mit IBM Cognos-Inhalten und externen Datenquellen erstellen können. Nachdem Sie überprüft haben, ob IBM Cognos Workspace korrekt ausgeführt wird, können Sie den Zugriff auf geschützte Tools und Funktionen konfigurieren.

Führen Sie die folgenden Konfigurationsaufgaben aus.

__ • Konfigurieren des Zugriffs auf IBM Cognos Workspace.

__ • Konfigurieren von unterstützten MIME-Typen in Microsoft Internet Information Services.

Nachdem Sie die Konfigurationsaufgaben abgeschlossen haben, können Sie bei Bedarf die folgenden Aufgaben ausführen:

__ • Einrichten einer Datenbank für Anmerkungen.

__ • Konfigurieren von IBM Cognos Workspace für die Verwendung von Inhalten eines TM1-Datenservers.

__ • Ändern von Stilen in Berichten.

__ • Verwenden von Beispielen.

Konfigurieren des Zugriffs auf IBM Cognos Workspace oder zugehörige Funktionen

Konfigurieren Sie den Zugriff auf IBM Cognos Workspace, indem Sie bestimmten Namespaces, Benutzern, Gruppen oder Rollen die erforderlichen Berechtigungen für die Funktion "Executive Dashboard" erteilen.

Sie können entweder uneingeschränkten Zugriff auf IBM Cognos Workspace oder nur den Zugriff auf die Publizierungsfunktion erteilen.

IBM Cognos Analytics muss konfiguriert und betriebsbereit sein, bevor Sie den Zugriff auf IBM Cognos Workspace konfigurieren können.

Gewähren des uneingeschränkten Zugriffs auf IBM Cognos Workspace

Um Zugriff auf IBM Cognos Workspace und alle zugehörigen Funktionen zu gewähren, erteilen Sie Ausführungsberechtigungen und Transitberechtigungen für die Funktion "Executive Dashboard".

Zusätzliche Informationen zum Konfigurieren von Berechtigungen für Benutzer finden Sie in einem entsprechenden technischen Hinweis (www.ibm.com/support/docview.wss?uid=swg21498402) auf der IBM Website.

Vorgehensweise

1. Starten Sie in IBM Cognos Analytics-Portal die **IBM Cognos Administration**.
2. Klicken Sie auf der Registerkarte **Sicherheit** auf **Funktionen**.
3. Suchen Sie die Funktion **Executive Dashboard**, klicken Sie neben dem Namen der Funktion auf die Schaltfläche  und wählen Sie dann die Option **Eigenschaften festlegen** aus.
4. Klicken Sie auf die Registerkarte **Berechtigungen**.
5. Gewähren Sie Ausführungsberechtigungen für alle Benutzergruppen, die Zugriff auf IBM Cognos Workspace haben sollen, und klicken Sie dann auf **OK**.

Gewähren des Zugriffs auf die Publizierungsfunktion für IBM Cognos Workspace

Um nur den Zugriff auf die Publizierungsfunktion in IBM Cognos Workspace zu gewähren, erteilen Sie Transitberechtigungen für die Funktion "Executive Dashboard" und Ausführungsberechtigungen für die geschützte Funktion "Dashboards in Collaboration Spaces publizieren".

Vorgehensweise

1. Starten Sie in IBM Cognos Analytics-Portal die **IBM Cognos Administration**.
2. Klicken Sie auf der Registerkarte **Sicherheit** auf **Funktionen**.
3. Wählen Sie die Funktion **Executive Dashboard** aus.
4. Klicken Sie neben **Dashboards in Collaboration Spaces publizieren** auf die Schaltfläche **Aktionen**  und anschließend auf **Eigenschaften festlegen**.
5. Klicken Sie auf die Registerkarte **Berechtigungen**.
6. Wenn Sie Zugriffsberechtigungen einzeln für jeden Eintrag festlegen möchten, wählen Sie **Die vom übergeordneten Eintrag geerbten Zugriffsberechtigungen überschreiben** aus.
7. Aktivieren Sie für die einzelnen Benutzergruppen jeweils das Kontrollkästchen für den Eintrag und aktivieren Sie dann im Feld neben der Liste die entsprechenden Kontrollkästchen, um Berechtigungen für den Eintrag zu gewähren.
8. Zum Aufnehmen neuer Einträge in die Liste klicken Sie auf **Hinzufügen** und entscheiden Sie sich für eine Methode zum Auswählen der Einträge:

- Wenn Sie verfügbare Einträge aus der Liste auswählen möchten, klicken Sie auf den entsprechenden Namespace und aktivieren Sie die Kontrollkästchen neben den betreffenden Benutzern, Gruppen oder Rollen.
- Wenn Sie Einträge suchen möchten, klicken Sie auf **Suchen** und geben Sie im Feld **Zeichenfolge, nach der gesucht werden soll** den Suchtext ein. Wenn Sie die Suchoptionen verwenden möchten, klicken Sie auf **Bearbeiten**. Suchen und klicken Sie auf den gewünschten Eintrag.
- Wenn Sie die Namen der hinzuzufügenden Einträge eingeben möchten, klicken Sie auf **Eingeben** und geben Sie die Namen von Gruppen, Rollen oder Benutzern ein. Verwenden Sie dabei das folgende Format und geben Sie die Einträge durch Semikolon (;) getrennt ein: *Namespace*/*Gruppenname*;*Namespace*/*Rollenname*;*Namespace*/*Benutzername*;

Anschließend können Sie für jeden neuen Eintrag die entsprechenden Berechtigungen gewähren.

9. Klicken Sie auf **OK**.

Konfigurieren unterstützter MIME-Typen in Microsoft Internet Information Services

Damit IBM Cognos Workspace bei Nutzung von Microsoft Internet Information Services (IIS) 6.0 erfolgreich geladen werden kann, müssen Sie den von IBM Cognos Workspace verwendeten MIME-Typ definieren.

Vorgehensweise

1. Öffnen Sie die Microsoft IIS-Managementkonsole.
2. Klicken Sie mit der rechten Maustaste auf den lokalen Computernamen und klicken Sie auf **Eigenschaften**.
3. Klicken Sie auf **MIME-Typen**.
4. Klicken Sie auf **Neu**.
5. Geben Sie im Feld **Erweiterung** die Dateinamenerweiterung **.cfg** ein.
6. Im Feld **MIME-Typ** geben Sie **text/plain** ein.
7. Übernehmen Sie die neuen Einstellungen.

   Die Änderungen werden wirksam, wenn der Worker-Prozess wiederverwendet wird. Sie können den World Wide Web Publishing Service starten, damit die Änderungen sofort und ohne Warten wirksam werden. Suchen Sie in der MSDN-Online-Bibliothek von Microsoft nach *Handling MIME Types in Internet Explorer* (Verarbeiten von MIME-Typen in Internet Explorer). Dort finden Sie weitere Informationen.

Erstellen von Tabellenbereichen für die Datenbank für benutzergeführte Aufgaben und Anmerkungen für IBM Db2 unter z/OS

Wenn Sie Db2 unter z/OS verwenden, muss ein Datenbankadministrator Scripts ausführen, um die Tabellenbereiche zu erstellen, die für die Datenbank für benutzergeführte Aufgaben und Anmerkungen erforderlich sind. Diese Scripts müssen angepasst werden, d. h., die Platzhalterparameter sind durch solche zu ersetzen, die für Ihre Umgebung geeignet sind.

Stellen Sie sicher, dass Sie die Namenskonventionen für Db2 unter z/OS verwenden. Beispielsweise müssen alle Parameternamen mit einem Buchstaben anfangen und dürfen maximal sechs Zeichen lang sein. Weitere Informationen finden Sie im Db2 Knowledge Center.

Sie können die Content Store-Datenbank oder eine separate Datenbank für die Datenbank für benutzergeführte Aufgaben und Anmerkungen verwenden. In beiden Fällen müssen Sie die Scripts zu Erstellen der Tabellenbereiche ausführen.

Vorgehensweise

1. Stellen Sie als Benutzer mit Berechtigungen zum Erstellen und Löschen von Tabellenbereichen sowie zum Ausführen von SQL-Anweisungen eine Verbindung mit der Datenbank her.
2. Wechseln Sie zur Erstellung der Tabellenbereiche mit den benutzergeführten Aufgaben in das Verzeichnis *installationsposition*/configuration/schemas/hts/zosdb2.
   a) Erstellen Sie eine Sicherungskopie der Scriptdatei HTS_tablespaces.sql und speichern Sie die Datei unter einer anderen Position.
   b) Öffnen Sie die ursprüngliche Scriptdatei HTS_TABLESPACES.sql und ersetzen Sie mithilfe der folgenden Tabelle die Standardparameter durch die für Ihre Umgebung geeigneten Parameter.

   Tabelle 32. Parameternamen für Tabellenbereiche und Beschreibungen für benutzergeführte Aufgaben in Db2 unter z/OS

Parametername	**Beschreibung**
NCCOG	Legt den Namen der Datenbank fest.
DSN8G810	Gibt den Namen der Speichergruppe an.
BP32K	Gibt den Namen des 32-K-Pufferpools an.

   Eine vollständige Liste der erforderlichen Parameter ist im Script enthalten.
   c) Speichern Sie das Script und führen Sie es aus.
   d) Öffnen Sie die Scriptdatei HTS2_CREATE_Db2zos.sql und ersetzen Sie die generischen Parameter durch die für Ihre Umgebung geeigneten Parameter mithilfe der folgenden Tabelle.

   Tabelle 33. Parameternamen für Tabellenbereiche und Beschreibungen für benutzergeführte Aufgaben in Db2 unter z/OS

Parametername	**Beschreibung**
NCCOG	Der Name der Datenbank.

   Eine vollständige Liste der erforderlichen Parameter ist im Script enthalten.
   e) Speichern Sie das Script und führen Sie es aus.
3. Wechseln Sie zur Erstellung der Tabellenbereiche mit den Anmerkungen in das Verzeichnis *installationsposition*/configuration/schemas/ans/zosdb2.
   a) Erstellen Sie eine Sicherungskopie der Scriptdatei ANN_TABLESPACES.sql und speichern Sie die Datei an einer anderen Position.
   b) Öffnen Sie die ursprüngliche Scriptdatei ANN_TABLESPACES.sql und ersetzen Sie mithilfe der folgenden Tabelle die Standardparameter durch die für Ihre Umgebung geeigneten Parameter.

   Tabelle 34. Parameternamen für Tabellenbereiche und Beschreibungen für Anmerkungen in Db2 unter z/OS

Parametername	**Beschreibung**
NCCOG	Der Name der Datenbank.
DSN8G810	Der Name der Speichergruppe.
BP32K	Der Name des 32-K-Pufferpools.

   Eine vollständige Liste der erforderlichen Parameter ist im Script enthalten.

c) Speichern Sie das Script und führen Sie es aus.

d) Öffnen Sie die Scriptdatei `ANS2_CREATE_Db2zos.sql` und ersetzen Sie die generischen Parameter durch die für Ihre Umgebung geeigneten Parameter mithilfe der folgenden Tabelle.

Tabelle 35. Parameternamen für Tabellenbereiche und Beschreibungen für Anmerkungen in Db2 unter z/OS

Parametername	**Beschreibung**
NCCOG	Der Name der Datenbank.

Eine vollständige Liste der erforderlichen Parameter ist im Script enthalten.

e) Speichern Sie das Script und führen Sie es aus.

Einrichten einer Datenbank für benutzergeführte Aufgaben und Anmerkungen

Die in IBM Cognos Workspace für benutzergeführte Aufgaben und Anmerkungen verwendeten Daten werden standardmäßig in derselben Datenbank wie der Content Store gespeichert. Sie können jedoch auch eine separate Datenbank für benutzergeführte Aufgaben und Anmerkungen konfigurieren.

Um die Datenbank einzurichten, müssen Sie zunächst die Datenbank sowie ein Benutzerkonto erstellen, unter dem die Datenbank ausgeführt werden soll. Anschließend konfigurieren Sie die Funktion für benutzergeführte Aufgaben und Anmerkungen für die Verwendung der neuen Datenbank.

Vorgehensweise

1. Erstellen Sie eine Datenbank. Befolgen Sie dazu die Anweisungen unter „Richtlinien zum Erstellen des Content Store" auf Seite 7.

   Wenn Sie IBM Db2 unter z/OS für Ihre Datenbank verwenden, müssen Sie die erforderlichen Tabellenbereiche durch das Ausführen von zwei Scripts erstellen. Weitere Informationen finden Sie im Abschnitt „Erstellen von Tabellenbereichen für die Datenbank für benutzergeführte Aufgaben und Anmerkungen für IBM Db2 unter z/OS" auf Seite 247.
2. Erstellen Sie ein Benutzerkonto, das zum Ausführen der Datenbank verwendet werden soll.
3. Starten Sie IBM Cognos Configuration für die Instanz, auf der die Komponenten der Anwendungsebene installiert sind.
4. Klicken Sie im **Explorer** mit der rechten Maustaste auf **Service für benutzergeführte Aufgaben und Anmerkungsservice** und wählen Sie **Neue Ressource** > **Datenbank** aus.
5. Geben Sie im Dialogfeld **Neue Ressource - Datenbank** einen Namen für die Datenbank ein, wählen Sie den Datenbanktyp aus und klicken Sie dann auf **OK**.
6. Konfigurieren Sie im Fenster **Eigenschaften** für die Datenbankressource Folgendes:
   - Geben Sie die erforderlichen Werte für alle mit einem Sternchen gekennzeichneten Eigenschaften an.
   - Geben Sie **Benutzer-ID und Kennwort** für das Konto an, unter dem die Datenbank ausgeführt wird.
7. Klicken Sie im Menü **Datei** auf **Speichern**.

   Die Anmeldeberechtigungsnachweise werden sofort verschlüsselt.
8. Zum Testen der Verbindung mit der neuen Datenbank klicken Sie im Menü **Aktionen** auf **Test**.
9. Wiederholen Sie diese Schritte für alle Instanzen von Komponenten der Anwendungsebene und Content Manager.

Konfigurieren von IBM Cognos Workspace für die Verwendung von IBM Cognos TM1-Daten

Damit Sie IBM Cognos TM1-Daten in IBM Cognos Workspace verwenden können, müssen Sie Konfigurationsdateien in Ihrer IBM Cognos Analytics-Installation modifizieren.

Führen Sie die folgenden Aufgaben aus, um den TM1-Datenserver für IBM Cognos Workspace zu konfigurieren:

__ • Definieren Sie die Verbindungsinformationen für den TM1 Server.

__ • Definieren Sie die Namen der IBM Cognos TM1-Server so wie sie in IBM Cognos Workspace angezeigt werden.

__ • Optional können Sie die Namen für die Ansichtenordner ändern.

Definieren von Verbindungsinformationen für den TM1 Server

Sie müssen eine Konfigurationsdatei modifizieren, um die Verbindungsinformationen für die TM1-Server zu definieren.

Ein Beispiel für eine Contribution-Datei ist in der IBM Cognos Analytics-Installation enthalten. Bei einer verteilten Installation steht die Konfigurationsdatei auf den Computern zur Verfügung, auf denen die Komponenten der Anwendungsebene installiert wurden.

Wenn das IBM Cognos Analytics-Gateway auf einem anderen Computer ausgeführt wird als TM1 Web, müssen Sie sicherstellen, dass die vollständig qualifizierten Domänennamen als Werte für die Servernamen verwendet werden, zum Beispiel `TM1WebHost`. Verwenden Sie z. B. `http://`*`EigenerComputer.EigeneDomäne`*`.com/ibmcognos`, nicht `http://`*`EigenerComputer`*`/ibmcognos`. Darüber hinaus müssen Sie auch im Abschnitt **Umgebung** von IBM Cognos Configuration für die Werte des Servernamens die vollständig qualifizierten Domänennamen verwenden.

Vorgehensweise

1. Wechseln Sie auf dem Computer, auf dem Sie die IBM Cognos Analytics Application Tier-Komponenten der Anwendungsebene installiert haben, in das Verzeichnis *`installationsposition`*`\configuration\icd\contributions\contrib` und benennen Sie die Datei `tm1_contribution.atom.sample` in `tm1_contribution.atom` um.
2. Öffnen Sie die Datei `tm1_contribution.atom` in einem Texteditor.

   Die Datei enthält drei `<atom:entry>`-Abschnitte. Sie müssen die Werte in einem der `<atom:entry>`-Abschnitte für jeden TM1-Server ändern, auf den in IBM Cognos Workspace zugegriffen werden soll. Wenn weitere TM1-Server hinzugefügt werden sollen, müssen Sie nach Bedarf `<atom:entry>`-Abschnitte hinzufügen. Darüber hinaus müssen Sie überzählige `<atom:entry>`-Abschnitte auf Kommentar setzen. Der dritte `<atom:entry>`-Abschnitt in der Beispieldatei ist bereits auf Kommentar gesetzt.

   Der erste `<atom:entry>`-Abschnitt ist für einen TM1-Server, der keine Cognos-Authentifizierung verwendet.

   Der zweite `<atom:entry>`-Abschnitt ist für einen TM1-Server, der die Cognos-Authentifizierung verwendet.
3. Ersetzen Sie im entsprechenden `<atom:entry>`-Abschnitt für die erforderliche Authentifizierung die Werte **`TM1WebHostName`** und **`TM1HostName`** durch den Namen oder die IP-Adresse des TM1-Web-Servers und TM1-Datenservers.

   Ändern Sie z. B. die hervorgehobenen Teile des Beispiels:

   ```
   TM1WebHost=TM1WebHostName&amp;
   TM1WebVirtualDirectory=tm1web&amp;
   TM1Host=TM1HostName&amp;
   ```
4. Für einen TM1 Server, der keine IBM Cognos-Authentifizierung nutzt, ändern Sie die hervorgehobenen Teile für den Wert des Typs `TM1DataServer`:

```
TM1DataServer=TM1ServerHostWithoutCAM&amp;
TM1username=admin&amp;TM1pass=apple
```

Ersetzen Sie **admin** und **apple** durch die Benutzer-ID und das Kennwort des Administratorkontos, das für den TM1 Server verwendet wird.

5. Für einen TM1 Server, der die IBM Cognos-Authentifizierung nutzt, ändern Sie die hervorgehobenen Teile für den Wert für `TM1DataServer`:

```
TM1DataServer=CamAuthenticatedTM1ServerHost
```

6. Ändern Sie die folgenden Eigenschaften, wenn Sie nicht die Standardwerte verwenden:
   - `https`

     Diese Eigenschaft beschreibt das für den TM1 Web Server verwendete Protokoll. Wenn der TM1 Web Server mit HTTP Secure ausgeführt wird, ersetzen Sie **0** durch **1**.
   - `TM1WebVirtualDirectory`

     Diese Eigenschaft ist der Name des virtuellen Verzeichnisses für den TM1 Web Server. Wenn der Verzeichnisname für TM1 Web nicht `tm1web` ist, ersetzen Sie den Wert der Eigenschaft `TM1Web-VirtualDirectory` durch den korrekten Namen.

     Zum Beispiel

     ```
     TM1WebVirtualDirectory=planningweb&amp;
     ```

   - `TM1Toolbar`

     Diese Eigenschaft legt fest, ob die interne Symbolleiste sichtbar ist. TM1Web-Versionen vor Version 9.5.2 lassen keine externe Symbolleiste zu. Der Standardwert von `TM1Toolbar` ist **0**. Zur Anzeige der internen Symbolleiste müssen Sie den Wert auf **1** setzen.
7. Wenn Sie mehrere TM1-Serververbindungen definieren, erstellen Sie jeweils einen `<atom:entry>`-Abschnitt für jeden TM1-Server.

   Alle Werte für `atom:id` in allen `.atom`-Einträgen müssen eindeutig sein. Zum Beispiel

   ```
   <atom:entry>
           <atom:id>tag:ibm.cognos.icd.com,2010-01-01:/tm1_rootfeed_2
   </atom:id>
   ```

   ```
   <atom:entry>
           <atom:id>tag:ibm.cognos.icd.com,2010-01-01:/tm1_rootfeed_2b
   </atom:id>
   ```

   `tm1_rootfeed_2` und `tm1_rootfeed_2b` machen die Beispiele eindeutig.

   Stellen Sie sicher, dass Sie für Werte wie **tm1_rootfeed_1**, **rootfeed_title_1** und **root-feed_summary_1** eindeutige Namen verwenden.
8. Stellen Sie sicher, dass alle nicht verwendeten `<atom:entry>`-Abschnitte auf Kommentar gesetzt sind.
9. Speichern Sie die Datei und schließen Sie sie.
10. Führen Sie einen Neustart der IBM Cognos-Services durch. Wenn Sie die Namen der TM1 Server so ändern möchten, wie sie in IBM Cognos Workspace angezeigt werden, können Sie die Services nach der nächsten Aufgabe neu starten.

Definieren der Namen des IBM Cognos TM1 Servers

Sie können die Namen Ihrer TM1 Server so definieren, wie sie in IBM Cognos Workspace angezeigt werden.

Wenn Sie eine andere Sprache als Deutsch verwenden, können Sie zusätzliche Sprachdateien erstellen, um die Namen in IBM Cognos Workspace anzuzeigen.

Vorgehensweise

1. Wechseln Sie auf dem Computer, auf dem die IBM Cognos Analytics-Komponenten der Anwendungsebene installiert sind, in das Verzeichnis *installationsposition*\configuration\icd\contributions\contrib.
2. Öffnen Sie die Datei tm1_en.properties in einem Texteditor.
3. Ändern Sie den Text nach dem Gleichheitszeichen (=) in einen aussagekräftigen Namen für den TM1 Server, der für den Titel definiert ist.

   Beispiel: Wenn Sie in der vorhergehenden Aufgabe eine TM1 Server-Verbindung im Abschnitt rootfeed_title_1 in der Datei tm1_contribution.atom definiert haben, ändern Sie den Namen wie folgt:

   ```
   rootfeed_title_1 = MyTM1Server
   ```

4. Ändern Sie die Beschreibung in der Eigenschaft rootfeed_summary_1 in eine aussagekräftige Beschreibung für den TM1 Server.

   Beispiel: Wenn Sie einen Namen für die TM1 Server-Verbindung in rootfeed_title_1 definiert haben, ändern Sie den Wert für rootfeed_summary_1 wie folgt:

   ```
   rootfeed_summary_1 = Detail about MyTM1Server
   ```

5. Fügen Sie neue Werte für jeden TM1-Server hinzu, den Sie in der vorherigen Aufgabe in der Datei tm1_contribution.atom hinzugefügt haben. Stellen Sie sicher, dass die Abschnitte rootfeed_title und rootfeed_summary mit den Werten übereinstimmen, die Sie in der Datei tm1_contribution.atom definiert haben.
6. Führen Sie die folgenden Schritte aus, wenn Ihre Umgebung mehrere Sprachen unterstützt:
   - Erstellen Sie eine Kopie der Datei tm1_en.properties.
   - Benennen Sie die Datei in tm1_*Sprachencode*.properties um; dabei ist *Sprachencode* der zweistellige Code für die verwendete Sprache, wie zum Beispiel 'ja' oder 'es'.

     Eine Beispieleigenschaftendatei für Französisch ist verfügbar: tm1_fr.properties.
7. Führen Sie einen Neustart für die IBM Cognos-Services durch, damit die Änderungen wirksam werden.

Ändern des Namens für den Ansichtenordner

Optional können Sie den Namen ändern, der in IBM Cognos Workspace für den Ordner **Ansichten** angezeigt wird.

Standardmäßig enthält IBM Cognos Workspace einen Anwendungsordner und einen Ansichtenordner für jeden TM1-Server, der in der Datei tm1_contribution.atom angegeben ist. Der Name des Anwendungsordners wird vom TM1-Server zurückgegeben. Der Name des Ansichtenordners wird durch eine in IBM Cognos Workspace enthaltene Nachrichtendatei vorgegeben.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis '*installationsposition*\templates\ps\messages'.
2. Erstellen Sie eine Kopie der Datei tm1buxmsgs_en.xml und benennen Sie sie dem jeweiligen Sprachencode entsprechend.

   Eine Beispielübersetzungsdatei für Französisch ist verfügbar: tm1buxmsgs_fr.xml.
3. Öffnen Sie die neue Übersetzungsdatei in einem XML-Editor.
4. Ersetzen Sie das Wort Views im folgenden Abschnitt durch den gewünschten Wert:

   ```
   <string id="TM1_VIEWS" type="String" usage="TM1 views">Views</string>
   ```

5. Speichern und schließen Sie die neue Datei.
6. Wiederholen Sie die Schritte für jede unterstützte Sprache.

Ändern des Stils von Berichtsobjekten in IBM Cognos Workspace

Wenn Sie ein Berichtsobjekt auf einen Arbeitsbereich ziehen, wird dieses im Verlaufsstil in silberner und blauer Farbe Ihres Produkts angezeigt. Sie können das Berichtsobjekt im ursprünglich erstellten Stil anzeigen, indem Sie die globale Eigenschaft in der Konfigurationsdatei von IBM Cognos Viewer ändern.

Zu den Berichtsobjekten, die durch die globale Einstellung gesteuert werden, zählen Abfragen, Analysen, Berichte und Berichtsteile, die im Stil von IBM Cognos Version 1.x, Version 8.x oder im Stil für Finanzen (Bilanzen) erstellt wurden. Diese Objekte übernehmen die globale Einstellung, auch wenn Sie die Objekte vor dem Ändern der globalen Einstellung gespeichert haben. Piktogramme von Arbeitsbereichen übernehmen die globale Einstellung nur, wenn Sie das Piktogramm erneut ausführen.

Einige Berichtsobjekte, z. B. PowerPlay-Berichte und Piktogramme von Berichtsobjekten, werden nicht durch die globale Einstellung gesteuert, sondern immer im erstellten Stil dargestellt.

Vorgehensweise

1. Wechseln Sie für jede Instanz von Content Manager und der Komponenten der Anwendungsebene in das Verzeichnis *Installationsposition*/webapps/p2pd/WEB-INF/classes.
2. Öffnen Sie die Datei `viewerconfig.properties` in einem Texteditor.
3. Um Berichtsobjekte im ursprünglich erstellten Stil darzustellen, ändern Sie den Wert für **useAuthoredReportStyles** in `true`.
4. Speichern Sie die Datei und starten Sie anschließend die Services neu.

Zugreifen auf die Beispiele für IBM Cognos Workspace

IBM Cognos Workspace-Beispiele sind in den IBM Cognos Analytics-Beispielen enthalten.

Fachanwender können auf die Beispiele für IBM Cognos Workspace zugreifen, indem Sie die Option zum Öffnen vorhandener Arbeitsbereiche auswählen und anschließend **Beispiele** > **Modelle** > **Cognos Workspace-Beispiele** auswählen.

Weitere Informationen zur Installation und Einrichtung der Beispiele finden Sie in der Veröffentlichung *IBM Cognos Analytics - Beispiele*. Weitere Informationen zur Verwendung der Beispiele finden Sie im *IBM Cognos Workspace Benutzerhandbuch*.

Konfigurieren des Routers für das Testen der Dispatcher-Verfügbarkeit

Wenn Sie zum Verteilen von Anforderungen an IBM Cognos-Dispatcher einen Router verwenden und dieser die Verfügbarkeit eines Servers unter Verwendung einer Test-URL testen kann, können Sie den Router für das Testen der Verfügbarkeit eines IBM Cognos-Dispatchers konfigurieren.

Vorgehensweise

Konfigurieren Sie den Router für die Verwendung einer URL mit dem Pfad `/p2pd/servlet/ping`.

Ist der Dispatcher nicht bereit, wird die folgende Antwort zurückgegeben:

```
503 Service Unavailable
```

Ist der Dispatcher bereit, wird folgende Antwort zurückgegeben:

```
200 OK
```

Konfigurieren von IBM Cognos Analytics zur Zusammenarbeit mit anderen IBM Cognos-Produkten

Bestimmte IBM Cognos-Produkte stellen Funktionen zur Verfügung, die in IBM Cognos Analytics nicht verfügbar sind.

Sie können diese Produkte weiterhin in derselben Umgebung verwenden. Eventuell sind zusätzliche Konfigurationsmaßnahmen erforderlich, damit IBM Cognos Analytics auf Objekte zugreifen kann, die mit anderen IBM Cognos-Produkten erstellt wurden. Weitere Zugriffsanforderungen sind von der Art und Weise der Ausführung abhängig, die Sie für die beiden Produkte ausgewählt haben.

Aktivieren von geplanten Berichten und Agenten für IBM Cognos Planning Contributor-Datenquellen

Zum Ausführen von geplanten Berichten und Agenten, die auf IBM Cognos Planning Contributor-Datenquellen basieren, müssen Sie ein gemeinsam verwendetes geheimes Kennwort angeben. Dies trägt dazu bei, eine sichere Kommunikation zwischen IBM Cognos Analytics-Servern und dem Contributor-Datenserver zu gewährleisten.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf dem Computer mit den Komponenten der Anwendungsebene.
2. Klicken Sie im Fenster **Explorer** unter **Datenzugriff** auf **IBM Cognos Planning** und dann auf **Contributor-Datenserver**.
3. Klicken Sie im Fenster **Eigenschaften** neben der Eigenschaft **Signatur-Kennwort** auf das Feld **Wert** und anschließend auf die Bearbeitungsschaltfläche  , wenn diese angezeigt wird.
4. Geben Sie im Feld **Wert - Signatur-Kennwort** das Kennwort ein, das digital signiert wird.

   Beim Kennwort wird zwischen Groß- und Kleinschreibung unterschieden und es muss mit der Eigenschaft **Signatur-Kennwort** übereinstimmen, die in Configuration Manager von IBM Cognos Series 7 konfiguriert wird (über **Cognos Planning**/**Cognos BI - Contributor-Datenserver**/**Allgemein**).
5. Klicken Sie im Menü **Datei** auf **Speichern**.

Ergebnisse

Es wird eine digitale Signatur erstellt, die auf dem Kennwort basiert. Die digitale Signatur wird von IBM Cognos Analytics verschlüsselt und vom Contributor-Datenserver entschlüsselt.

Konfigurieren des Software Development Kit

Um das IBMCognos Software Development Kit verwenden zu können, müssen Sie einige Konfigurations- und Einrichtungstasks ausführen.

Zum Konfigurieren des Software Development Kit folgen Sie diesem Prozess:

- Wenn Sie den Framework Manager-Scriptplayer von außerhalb des Verzeichnisses 'bin' ausführen möchten, konfigurieren Sie die Umgebungsvariable FM_INI_FILE_PATH als Systemvariable unter einem Microsoft Windows-Betriebssystem. Die Umgebungsvariable muss auf das Verzeichnis *Framework_Manager_location*`\configuration\fm.ini` verweisen.
- Um das Durchsuchen oder Importieren von Systemobjekten wie Tabellen, Ansichten, Synonymen, gespeicherten Prozeduren oder Funktionen aus einer relationalen Datenbank in Framework Manager zu ermöglichen, bearbeiten Sie den Eintrag für 'ImportDatabaseSystemObjects' in Ihrer `fm.ini`-Datei.

  Standardmäßig ist 'ImportDatabaseSystemObjects' auf 'FALSE' gesetzt. Benutzer können in den Dialogfeldern für den Import- und Ausdruckseditor nur die Benutzertabellen anzeigen. Um das Durchsuchen oder Importieren von Systemobjekten zu ermöglichen, setzen Sie die Vorgabe auf 'TRUE'.
- Richten Sie die Beispiele für IBMCognos Analytics und Framework Manager ein.

  Weitere Informationen finden Sie im Handbuch zur Installation und Konfiguration für Ihr IBM Cognos-Produkt.
- Richten Sie die IBM Cognos-Software für die Verwendung der Codebeispiele des Software Development Kits ein.

Weitere Informationen finden Sie in der Veröffentlichung *IBM Cognos Software Development Kit Developer Guide.*

- Richten Sie die IBM Cognos-Software für die Verwendung der Mashup-Servicebeispiele ein.

  Weitere Informationen finden Sie in der Veröffentlichung *IBM Cognos Mashup Service Developer Guide.*

Kapitel 13. Konfigurieren von Authentifizierungsprovidern

IBM Cognos-Komponenten werden mit zwei Zugriffsebenen ausgeführt: anonym und authentifiziert. Standardmäßig ist der anonyme Zugriff aktiviert.

Sie können in Ihrer Installation beide Anmeldearten verwenden. Wenn Sie nur die authentifizierte Anmeldung verwenden möchten, müssen Sie den anonymen Zugriff inaktivieren. Weitere Informationen finden Sie in Inaktivieren des anonymen Zugriffs.

Für die authentifizierte Anmeldung müssen Sie IBM Cognos Analytics-Komponenten mit einem Namespace konfigurieren, der für den Authentifizierungsprovider in Ihrer Umgebung geeignet ist. Sie können mehrere Namespaces für die Authentifizierung konfigurieren und anschließend bei der Ausführung bestimmen, welche Namespaces verwendet werden sollen. Weitere Informationen finden Sie im Handbuch *Verwaltung und Sicherheit*.

Wenn Sie von ReportNet aktualisiert haben und IBM Cognos einen Namespace gefunden hat, der nicht mehr konfiguriert ist, wird dieser in der Liste mit Authentifizierungsprovidern im Administrationsportal angezeigt. Wenn Sie die Benutzerkontoinformationen weiterhin benötigen, können Sie den Namespace konfigurieren. Andernfalls können Sie den Namespace löschen. Auch wenn Sie eine Aktualisierung von einer Version zur anderen durchführen, müssen Sie für beide Versionen dieselben Authentifizierungs-Namespaces verwenden. Andernfalls geht der Zugriff auf den alten gesicherten Inhalt verloren, weil die neue Version möglicherweise nicht dieselben Richtlinien, Benutzer, Rollen und Gruppen enthält.

IBM Cognos-Komponenten unterstützen die folgenden Typen von Servern als Authentifizierungsquellen:

- Active Directory Server
- OpenID Connect
- Benutzerdefinierter Java-Authentifizierungsprovider
- IBM Cognos Series 7-Namespace
- LDAP
- SiteMinder
- SAP

Wenn Sie mehrere Content Manager verwenden, müssen Sie in jedem Content Manager-Verzeichnis identische Authentifizierungsprovider konfigurieren. Das bedeutet, dass der ausgewählte Authentifizierungsprovider-Typ und dessen Konfiguration in allen Verzeichnissen für alle Plattformen übereinstimmen müssen. In der Konfiguration müssen Informationen enthalten sein, auf die von allen Content Managern zugegriffen werden kann.

Wenn IBM Cognos auf einem einzelnen Linux-basierten Computer oder Content Manager auf einem einzelnen Linux-basierten Computer installiert ist, kann IBM Cognos so konfiguriert werden, dass ausschließlich LDAP V3-kompatible Verzeichnisserver und benutzerdefinierte Provider als Authentifizierungsquellen verwendet werden.

Für einige Authentifizierungsprovider müssen Bibliotheken außerhalb der IBM Cognos-Umgebung zur Verfügung stehen. Wenn diese Bibliotheken unter Linux nicht zur Verfügung stehen, kann der Authentifizierungsprovider nicht initialisiert werden.

Wenn Sie eine der folgenden Quellen als Authentifizierungsquelle konfigurieren möchten, müssen Sie Content Manager unter einem Betriebssystem installieren, das von Content Manager unterstützt wird:

- IBM Cognos Series 7-Namespace (Windows, Solaris, AIX)
- Active Directory Server (nur Windows)
- SAP BW (alle mit Ausnahme von Power PC, z/OS, z/Linux)

Wenn Sie die Sicherheit aktivieren, müssen Sie die Sicherheitseinstellungen unmittelbar nach der Installation und Konfiguration einrichten. Weitere Informationen finden Sie im Handbuch *Verwaltung und Sicherheit*.

Wichtig: Nachdem Sie die Sicherheit aktiviert haben, inaktivieren Sie sie nicht mehr. Vorhandene Einstellungen für die Zugriffsberechtigungen werden weiterhin auf Benutzer, Gruppen oder Rollen weisen, die nicht mehr vorhanden sind. Dies hat zwar keine Auswirkungen auf die Funktion der Zugriffsberechtigungen, jedoch werden dem Benutzer, der die Berechtigungseinstellungen verwaltet, möglicherweise "unbekannte" Einträge angezeigt. Da diese Einträge auf Benutzer, Gruppen und Rollen verweisen, die nicht mehr existieren, können Sie sie einfach löschen. "Unbekannte" Einträge können jedoch auch angezeigt werden, wenn Sie nicht für alle Namespaces authentifiziert sind. In diesem Szenario dürfen Sie "unbekannte" Einträge nicht löschen.

Nach der Konfiguration eines Authentifizierungsproviders für IBM Cognos-Komponenten können Sie die Einzelanmeldung (Single Sign-on) zwischen der Umgebung Ihres Authentifizierungsproviders und IBM Cognos-Komponenten aktivieren. Dies bedeutet, dass sich die Benutzer anmelden und dann zu einer anderen Anwendung wechseln können, ohne sich erneut anmelden zu müssen.

Benutzer können bei der Anmeldung am IBM Cognos Analytics-Portal Namespaces auswählen. Sie können benutzerdefinierte Java-Namespaces und SiteMinder-Namespaces für Benutzer ausblenden. Weitere Informationen finden Sie im Abschnitt „Ausblenden des Namespace von Benutzern während der Anmeldung” auf Seite 275.

Inaktivierung der anonymen Anmeldung

Wenn Sie IBM Cognos Analytics nur für die authentifizierte Anmeldung konfigurieren möchten, müssen Sie den anonymen Zugriff auf die Anwendung inaktivieren.

Standardmäßig erfordern IBM Cognos-Komponenten keine Benutzerauthentifizierung. Benutzer können sich anonym anmelden.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf allen Computern, auf denen Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** > **Authentifizierung** auf **Cognos**.

   Der Cognos-Namespace enthält Informationen zu IBM Cognos-Gruppen, -Rollen, -Kontakten, Verteilerlisten usw. sowie Verweise auf Objekte in anderen Sicherheits-Namespaces.
3. Aktivieren Sie im Fenster **Eigenschaften** das Kontrollkästchen neben der Eigenschaft **Anonymen Zugriff zulassen**, und wählen Sie **Falsch**.
4. Klicken Sie im Menü **Datei** auf **Speichern**.

Ergebnisse

Sie müssen nun einen Namespace konfigurieren, damit Benutzer beim Zugriff auf IBM Cognos Analytics aufgefordert werden, Anmeldeberechtigungsnachweise einzugeben.

Beschränken des Benutzerzugriffs auf den Cognos-Namespace

Sie können den Zugriff auf IBM Cognos Analytics konfigurieren, dass nur Benutzer auf die Anwendung zugreifen können, die Mitglied einer beliebigen Gruppe oder Rolle im **Cognos**-Namespace sind.

Stellen Sie sicher, dass Sie Mitglied der integrierten Rolle **Systemadministratoren** im **Cognos**-Namespace sind, bevor Sie diese Konfiguration aktivieren.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf jedem Content Manager-Computer.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** auf **Authentifizierung**.

3. Ändern Sie im Fenster **Eigenschaften** den Wert unter **Zugriff auf Mitglieder des integrierten Namespace begrenzen** auf **Wahr**.
4. Klicken Sie im Menü **Datei** auf **Speichern**.

Nächste Schritte

Sie müssen nun die Gruppe **Jeder** aus bestimmten, in Cognos integrierten Gruppen und Rollen entfernen und sicherstellen, dass autorisierte Benutzer zu mindestens einer Cognos-Gruppe oder -Rolle gehören. Diese Tasks werden von Administratoren in den Cognos Analytics-Verwaltungsschnittstellen ausgeführt. Weitere Informationen finden Sie in den Publikationen *IBM Cognos Analytics-Handbuch für Verwaltung* oder *IBM Cognos Analytics-Handbuch für Administration und Sicherheit*.

Konfigurieren der Lightweight Third Party Authentication

Sie können IBM Cognos Analytics-Komponenten für die Verwendung von IBM Lightweight Third-Party Authentication (LTPA) konfigurieren. Die Verfahren, die in diesem Thema beschrieben werden, basieren auf einer verteilten Umgebung von Cognos Analytics 11.0.7 mit IBM Tivoli Directory Server LDAP oder Microsoft Active Directory als Authentifizierungsquellen.

Bei LTPA authentifiziert sich der Benutzer beim ersten Server, auf den zugegriffen wird, mit einem Benutzernamen und einem Passwort. Nach der Authentifizierung empfängt der Benutzer ein LTPA-Token, das lediglich für eine Sitzung gültig ist. Mithilfe des Tokens wird der Benutzer auf anderen Servern innerhalb desselben DNS (Domain Name System), in dem die Server zur Verwendung von LTPA konfiguriert sind, identifiziert. Daher gibt der Benutzer lediglich ein einziges Mal einen Benutzernamen und ein Kennwort ein und es wird auch nur ein einziges Mal auf das Benutzerverzeichnis zugegriffen, um die Identität dieses Benutzers zu überprüfen.

Um LTPA implementieren zu können, muss Cognos Analytics so konfiguriert sein, dass eine Authentifizierungsquelle verwendet wird, die in dem WebSphere Liberty-Container konfiguriert ist, in dem ihre Ausführung erfolgt. Sie können Single Sign-on zwischen Cognos Analytics und WebSphere Liberty konfigurieren, indem Sie die Identitätsabgleichskonfiguration im Cognos-Namespace verwenden. Beispiel: Sie können WebSphere Liberty so konfigurieren, dass ein LDAP- oder Active Directory-Server für die Authentifizierung verwendet wird. Anschließend können Sie Cognos Analytics so konfigurieren, dass derselbe LDAP- oder Active Directory-Server verwendet wird, und für den Identitätsabgleich REMOTE_USER festlegen.

Für Cognos Analytics bedeutet dies, dass ein Benutzer für eine Identität authentifiziert werden muss, die der HTTP-Sitzung zugewiesen ist, bevor innerhalb dieser Sitzung auf Cognos Analytics zugegriffen wird. Die Authentifizierung wird abgeschlossen, indem einem für Cognos externen Sicherheitssystem Berechtigungsnachweise vorgelegt werden. Das Sicherheitssystem kann die Identität und bestimmte Berechtigungsnachweisinformationen, mit denen Single Sign-on bei anderen Systemen möglich ist, bereitstellen. Dies erfolgt normalerweise in Form eines SSO-Tokens. Typische Kandidaten für solche Sicherheitssysteme sind Authentifizierungsproxys wie IBM Tivoli WebSEAL, Oracle Oblix, Site Minder oder andere Software- oder Hardware-Lösungen, die eine HTTP-Sitzung authentifizieren können und diese Authentifizierung in einem Token speichern (d. h. als persistent definieren) können.

WebSphere Liberty bietet zahlreiche verschiedene Optionen zur Benutzerauthentifizierung. Weitere Informationen finden Sie in der WebSphere Liberty-Dokumentation: https://www.ibm.com/support/knowledgecenter/en/SSD28V_8.5.5.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration auf einem Computer, auf dem der Cognos Analytics-Server installiert ist.
2. Erweitern Sie im Fenster mit dem **Explorer** die Kategorie **Umgebung** und anschließend die Kategorie **IBM Cognos-Services**.
3. Klicken Sie auf den Service **IBM Cognos**.
4. Klicken Sie im Fenster für Eigenschaften auf die Eigenschaft **IBM Lightweight Third Party Authentication (LTPA) aktivieren** und ändern Sie den Wert in **Wahr**.

5. Speichern Sie die Konfiguration und führen Sie einen Neustart für den Service **IBM Cognos** durch.
6. Wiederholen Sie diese Schritte auf allen Computern, auf denen der Cognos Analytics-Server installiert ist.

Nächste Schritte

Wenn LTPA verwendet werden soll, öffnen Sie die Datei `installationsposition/configuration/bi-services/bi-service.xml` und ändern Sie wie nachfolgend beschrieben die Angabe für den Sondersubjekttyp (`special subject type`) von `EVERYONE` in `ALL_AUTHENTICATED_USERS`:

```
<special-subject type="ALL_AUTHENTICATED_USERS"/>
```

Nehmen Sie diese Änderung auf allen Computern vor, auf denen Cognos Analytics-Server installiert sind.

Konfigurieren von LTPA mit einem LDAP-Namespace

Die folgende Prozedur beschreibt die Konfiguration von LTPA für Cognos Analytics, wenn LDAP von IBM Tivoli Directory Server als Authentifizierungsquelle verwendet wird.

Details zur LDAP-Konfiguration finden Sie in „Konfigurieren von IBM Cognos-Komponenten für die Verwendung von LDAP" auf Seite 280.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration an jeder Position, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** mit der rechten Maustaste auf **Authentifizierung** und klicken Sie anschließend auf **Neue Ressource** > **Namespace**.
3. Geben Sie im Feld **Name** einen Namen für den Authentifizierungsnamespace ein.
4. Wählen Sie in der Liste **Typ** die Option **LDAP – allgemeine Standardwerte** aus.
5. eben Sie im Fenster **Eigenschaften** für die Eigenschaft **Namespace-ID** eine eindeutige ID für den Namespace ein.
6. Geben Sie die folgenden Eigenschaften an:

   Host und Port
   Vollständig qualifizierter Host- und Portname des LDAP-Servers.

   Basis-DN
   Beispiel: `o=`*`Organisationsname`*`.com`

   Benutzersuche
   Beispiel: `uid=${userID},ou=people`

   Externe Identität verwenden
   `Wahr`

   Externer Identitätsabgleich
   Beispiel: `uid=${environment("REMOTE_USER")},ou=people`
7. Falls der LDAP-Authentifizierungsprovider mithilfe der Eigenschaft **Benutzer-DN und Kennwort für Bindung** eine Bindung zum Verzeichnisserver herstellen soll, wenn Sie Suchvorgänge durchführen, geben Sie diese Werte an.

   Wenn keine Werte angegeben werden, stellt der LDAP-Authentifizierungsprovider eine anonyme Bindung her.

   Wenn der externe Identitätsabgleich aktiviert ist, wird **Benutzer-DN und Kennwort für Bindung** grundsätzlich für den Zugriff auf LDAP verwendet. Wenn der externe Identitätsabgleich nicht aktiviert ist, wird die Option **Benutzer-DN und Kennwort für Bindung** nur verwendet, wenn für die Eigenschaft **Benutzersuche** ein Suchfilter angegeben ist. In diesem Fall werden, sobald der Benutzer-DN vorliegt, nachfolgende Anforderungen an den LDAP-Server unter dem Authentifizierungskontext des Benutzers ausgeführt.
8. Wenn Sie keinen externen Identitätsabgleich verwenden, suchen Sie mithilfe von Bindungsberechtigungsnachweisen nach dem LDAP-Verzeichnisserver, indem Sie die folgende Schritte ausführen:

- Stellen Sie sicher, dass für die Eigenschaft **Externe Identität verwenden** der Wert **False** festgelegt ist.
- Legen Sie für die Eigenschaft **Bindungsberechtigungsnachweise für die Suche verwenden** den Wert **True** fest.
- Geben Sie für **Benutzer-DN und Kennwort für Bindung** die Benutzer-ID und das Kennwort an.

Wenn Benutzer-ID und Kennwort nicht angeben werden und der anonyme Zugriff aktiviert ist, wird der Suchvorgang anonym ausgeführt.

9. Überprüfen Sie die Zuordnungseinstellungen für die erforderlichen Objekte und Attribute.

   Je nach LDAP-Konfiguration müssen Sie gegebenenfalls einige Standardwerte ändern, um eine erfolgreiche Kommunikation zwischen IBM Cognos-Komponenten und dem LDAP-Server sicherzustellen.

   Auf LDAP-Attribute, die in **Ordnerzuordnungen**, **Gruppenzuordnungen** oder **Kontozuordnungen** der Eigenschaft **Name** zugeordnet sind, müssen alle authentifizierten Benutzer zugreifen können. Die Eigenschaft **Name** darf außerdem nicht leer sein.
10. Klicken Sie im Menü **Datei** auf **Speichern**.
11. Erstellen Sie eine XML-Datei mit dem Namen `local-server.xml` und speichern Sie sie im Verzeichnis *Installationsposition*`/configuration`.
12. Geben Sie in der Datei `local-server.xml` die Werte ein, die der verwendeten Umgebung entsprechen:

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
    <featureManager>
        <feature>ldapRegistry-3.0</feature>
        <feature>appSecurity-2.0</feature>
    </featureManager>
    <ldapRegistry id="ID" realm="Realm"
        host="Host" port="Port" ignoreCase="true"
        baseDN="o=basedn" ldapType="Custom" sslEnabled="false">
        <idsFilters
            userFilter="(uid=%v,ou=people)"
            userIdMap="*:uid"
            groupFilter='(objectclass=groupofnames)'
            groupIdMap="*:cn" />
    </ldapRegistry>
      <webAppSecurity allowFailOverToBasicAuth="true" displayAuthenticationRealm="true"/>
</server>
```

13. Wenn Cognos Analytics für die Verwendung von SSL konfiguriert wird, finden Sie in „Konfigurieren des SSL-Protokolls für Cognos Analytics-Komponenten” auf Seite 208 weitere Informationen hierzu.
14. Melden Sie sich zur Verifizierung der Konfiguration bei `http://`*Host*`:`*Port*`/bi` bzw. für SSL-fähige Systeme bei `https://`*Host*`:`*Port*`/bi` an; dabei ist die Hostangabe die vollständig qualifizierte Hostdomäne von Cognos Analytics.

    Die Cognos Analytics-Anmeldeseite wird nicht angezeigt. Stattdessen werden Sie vom Browser zur Anmeldung aufgefordert.

Nächste Schritte

Wenn Sie Single Sign-on zwischen der Cognos Analytics-Anwendung, die mit LTPA-Authentifizierung eingerichtet wurde, und der Anwendung, die in einer WebSphere-Instanz bereitgestellt ist, konfigurieren möchten, installieren Sie den WebSphere-Schlüssel auf jedem Cognos Analytics-Dispatcher, auf dem LTPA eingerichtet wurde, und aktualisieren Sie die Datei `local-server.xml` mit dem folgenden Element `<ltpa>`:

```
<ltpa keysFileName="yourLTPAKeysFileName.keys"
keysPassword="keysPassword" expiration="120" />
```

Weitere Informationen finden Sie in der WebSphere Liberty-Dokumentation.

Konfigurieren von LTPA mit einem Active Directory-Namespace

Die folgende Prozedur beschreibt die Konfiguration von LTPA für Cognos Analytics, wenn Microsoft Active Directory als Authentifizierungsquelle verwendet wird.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration an jeder Position, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** mit der rechten Maustaste auf **Authentifizierung** und klicken Sie anschließend auf **Neue Ressource** > **Namespace**.
3. Geben Sie im Feld **Name** einen Namen für den Authentifizierungsnamespace ein.
4. Wählen Sie in der Liste **Typ** die Option **LDAP - Standardwerte für Active Directory** aus und klicken Sie dann auf **OK**.

   Die neue Authentifizierungsprovider-Ressource wird im Fenster **Explorer** unter der Komponente **Authentifizierung** angezeigt. Die Standardwerte werden vom Programm generiert. Überprüfen Sie sie und nehmen Sie bei Bedarf Änderungen vor.
5. Geben Sie im Fenster **Eigenschaften** für die Eigenschaft **Namespace-ID** eine eindeutige ID für den Namespace ein.

   Tipp: Verwenden Sie keine Doppelpunkte (:) in der Eigenschaft **Namespace-ID**.
6. Geben Sie die Werte für alle anderen erforderlichen Eigenschaften an, um sicherzustellen, dass IBM Cognos-Komponenten den vorhandenen Authentifizierungsprovider finden und verwenden können.
   - Für **Benutzersuche** geben Sie `(sAMAccountName=${`**`Benutzer-ID`**`})` ein.
   - Beim Single Sign-on setzen Sie den Wert für **Externe Identität verwenden** auf **Wahr**.
   - Beim Single Sign-on setzen Sie **Externer Identitätsabgleich** auf `(sAMAccountName=${environment("REMOTE_USER")})`.

     Wenn Sie den Domänennamen aus der Variablen REMOTE_USER entfernen möchten, geben Sie `(sAMAccountName=${replace(${environment("REMOTE_USER")}, "`**`Domäne`**`\\","")})` ein.

     Wichtig: Achten Sie darauf, nur die Variable REMOTE_USER zu verwenden. Die Verwendung einer anderen Variablen kann eine Sicherheitslücke verursachen.
   - Für **Benutzer-DN und Kennwort für Bindung** geben Sie **`Benutzer`@Domäne** ein.
   - Für **Eindeutige Identifizierung** geben Sie `objectGUID` ein.
7. Erstellen Sie eine XML-Datei mit dem Namen `local-server.xml` und speichern Sie sie im Verzeichnis *Installationsposition*`/configuration`.
8. Geben Sie in der Datei `local-server.xml` die Werte ein, die der verwendeten Umgebung entsprechen:

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
    <featureManager>
        <feature>ldapRegistry-3.0</feature>
        <feature>appSecurity-2.0</feature>
    </featureManager>
    <ldapRegistry id="ID" realm="Realm"
    host="Host" port="Port" ignoreCase="true"
    baseDN="DC=DC,DC=DC,DC=DC" bindDN="CN=doejohn,
            OU=Benutzer,DC=DC,DC=DC,DC=DC"
    bindPassword="password" ldapType="Microsoft Active Directory" sslEnabled="false">
        <actived Filters
            userFilter="(&amp;(sAMAccountName=%v)(objectcategory=user))"
            groupFilter="(&amp;(cn=%v)(objectcategory=group))"
            userIdMap="user:sAMAccountName"
            groupIdMap="*:cn"
            groupMemberIdMap="memberOf:member">
        </actived Filters>
    </ldapRegistry>
    <webAppSecurity allowFailOverToBasicAuth="true" displayAuthenticationRealm="true"/>
</server>
```

9. Wenn Cognos Analytics für die Verwendung von SSL konfiguriert wird, finden Sie in „Konfigurieren des SSL-Protokolls für Cognos Analytics-Komponenten” auf Seite 208 weitere Informationen hierzu.
10. Melden Sie sich zur Verifizierung der Konfiguration bei `http://Host:Port/bi` bzw. für SSL-fähige Systeme bei `https://Host:Port/bi` an; dabei ist die Hostangabe die vollständig qualifizierte Hostdomäne von Cognos Analytics.

    Die Cognos Analytics-Anmeldeseite wird nicht angezeigt. Stattdessen werden Sie vom Browser zur Anmeldung aufgefordert.

Nächste Schritte

Wenn Sie Single Sign-on zwischen der Cognos Analytics-Anwendung, die mit LTPA-Authentifizierung eingerichtet wurde, und der Anwendung, die in einer WebSphere-Instanz bereitgestellt ist, konfigurieren möchten, installieren Sie den WebSphere-Schlüssel auf jedem Cognos Analytics-Dispatcher, auf dem LTPA eingerichtet wurde, und aktualisieren Sie die Datei `local-server.xml` mit dem folgenden Element `<ltpa>`:

```
<ltpa keysFileName="yourLTPAKeysFileName.keys"
keysPassword="keysPassword" expiration="120" />
```

Weitere Informationen finden Sie in der WebSphere Liberty-Dokumentation. Das Stammverzeichnis der in diesem Dokument erwähnten automatisch generierten LTPA-Schlüsseldateidatei `${server.output.dir}/resources/security/ltpa.keys` lautet *position_von_cognos_analytics*`/wlp/usr/servers/cognosserver`.

Konfigurieren von IBM Cognos-Komponenten für die Verwendung von Active Directory Server

Wenn Sie Content Manager auf einem Computer unter einem Microsoft Windows-Betriebssystem installieren, können Sie einen Active Directory-Namespace als Authentifizierungsquelle konfigurieren.

Wenn Sie Content Manager auf einem UNIX-basierten Computer installieren, müssen Sie stattdessen einen LDAP-Namespace verwenden, um Active Directory als Authentifizierungsquelle zu konfigurieren. Wenn Sie Content Manager auf einer Kombination aus Windows- und UNIX-Computern installieren, müssen Sie Active Directory für alle Content Manager mithilfe eines LDAP-Namespace konfigurieren. Wenn Sie einen LDAP-Namespace zur Authentifizierung beim Active Directory Server verwenden, stehen Ihnen nur LDAP-Funktionen zur Verfügung. Sie haben keinen Zugriff auf Active Directory-Funktionen, z. B. erweiterte Eigenschaften für Domänen und Einzelanmeldung mit der Kerberos-Delegierung.

Wenn Sie Content Manager auf einem Linux-basierten Computer installieren, gelten dieselben Einschränkungen wie für UNIX. Sie müssen einen LDAP-Namespace verwenden, um Active Directory als Ihre Authentifizierungsquelle zu konfigurieren.

Wenn Sie Microsoft SQL Server oder Microsoft Analysis Server als Datenquelle für die Einzelanmeldung zum Authentifizieren verwenden möchten, müssen Sie Active Directory als Authentifizierungsquelle verwenden.

Sie können keine Verbindung zum globalen Katalog von Active Directory herstellen. Der globale Katalog ist ein Caching-Server für Active Directory Server. Wenn für die Verbindung Port 3268 verwendet wird, müssen Sie diese Einstellung ändern. In der Standardeinstellung verwendet Active Directory Server Port 389.

Vorgehensweise

1. Konfigurieren Sie IBM Cognos-Komponenten für die Verwendung mit einem Active Directory Server-Namespace.
2. Aktivieren Sie gegebenenfalls die sichere Kommunikation mit dem Active Directory Server.
3. Aktivieren Sie die Einzelanmeldung zwischen Active Directory und IBM Cognos-Komponenten.

Konfigurieren eines Active Directory-Namespace

Sie können Active Directory Server als Authentifizierungsprovider verwenden.

Sie können auch angepasste Benutzereigenschaften von Active Directory Server in IBM Cognos-Komponenten zur Verfügung stellen.

Vorbereitende Schritte

Damit IBM Cognos ordnungsgemäß mit Active Directory Server funktioniert, müssen Sie sicherstellen, dass die Gruppe 'Authentifizierte Benutzer' über eine Leseberechtigung für den Active Directory-Ordner verfügt, in dem die Benutzer gespeichert sind.

Wenn Sie einen Active Directory-Namespace konfigurieren, um das Single Sign-on mit der Datenquelle Microsoft SQL Server oder Microsoft Analysis Server zu unterstützen, ist folgende Konfiguration erforderlich:

- IBM Cognos Gateway muss auf einem IIS-Web-Server installiert sein, der für die integrierte Authentifizierung unter dem Microsoft Windows-Betriebssystem konfiguriert ist.
- Das Gateway muss im Web-Browser der lokalen Intranet-Website zugewiesen sein.
- Content Manager muss auf einem Server unter Windows 2008 oder Windows 2012 installiert sein.
- Content Manager, Komponenten der Anwendungsebene, der IIS-Web-Server und der Datenquellenserver (Microsoft SQL Server oder Microsoft Analysis Server) müssen der Active Directory-Domäne angehören.
- Die Datenquellenverbindung für Microsoft SQL Server oder Microsoft Analysis Server muss für **Externer Namespace** konfiguriert sein und dieser Namespace muss der Active Directory-Namespace sein.

Weitere Informationen zu Datenquellen finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration an jeder Position, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** mit der rechten Maustaste auf **Authentifizierung** und klicken Sie anschließend auf **Neue Ressource** > **Namespace**.
3. Geben Sie im Feld **Name** einen Namen für den Authentifizierungsnamespace ein.
4. Klicken Sie in der Liste **Typ** auf den entsprechenden Namespace und anschließend auf **OK**.

   Die neue Authentifizierungsprovider-Ressource wird im Fenster **Explorer** unter der Komponente **Authentifizierung** angezeigt.
5. eben Sie im Fenster **Eigenschaften** für die Eigenschaft **Namespace-ID** eine eindeutige ID für den Namespace ein.
6. Geben Sie die Werte für alle anderen erforderlichen Eigenschaften an, um sicherzustellen, dass IBM Cognos-Komponenten den vorhandenen Authentifizierungsprovider lokalisieren und verwenden können.
7. Geben Sie die Werte für die Eigenschaft **Host und Port** an.

   Um den Ausfallschutz für Active Directory Server zu unterstützen, können Sie den Domänennamen anstelle eines bestimmten Domänencontrollers angeben.

   Verwenden Sie beispielsweise '*meineDomäne*.com:389' anstelle von 'dc1.*meineDomäne*.com:389'.
8. Wenn die Authentifizierung fehlschlägt, können Sie Ihre Benutzer-ID und das Kennwort für die Eigenschaft **Bindungsberechtigungsnachweise** angeben, um nach weiteren Informationen zu suchen.

   Verwenden Sie die Berechtigungsnachweise eines Active Directory Server-Benutzers, der über Such- und Lesezugriff für diesen Server verfügt.
9. Klicken Sie im Menü **Datei** auf **Speichern**.

10. Testen Sie die Verbindung zu einem neuen Namespace. Klicken Sie im Fenster **Explorer** unter **Authentifizierung** mit der rechten Maustaste auf die neue Authentifizierungsressource und klicken Sie auf **Test**.

    Sie werden dazu aufgefordert, die Berechtigungsnachweise für einen Benutzer im Namespace einzugeben, um den Test auszuführen.

    Abhängig von der Konfiguration des Namespace können Sie entweder eine gültige Benutzer-ID und ein gültiges Kennwort für einen Benutzer im Namespace eingeben oder den Wert der Eigenschaft 'Benutzer-DN und Kennwort für Bindung'.

Ergebnisse

IBM Cognos lädt, initialisiert und konfiguriert die Providerbibliotheken für den Namespace.

Bereitstellen von benutzerdefinierten Active Directory-Benutzereigenschaften für IBM Cognos-Komponenten

In IBM Cognos-Komponenten können Sie beliebige Benutzerattribute von Active Directory Server verwenden. Zur entsprechenden Konfiguration sind diese Attribute als benutzerdefinierte Eigenschaften für den Active Directory-Namespace hinzuzufügen.

Die benutzerdefinierten Eigenschaften stehen als Sitzungsparameter über Framework Manager zur Verfügung. Weitere Informationen zu Sitzungsparametern finden Sie im *Framework Manager User Guide*.

Sie können auch die benutzerdefinierten Eigenschaften innerhalb von Befehlsblöcken verwenden, um Oracle-Sitzungen und -Verbindungen zu konfigurieren. Sie können die Befehlsblöcke mit leichten Verbindungen und virtuellen privaten Datenbanken von Oracle verwenden. Weitere Informationen finden Sie in der Veröffentlichung *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration an jeder Position, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** > **Authentifizierung** auf den Active Directory-Namespace.
3. Klicken Sie im Fenster **Eigenschaften** unter **Benutzerdefinierte Eigenschaften** auf die Spalte **Wert** und klicken Sie anschließend auf das Symbol **Bearbeiten**.
4. Klicken Sie im Fenster **Wert - Benutzerdefinierte Eigenschaften** auf **Hinzufügen**.
5. Klicken Sie auf die Spalte **Name** und geben Sie den Namen ein, der von den IBM Cognos-Komponenten als Sitzungsparameter verwendet werden soll.
6. Klicken Sie auf die Spalte **Wert** und geben Sie den Namen des Kontoparameters in Active Directory Server ein.
7. Wiederholen Sie die Schritte 4 bis 6 für jeden benutzerdefinierten Parameter.
8. Klicken Sie auf **OK**.
9. Klicken Sie im Menü **Datei** auf **Speichern**.

Aktivieren der sicheren Kommunikation mit dem Active Directory Server

Wenn Sie eine SSL-Verbindung zum Active Directory Server verwenden, müssen Sie das Zertifikat vom Active Directory Server in das Content Manager-Verzeichnis kopieren.

Vorgehensweise

1. Stellen Sie in jedem Content Manager-Verzeichnis über den Web-Browser eine Verbindung mit dem Active Directory Server her und kopieren Sie das CA Root-Zertifikat in das Content Manager-Verzeichnis.

2. Fügen Sie das CA Root-Zertifikat zum Zertifikatspeicher für das Konto hinzu, das Sie für die aktuelle IBM Cognos-Sitzung verwenden:
   - Wenn Sie die IBM Cognos-Sitzung unter einem Benutzerkonto ausführen, verwenden Sie den Web-Browser aus Schritt 1, um das CA Root-Zertifikat in den Zertifikatspeicher für das Benutzerkonto zu importieren.

     Informationen hierzu finden Sie in der Dokumentation für den Web-Browser.
   - Wenn Sie die IBM Cognos-Sitzung unter dem lokalen Konto ausführen, importieren Sie das CA Root-Zertifikat mithilfe von Microsoft Management Console (MMC) in den Zertifikatspeicher für den lokalen Computer.

     Informationen hierzu finden Sie in der Dokumentation für MMC.
3. Starten Sie in IBM Cognos Configuration den Service neu:
   - Klicken Sie im Fenster **Explorer** auf **IBM Cognos-Services** > **IBM Cognos**.
   - Klicken Sie im Menü **Aktionen** auf **Neustart**.

Ein- oder Ausschließen von Domänen, die erweiterte Eigenschaften verwenden

Wenn Sie einen Authentifizierungs-Namespace für IBM Cognos konfigurieren, können sich nur Benutzer aus einer Domäne anmelden. Mithilfe von erweiterten Eigenschaften für Active Directory Server können sich auch Benutzer aus verwandten Domänen (Über- und Unterordnung) und nicht verwandten Domänenstrukturen innerhalb derselben Gesamtstruktur anmelden. Gesamtstrukturübergreifende Unterstützung besteht nicht; für jede Gesamtstruktur muss ein separater Namespace vorhanden sein.

Wenn Sie den Parameter "chaseReferrals" auf "wahr" festlegen, können sich Benutzer in der ursprünglich authentifizierten Domäne und allen untergeordneten Domänen der Domänenstruktur bei IBM Cognos anmelden. Benutzer in Domänen, die der ursprünglich authentifizierten Domäne übergeordnet sind oder sich in einer anderen Domänenstruktur befinden, können sich nicht anmelden.

Wenn Sie den Parameter "MultiDomainTrees" auf "wahr" festlegen, können sich Benutzer in allen Domänenstrukturen in der Gesamtstruktur bei IBM Cognos anmelden.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration an jeder Position, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** > **Authentifizierung** auf den Active Directory-Namespace.
3. Legen Sie im Fenster **Eigenschaften** die Eigenschaft **Host und Port** fest:
   - Geben Sie für Benutzer in einer Domäne den Host und den Port eines Domänencontrollers für die einzelne Domäne an.
   - Geben Sie für Benutzer in einer Domänenstruktur den Host und den Port des Controllers auf der obersten Ebene für die Domänenstruktur an.
   - Geben Sie für Benutzer in allen Domänenstrukturen in der Gesamtstruktur den Host und den Port eines beliebigen Controllers in der Gesamtstruktur an.
4. Klicken Sie auf die Spalte **Wert** für **Erweiterte Eigenschaften** und klicken Sie auf das Symbol **Bearbeiten**.
5. Klicken Sie im Fenster **Wert - Erweiterte Eigenschaften** auf **Hinzufügen**.
6. Definieren Sie zwei neue Eigenschaften, **chaseReferrals** und **MultiDomainTrees**, mit den Werten aus der folgenden Tabelle:

Tabelle 36. Einstellungen für erweiterte Eigenschaften		
Authentifizierung für	**chaseReferrals**	**MultiDomainTrees**
Eine Domäne	Falsch	Falsch
Eine Domänenstruktur	Wahr	Falsch
Alle Domänenstrukturen in der Gesamtstruktur	Wahr	Wahr

7. Klicken Sie auf **OK**.
8. Klicken Sie im Menü **Datei** auf **Speichern**.

Aktivieren der Einzelanmeldung zwischen Active Directory Server und IBM Cognos-Komponenten

Standardmäßig verwendet der Active Directory-Provider die Kerberos-Authentifizierung. Er ermöglicht die Integration mit dem Microsoft IIS-Web-Server (IIS = Internet Information Services) für die Einzelanmeldung (Single Sign-on), wenn die Windows-Authentifizierung (früher als NT Challenge Response(Anfrage/Antwort) bezeichnet) auf dem IIS-Web-Server aktiviert ist.

Bei Aktivierung der Windows-Authentifizierung werden Sie nicht dazu aufgefordert, die Authentifizierungsinformationen erneut einzugeben, wenn Sie auf IBM Cognos-Inhalte zugreifen, die durch den Active Directory-Namespace gesichert sind.

Bei Verwendung der Kerberos-Authentifizierung können Sie auch "Service for User" (S4U) auswählen. S4U ermöglicht auch den Zugriff auf IBM Cognos Analytics von Computern außerhalb der Active Directory-Domäne. Zur Aktivierung von S4U müssen Sie die eingeschränkte Delegierung aktivieren.

Die Computer einiger Ihrer Benutzer gehören nicht zur Domäne, die Benutzer kennen aber das Domänenkonto. Beim Öffnen der Web-Browser auf diesen Computern wird das Domänenkonto angefordert. Die Benutzer erhalten das Kerberos-Ticket jedoch nur mit der Berechtigung "Identität", weshalb sie sich nicht bei IBM Cognos Analytics authentifizieren können. Zur Lösung dieses Problems können Sie S4U verwenden.

Wenn Sie keine Kerberos-Authentifizierung wünschen, können Sie den Provider so konfigurieren, dass er für die Einzelanmeldung auf die Umgebungsvariable **REMOTE_USER** zugreift.

Wichtig: Achten Sie darauf, nur die Variable **REMOTE_USER** zu verwenden. Die Verwendung einer anderen Variablen kann eine Sicherheitslücke verursachen.

Zur Einrichtung der Einzelanmeldung, so dass diese die Kerberos-Authentifizierung verwendet, müssen Sie die folgenden Aufgaben ausführen:

1. Konfigurieren Sie die Windows-Authentifizierung auf dem Microsoft IIS-Web-Server für die 'ibmcognos/cgi-bin'-Anwendung.
2. Installieren Sie den aktiven und die Standby-Content Manager auf Computern innerhalb der Active Directory-Domäne.
3. Richten Sie die Computer oder das Benutzerkonto, unter dem Content Manager ausgeführt wird, als vertrauenswürdig ein.

Weitere Informationen finden Sie in den folgenden Dokumenten mit technischen Hinweisen (Technotes):

- Enabling single sign-on to CRN or Cognos secured against Active Directory (www.ibm.com/support/docview.wss?uid=swg21341889)
- When using Kerberos Single Sign-on (SSO) with Active Directory in Cognos, user is prompted for credentials (www.ibm.com/support/docview.wss?uid=swg21659267)

Aktivieren der Einzelanmeldung zwischen Active Directory Server und IBM Cognos-Komponenten mit REMOTE_USER

Wenn Sie keine Kerberos-Authentifizierung wünschen, können Sie den Provider so konfigurieren, dass er für die Einzelanmeldung auf die Umgebungsvariable **REMOTE_USER** zugreift.

Sie müssen die erweiterte Eigenschaft **singleSignonOption** auf den Wert **IdentityMapping** setzen. Darüber hinaus müssen Sie Bindungsberechtigungsnachweise für den Active Directory-Namespace festlegen.

Microsoft IIS legt **REMOTE_USER** standardmäßig bei der Aktivierung der Windows-Authentifizierung fest. Ohne Kerberos-Authentifizierung sind keine Einzelanmeldungen bei Microsoft OLAP (MSAS)-Datenquellen möglich.

Bei der Definition von **REMOTE_USER** können Sie **REMOTE_USER** auch als vertrauenswürdigen Berechtigungsnachweis speichern. Dies bedeutet, dass geplante Jobs den **REMOTE_USER** mit den Berechtigungen der **Bindungsberechtigungsnachweise** authentifizieren.

Wichtig: Achten Sie darauf, nur die Variable **REMOTE_USER** zu verwenden. Eine andere Variable kann zu einer Sicherheitslücke führen.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration auf dem Computer, auf dem Content Manager installiert ist.
2. Wählen Sie im Fenster **Explorer** unter **Sicherheit** > **Authentifizierung** den Active Directory-Namespace aus.
3. Klicken Sie auf die Spalte **Wert** für **Erweiterte Eigenschaften** und klicken Sie auf das Bearbeitungssymbol.
4. Klicken Sie im Dialogfeld **Wert - Erweiterte Eigenschaften** auf **Hinzufügen**.
5. Geben Sie in der Spalte **Name** Folgendes ein: `singleSignonOption`
6. Geben Sie in der Spalte **Wert** die Angabe `IdentityMapping` ein.
7. Wenn Sie REMOTE_USER als vertrauenswürdigen Berechtigungsnachweis speichern möchten, klicken Sie im Dialogfeld **Wert - Erweiterte Eigenschaften** auf **Hinzufügen**.
8. Geben Sie in der Spalte **Name** `trustedCredentialType` ein.
9. Geben Sie in der Spalte **Wert** `IdentityMappingForTC` ein.
10. Klicken Sie auf **OK**.
11. Klicken Sie in die Spalte **Wert** für **Bindungsberechtigungsnachweise** und klicken Sie auf das Bearbeitungssymbol.
12. Geben Sie im Dialogfeld **Wert - Bindungsberechtigungsnachweise** eine Benutzer-ID und das entsprechende Kennwort ein und klicken Sie anschließend auf **OK**.

Aktivieren der Einzelanmeldung mit Kerberos-Authentifizierung

Wenn Ihr IIS-Web-Server für die Windows-Authentifizierung konfiguriert ist, sind keine weiteren Einstellungen erforderlich. Die Kerberos-Authentifizierung wird in diesem Fall standardmäßig verwendet.

Aktivieren der Einzelanmeldung mit Kerberos-Authentifizierung und eingeschränkter Delegierung

Zur Verwendung der eingeschränkten Delegierung müssen Sie für diejenigen Benutzer, die die IBM Cognos-Komponenten ausführen dürfen, Dienstprinzipalnamen (Service Principal Names, SPNs) definieren. Des Weiteren müssen Sie den Anwendungspool Ihres Microsoft Internet Information Services (IIS)-Web-Servers in Ihrer Active Directory-Domäne konfigurieren.

Bei Verwendung von Kerberos mit eingeschränkter Delegierung müssen Sie bei der Konfiguration Ihres Gateways einen Benutzer des Typs **sAMAccountName** für Content Manager hinzufügen. Alle aktiven und Standby-Content Manager müssen unter demselben Konto ausgeführt werden.

Bei der Konfiguration der Einzelanmeldung für Ihre Datenbankserver müssen Sie beim Hinzufügen des Active Directory-Namespace **sAMAccountName** für den Benutzer konfigurieren, der die Komponenten der Anwendungsebene ausführt. Alle Komponenten der Anwendungsebene müssen unter demselben Konto ausgeführt werden.

Bei den SPNs handelt es sich um die Benutzer, die Sie in IBM Cognos Configuration in den Feldern des Typs **sAMAccountName** eingeben.

Angenommen, Sie haben einen Benutzer, der Content Manager ausführt, einen weiteren, der die Komponenten der Anwendungsebene ausführt, und wieder einen anderen Benutzer, der den Anwendungspool des Web-Servers ausführt. Der Content Manager-Benutzer heißt `CognosCMUser`. Der Benutzer der Komponenten der Anwendungsebene heißt `CognosATCUser`. Der Benutzer des Anwendungspools heißt `IISUser`. Alle diese Benutzer gehören zur Domäne `MyDomain`.

1. Sie müssen IIS so einrichten, dass `MyDomain\IISUser` die Identität des Anwendungspools ist.
2. Führen Sie den Befehl `setspn` für den Computer aus, auf dem IIS ausgeführt wird.

   Beispiel:

   ```
   setspn -A http/IISServerName MyDomain\IISUser
   setspn -A http/IISServerName.MyDomain.com MyDomain\IISUser
   ```

3. Führen Sie den Befehl `setspn` für Ihre IBM Cognos-Benutzer aus.

   Beispiel:

   ```
   setspn -A ibmcognosba/CognosCMUser MyDomain\CognosCMUser
   setspn -A ibmcognosba/CognosATCUser MyDomain\CognosATCUser
   ```

   In diesen Befehlen müssen Sie `ibmcognosba` wie in den Beispielen gezeigt verwenden. Die Benutzernamen und Domänen müssen Ihrer Umgebung entsprechen.

   Anmerkung: In diesem Beispiel müssen Sie als **sAMAccountName**-Benutzer `CognosCMUser` und `CognosATCUser` eingeben.
4. Wenn Sie die Einzelanmeldung für Ihren Microsoft SQL Server- oder Microsoft SQL Server Analysis Services-Datenbankserver konfigurieren, müssen Sie den SPN für den Datenbankserver einrichten. Weitere Informationen finden Sie in der Dokumentation Ihres Datenbankservers.
5. Schließlich müssen Sie die eingeschränkte Delegierung im Verwaltungstool Active Directory-Benutzer und -Computer konfigurieren. Hierzu wählen Sie auf der Registerkarte **Delegierung** für alle Benutzer (`IISUser`, `CognosCMUser` und `CognosATCUser`) **Computer bei Delegierungen angegebener Dienste vertrauen** und **Nur Kerberos verwenden** aus, um Kerberos mit eingeschränkter Delegierung zu verwenden. Wenn Sie die Kerberos-Erweiterung S4U verwenden, wählen Sie **Computer bei Delegierungen angegebener Dienste vertrauen** und **Beliebiges Authentifizierungsprotokoll verwenden** aus.

   Danach müssen Sie die erforderlichen SPNs hinzufügen. Fügen Sie zum Beispiel `ibmcognosba` als Servicetyp hinzu. Fügen Sie des Weiteren `DomainController1` und `DomainController2` als `ldap` des Servicetyps hinzu.

   Wenn Sie Single Sign-on für die Datenquelle konfigurieren, fügen Sie den Service MSQLSVC hinzu.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration auf dem Computer, auf dem Content Manager installiert ist.
2. Wählen Sie im Fenster **Explorer** unter **Sicherheit** > **Authentifizierung** den Active Directory-Namespace aus.
3. Klicken Sie auf die Spalte **Wert** für **Erweiterte Eigenschaften** und klicken Sie auf das Bearbeitungssymbol.
4. Klicken Sie im Dialogfeld **Wert - Erweiterte Eigenschaften** auf **Hinzufügen**.
5. Geben Sie in der Spalte **Name** `singleSignonOption` ein.
6. Geben Sie in der Spalte **Wert** einen der folgenden Werte ein:

- `KerberosS4UAuthentication`, wenn zuerst die Kerberos-Authentifizierung verwendet werden soll. Schlägt Kerberos fehl, wird die Authentifizierung mit "Service For User" (S4U) versucht. Schlägt S4U fehl, wird der Benutzer nach seinen Berechtigungsnachweisen gefragt.
- `S4UAuthentication`, wenn zuerst die S4U-Authentifizierung verwendet werden soll. Schlägt S4U fehl, wird der Benutzer nach seinen Berechtigungsnachweisen gefragt.

7. Klicken Sie im Dialogfeld **Wert - Erweiterte Eigenschaften** auf **Hinzufügen**.
8. Geben Sie in der Spalte **Name** `trustedCredentialType` ein.
9. Geben Sie in der Spalte **Wert** einen der folgenden Werte ein:
   - `CredentialForTC`, wenn die Berechtigungsnachweise des Benutzers als vertrauenswürdige Berechtigungsnachweise gespeichert werden sollen. Dies empfiehlt sich zum Beispiel, wenn mit diesen Berechtigungsnachweisen geplante Jobs ausgeführt werden sollen.
   - `S4UForTC`, wenn nur der authentifizierte Benutzername als vertrauenswürdiger Berechtigungsnachweis gespeichert werden soll. Der Benutzername wird im UPN-Format gespeichert. In diesem Format können geplante Jobs allein über den Benutzernamen ausgeführt werden, eine Kennworteingabe ist nicht erforderlich.
10. Klicken Sie auf **OK**.
11. Klicken Sie für **Komponenten der Anwendungsebene - sAMAccountName** in die Spalte **Wert** und geben Sie den **sAMAccountName** des Benutzers ein, der die Komponenten der Anwendungsebene ausführt.

    Wichtig: Dieser Wert ist nur erforderlich, wenn Sie Single Sign-on für Microsoft SQL Server konfigurieren. Andernfalls sollten Sie diesen Wert nicht ändern.
12. Klicken Sie auf **Datei** > **Speichern**.
13. Starten Sie den IBM Cognos-Service neu.
14. Öffnen Sie IBM Cognos Configuration auf dem Computer, auf dem die Gateway-Komponenten installiert sind.
15. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
16. Klicken Sie für **Content Manager-sAMAccountName** in die Spalte **Wert** und geben Sie den **sAMAccountName** des Benutzers ein, der Content Manager ausführt.
17. Klicken Sie auf **Datei** > **Speichern**.

OpenID Connect-Authentifizierungsprovider

OpenID Connect ist eine einfach Identitätsschicht über Ihrem OAuth 2.0-Protokoll. Sie wird mit vielen Anwendungen, die denselben Identitätsprovider verwenden, für eine eingebundene Identität und Authentifizierung verwendet. OpenID Connect ist der bevorzugte webbasierte Authentifizierungsprovider, wenn Sie IBM Cognos Analytics in andere Anwendungen einbinden möchten.

OpenID Connect ist ein moderner Standard, der die Standards OpenID und OAuth 2.0 enthält. Es wird für lokale und für Cloud-Installationen von Cognos Analytics unterstützt.

Cognos Analytics unterstützt folgende Typen von OpenID Connect-Identitätsprovidern:

- ADFS (Active Directory Federation Services)
- Azure AD (Active Directory)
- Generic
- Google
- IBM Cloud Identity
- IBMid (IBM Identitätsprovider)
- MS Identity
- OKTA
- Ping

- SalesForce
- SiteMinder

Tipp: Wenden Sie sich an den für den Identitätsprovider zuständigen Administrator in Ihrem Unternehmen oder an die Vertriebs- und Unterstützungsorganisation, um zu erfahren, welche Produktversion Sie verwenden sollten.

Konfigurieren eines OpenID Connect-Namespace

Um einen OpenID Connect-Identitätsprovider mit IBM Cognos Analytics zu verwenden, müssen Sie einen OpenID Connect-Namespace konfigurieren.

Wenn Sie IBMid als Ihren OpenID Connect-Identitätsprovider verwenden, finden Sie weitere Informationen dazu in Verwalten von OpenID Connect-Namespaces.

Wenn Benutzer nach der erfolgreichen Konfiguration des OpenID Connect-Namespace Probleme haben, können Sie die Protokollierung zu Diagnosezwecken in der Komponente **Verwalten** von Cognos Analytics verwenden, um Fehler zu beheben. Sie müssen ein neues Protokollierungstopic erstellen, dass auf dem vordefinierten Topic **AAA** basiert. Ändern Sie das Protokollierungstopic **AAA**, indem Sie dem Topic den folgenden Code hinzufügen:

```
{
"loggerDefinitions": [
{
"loggerName": "com.ibm.cognos.camaaa.internal.OIDC",
"level": "DEBUG",
"additivity": true
}
],
"topicName": "OIDC"
}
```

Weitere Informationen zur Protokollierung zu Diagnosezwecken finden Sie in Protokollierungstypen und -dateien.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration auf Ihrem Content Manager-Manager.
2. Unter **Sicherheit** > **Authentifizierung** klicken Sie mit der rechten Maustaste auf **Neue Ressource** > **Namespace** und wählen diese aus.
3. Wählen Sie als **Typ** (Gruppe) die Möglichkeit **OpenID Connect** aus.
4. Wählen Sie als **Typ** einen der Identitätsprovider in der Dropdown-Liste aus, in der die unterstützten Identitätsprovider enthalten sind.
5. Geben Sie den Namespace-Namen in das Feld **Name** ein und klicken Sie anschließend auf **OK**.

   Der neue Namespace wird im Fenster **Explorer** unter **Sicherheit** > **Authentifizierung** hinzugefügt und seine Eigenschaften werden im Fenster 'Eigenschaften' angezeigt.
6. Geben Sie Werte für die Namespace-Eigenschaften an.

   Tipp: Informationen zu den einzelnen Eigenschaften werden in der Benutzerschnittstelle angezeigt, wenn Sie auf die Eigenschaft klicken.

   - Die **Namespace-ID** wird in der CAMID verwendet.
   - Geben Sie für **Erkennungsendpunkt**, **Client-ID** und **Geheimer Clientschlüssel für OpenID Connect** die von Ihrem OpenID Connect-Administrator vorgeschlagenen Werte an.
   - Wenn Sie einen Forward Proxy verwenden, um einen Tunnel zwischen Cognos Analytics und dem OIDC-Namespace zu konfigurieren,

     a. Wählen Sie **Erweiterte Eigenschaften** aus und klicken Sie dann auf das Bearbeitungssymbol .

     b. Legen Sie das folgende Name/Wert-Paar fest:

     – Name: `https_proxy`

– Wert: *proxy_server*:*port*

Dabei steht *proxy_server* für den vollständig qualifizierten Namen des Proxy-Servers

c. Klicken Sie mit der rechten Maustaste auf den Namespace und wählen Sie **Test** aus, um die ordnungsgemäße Funktionsweise des Namespace zu überprüfen.

d. Vergewissern Sie sich, dass der Cognos Analytics-Server eine Tunnelung über den Proxy verwendet:

– Stoppen Sie den Service auf dem Proxy-Server.

– Klicken Sie auf den Namespace und wählen Sie **Test** aus.

Der Test sollte fehlschlagen, da die Tunnelung inaktiviert ist.

- Aktualisieren Sie die **Rückgabe-URL** wie im folgenden Beispiel gezeigt mit der URL Ihres Gateways oder mit der Dispatcher URL:

  `http://meineFirma:9300/bi/completeAuth.jsp`

  Wenn Sie in Ihrer Umgebung eine Lastausgleichsfunktion verwenden, schließen Sie den DNS-Eintrag für die Lastausgleichsfunktion in der **>Rückgabe-URL** wie im folgenden Beispiel gezeigt vor dem Gateway oder den Dispatcherknoten ein:

  `https://MeinLastausgleichsfunktions-DNS.meineFirma.com:443/ibmcognos/bi/completeAuth.jsp`

  In diesem Beispiel wird das Gateway für Cognos Analytics auf dem Web-Server installiert.

  Wenn Sie hinter der Lastausgleichsfunktion eine Gruppe von Dispatcherknoten verwenden, auf denen das Cognos Analytics-Gateway nicht auf dem Web-Server installiert ist, sieht die **Rückgabe-URL** möglicherweise wie folgt aus:

  `https://MeinLastausgleichsfunktions-DNS.mycompany.com:9300/bi/completeAuth.jsp`

Tipp: Die Eigenschaften für die **Multi-Tenant-Funktionalität** müssen nicht jetzt angegeben werden.

7. Importieren Sie das Zertifikat der OpenID Connect-Stammzertifizierungsstelle in den Cognos Analytics-Keystore, indem Sie das Drittanbieter-Zertifikat-Tool verwenden.

   - Geben Sie auf UNIX- oder Linux-Betriebssystemen Folgendes ein: `ThirdPartyCertificateTool.sh -i -T -r Zertifikat.cer -p` **`NoPassWordSet`**
   - Geben Sie auf Windows-Betriebssystemen Folgendes ein: `ThirdPartyCertificateTool.bat -i -T -r Zertifikat.cer -p` **`NoPassWordSet`**

   Tipp: Ersetzen Sie die Variable *Zertifikat* durch den Namen der Zertifikatsdatei, die von Ihrem OpenID Connect-Identitätsprovider verwendet wird. Für IBMid lautet der Dateiname `blueid.cer`.

   Der Befehl verwendet das angegebene Kennwort und importierte den Inhalt in die Datei `CAMKeystore` im Verzeichnis `certs`.

8. Führen Sie dieselben Konfigurationsschritte auf Ihrem Content Manager-Sicherungscomputer aus.
9. Starten Sie den IBM Cognos-Service auf den Content Manager-Computern und den Content Manager-Sicherungscomputern.

Ergebnisse

Alle Benutzer, die über Ihren OpenID Connect-Identitätsprovider registriert sind, sollten nun Zugriff auf Cognos Analytics haben.

OIDC-Providertyp 'IBMid'

IBMid ist der IBM OpenID Connect-Identitätsprovider. Wenn Ihr Identitätsprovider (IdP – Identity Provider) OpenID Connect nicht unterstützt, jedoch SAML 2.0 unterstützt, können Sie IBMid verwenden, um in Cognos Analytics einen OpenID Connect-Namespace als Ihren Authentifizierungsprovider zu konfigurieren.

Anmerkung: Sie können den Wert 'IBMid' nur als OIDC-Providertyp verwenden, wenn Ihr Identitätsprovider nicht bereits bei einem anderen Identitätsprovider eingebunden ist. Wenn Ihr Identitätsprovider bereits eingebunden ist, müssen Sie beim Erstellen Ihres Namespace den generischen Typ in Cognos Configuration auswählen.

Mit dieser Namespacekonfiguration können Sie Cognos Analytics mit den meisten SAML 2.0-Authentifizierungsprovidern einbinden. Als Ergebnis werden Benutzer, die sich bei Cognos Analytics anmelden, auf die IBMid-Anmeldeseite weitergeleitet, wenn sie ihre E-Mail-Adresse eingeben. Wenn die E-Mail-Adresse von IBMid erkannt wird, werden die Benutzer auf die Anmeldeseite des SAML 2.0-Identitätsproviders ihres Unternehmens weitergeleitet. Auf dieser Seite schließen die Benutzer den Authentifizierungsprozess durch Angabe ihrer Berechtigungsnachweise ab. Sie haben dann Zugriff auf Cognos Analytics.

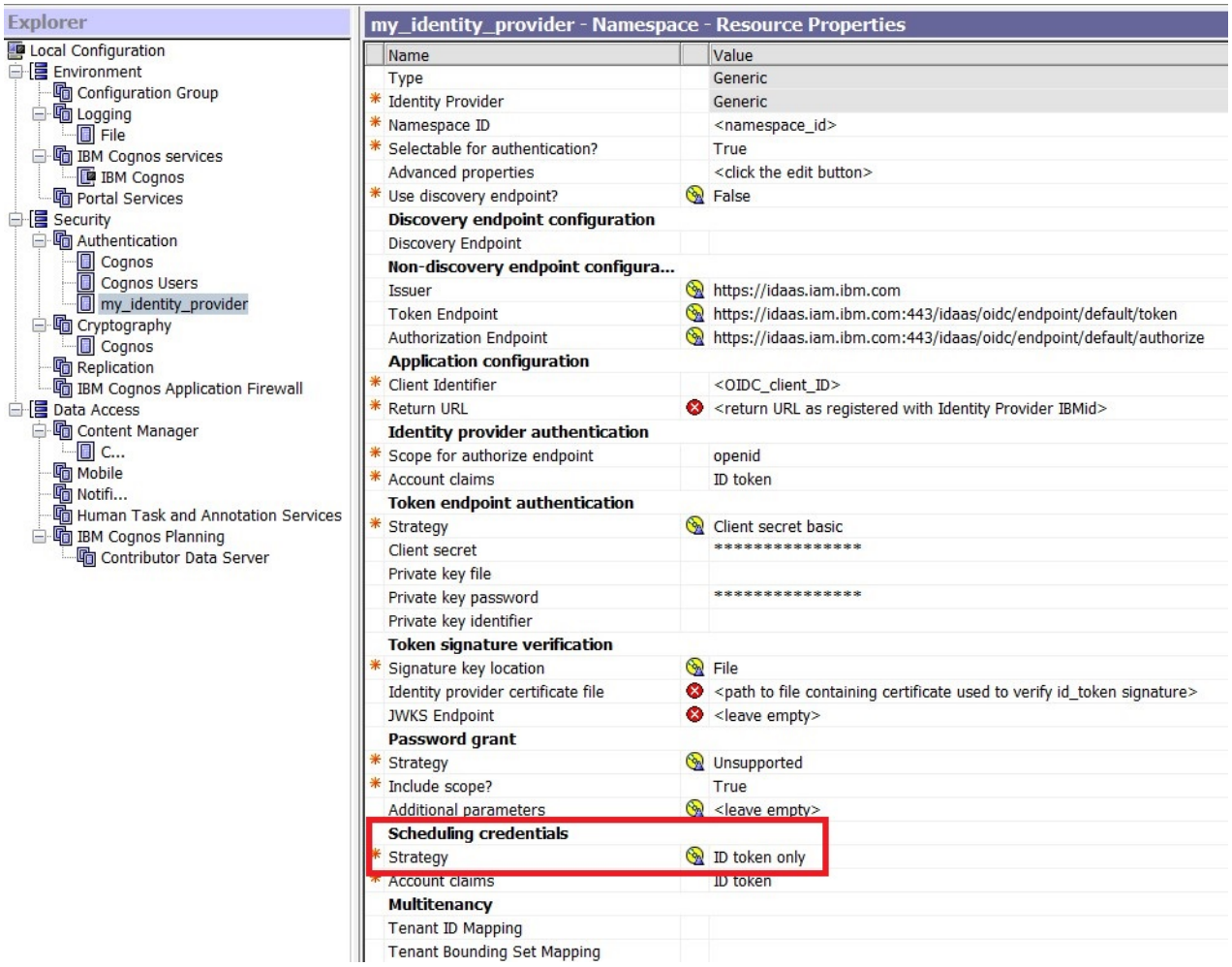
Generischer OIDC-Providertyp

IBMid ist der IBM OpenID Connect-Identitätsprovider. Wenn Ihr Identitätsprovider jedoch bereits bei anderen Identitätsprovidern eingebunden ist, müssen Sie den generischen Typ auswählen, wenn ein OpenID Connect-Namespace als Ihr Authentifizierungsprovider in Cognos Analytics konfiguriert werden soll.

Wenn Sie Ihren Identitätsprovider mit IBMid konfigurieren und der Identitätsprovider bereits eingebunden ist, treten bei Benutzern bei dem Versuch, Berechtigungsnachweise zu erneuern oder einen Zeitplan zu erstellen, Authentifizierungsfehler auf. Die Auswahl des generischen Typs anstelle von **IBMid** ist erforderlich, da IBMid den Ablauf für `password_grant` bei der Einbindung in eine externe Authentifizierungsquelle nicht unterstützt.

Anmerkung: Wählen Sie in Cognos Configuration für die Konfiguration unter **Sicherheit** > **Authentifizierung** > ***Eigener Identitätsprovider*** > **Berechtigungsnachweise für Zeitplanung** > **Strategie** keinen Wert aus, der die Zeichenfolge "Credentials" enthält. Legen Sie stattdessen für die Eigenschaft **Strategie** den Wert **Nur ID-Token** fest.

Ein Beispiel für eine Konfiguration, die den generischen OIDC-Typ verwendet, ist in der folgenden Abbildung dargestellt:



OpenID Connect-Identitätsprovider mit SSO-Unterstützung

Wenn Ihr OpenID Connect-Identitätsprovider Single Sign-on und die Zwei-Faktor-Authentifizierung unterstützt, kann Cognos Analytics diese Funktionalität nutzen.

Unterstützt der Identitätsprovider Single Sign-on nicht, wird der Benutzer zur Anmeldeseite des OpenID Connect-Identitätsproviders weitergeleitet, wenn ein Benutzer eine Authentifizierungsanfrage an Cognos Analytics richtet. Nach Angabe der erforderlichen Informationen wird der Benutzer mit einem Autorisierungscode, der gegen ein ID-Token eingelöst wird, das die Identität des Benutzers enthält, an Cognos Analytics zurückgeleitet. Der Benutzer kann dann auf Cognos Analytics zugreifen.

Unterstützt der Identitätsprovider Single Sign-on, empfängt der Benutzer das ID-Token, wenn er eine Authentifizierungsanforderung an Cognos Analytics richtet und er kann sofort auf die Anwendung zugreifen.

Konfigurieren von IBM Cognos für die Verwendung eines benutzerdefinierten Java-Authentifizierungsproviders

Wenn Sie einen benutzerdefinierten Java-Authentifizierungsprovider mit der vorhandenen Sicherheitsinfrastruktur implementiert haben, können Sie IBM Cognos-Komponenten für die Verwendung dieses Providers konfigurieren.

Sie können einen benutzerdefinierten Authentifizierungsprovider verwenden, um auf Benutzer zuzugreifen und diese bei einer Authentifizierungsquelle zu authentifizieren. Sie können ihn darüber hinaus als Mechanismus für die Einzelanmeldung (Single Sign-on) verwenden, um IBM Cognos-Komponenten in Ihre Sicherheitsinfrastruktur zu integrieren. Sie können den Namespace von Benutzern während der Anmeldung ausblenden.

Weitere Informationen finden Sie im *Custom Authentication Provider Developer Guide*.

Konfigurieren eines benutzerdefinierten Java-Authentifizierungsnamespace

Sie können IBM Cognos-Komponenten für die Verwendung eines benutzerdefinierten Authentifizierungs-Namespace konfigurieren. Alle zusätzlichen Konfigurationseinstellungen für den Zugriff auf Authentifizierungsquellen, die Einzelanmeldung und benutzerdefinierte Attribute hängen von der Implementierung des benutzerdefinierten Authentifizierungsproviders ab.

Stellen Sie sicher, dass die verwendeten Versionen von Java Runtime Environment (JRE) und Java Software Development Kit miteinander kompatibel sind. Wenn Sie unterstützte Versionen von JRE und Java Software Development Kit verwenden, die miteinander nicht kompatibel sind, wird der von Ihnen konfigurierte benutzerdefinierte Java-Authentifizierungsprovider nicht in der Liste der Namespaces in IBM Cognos Configuration angezeigt.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration an allen Positionen, an denen Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** mit der rechten Maustaste auf **Authentifizierung**. Klicken Sie dann auf **Neue Ressource** > **Namespace**.
3. Geben Sie im Feld **Name** einen Namen für den Authentifizierungsnamespace ein.
4. Wählen Sie in der Liste **Typ** die Option **Benutzerdefinierter Java-Provider** aus und klicken Sie auf **OK**.

   Die neue Authentifizierungsprovider-Ressource wird im Fenster **Explorer** unter der Komponente **Authentifizierung** angezeigt.
5. Geben Sie im Fenster **Eigenschaften** für die Eigenschaft **Namespace-ID** eine eindeutige ID für den Namespace ein.

   Tipp: Verwenden Sie keine Doppelpunkte (:) in der Eigenschaft **Namespace-ID**.
6. Geben Sie die Werte für alle anderen erforderlichen Eigenschaften an, um sicherzustellen, dass IBM Cognos den vorhandenen Authentifizierungsprovider finden und verwenden kann.
7. Klicken Sie im Menü **Datei** auf **Speichern**.
8. Testen Sie die Verbindung zu einem neuen Namespace. Klicken Sie im Fenster **Explorer** unter **Authentifizierung** mit der rechten Maustaste auf die neue Authentifizierungsressource und klicken Sie auf **Test**.

   Sie werden dazu aufgefordert, die Berechtigungsnachweise für einen Benutzer im Namespace einzugeben, um den Test auszuführen.

   Abhängig von der Konfiguration des Namespace können Sie entweder eine gültige Benutzer-ID und ein gültiges Kennwort für einen Benutzer im Namespace eingeben oder den Wert der Eigenschaft 'Benutzer-DN und Kennwort für Bindung'.

Ergebnisse

IBM Cognos lädt, initialisiert und konfiguriert die Providerbibliotheken für den Namespace.

Ausblenden des Namespace von Benutzern während der Anmeldung

Sie können den Namespace von Benutzern während der Anmeldung ausblenden. Dies ermöglicht Trusted-Sign-on-Namespaces (vertrauenswürdige Anmelde-Namespaces), die nicht in der Namespace-Auswahlliste angezeigt werden, wenn sich Benutzer anmelden.

Beispielsweise kann es sein, dass Sie eine systemübergreifende Einzelanmeldung integrieren, aber Kunden weiterhin die Möglichkeit geben möchten, sich direkt für IBM Cognos zu authentifizieren, ohne zur Auswahl eines Namespace aufgefordert zu werden.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration an jeder Position, an der Sie einen benutzerdefinierten Java-Authentifizierungsprovider konfiguriert haben.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** > **Authentifizierung** auf den benutzerdefinierten Java-Authentifizierungsprovider.
3. Klicken Sie im Fenster **Eigenschaften** auf das Feld neben **Zur Authentifizierung auswählbar** und wählen Sie **Falsch**.
4. Klicken Sie im Menü **Datei** auf **Speichern**.

Ergebnisse

Der Namespace erscheint nicht in der bei der Anmeldung angezeigten Auswahlliste.

OpenID Connect-Authentifizierungsproxy

Cognos Analytics stellt einen anderen Providertyp (OpenID Connect-Authentifizierungsproxy) in Cognos Configuration bereit.

Das Menü für den OpenID Connect-Authentifizierungsproxy enthält die Option 'Trusted Signon Provider' (TSP) für OpenID Connect. Ähnlich wie bei OpenID Connect-Einträgen wird eine Liste mit Identitätsprovidern angezeigt, die derzeit unterstützt werden.

Weitere Einträge für Konfigurationseinstellungen werden unter 'Erweiterte Eigenschaften' angezeigt. Sie müssen die Anforderung, die an den tatsächlichen Provider übergeben werden soll, sowie die Namespace-ID des tatsächlichen Providers konfigurieren.

- Name der Identitätsanforderung: Gibt den Namen der Anforderung an, die an den Zielnamespace gesendet wird (z. B. John Doe).
- Name der vertrauenswürdigen Umgebung: Gibt den Umgebungsvariablennamen an, der für die Übertragung der Anforderung an den Zielnamespace verwendet wird (z. B. REMOTE_USER).
- ID des Weiterleitungsnamespace: Gibt die Namespace-ID an, die mit der Anforderung aufgerufen wird, die vom OpenID-Identitätsprovider abgerufen wurde (z. B. LDAP).

Konfigurieren von IBM Cognos für die Verwendung von IBM Cognos Series 7-Namespaces

Sie können IBM Cognos-Komponenten so konfigurieren, dass ein IBM Cognos Series 7-Namespace als Authentifizierungsprovider verwendet wird. Die Benutzer werden basierend auf der Authentifizierungs- und Anmeldekonfiguration des IBM Cognos Series 7-Namespace authentifiziert.

Wenn Sie IBM Cognos Series 7-PowerCubes und Transformer-Modelle in IBM Cognos Analytics verwenden möchten, ist ein IBM Cognos Series 7-Namespace erforderlich. Sie müssen den Namespace konfigurieren, bevor Sie die Transformer-Modelle laden.

Anmerkung: Für die Authentifizierung mit IBM Cognos-Komponenten kann keine lokale Authentifizierungsexportdatei (LAE-Datei) von IBM Cognos Series 7 verwendet werden.

Sie können IBM Cognos-Komponenten so konfigurieren, dass mehrere IBM Cognos Series 7-Authentifizierungsprovider verwendet werden. Alle IBM Cognos Series 7-Namespaces müssen denselben primären IBM Cognos Series 7-Ticket-Server verwenden. Andernfalls können Fehlernachrichten ausgegeben werden oder Sie müssen sich mehrmals authentifizieren. Achten Sie im Interesse der Leistung zudem darauf, dass der Ticket Server ausgeführt wird.

Wenn Sie die Konfigurationsinformationen, die in dem für IBM Cognos Series 7 verwendeten Verzeichnisserver gespeichert sind, ändern, müssen Sie den IBM Cognos-Service neu starten, damit die Änderungen in der IBM Cognos-Installation wirksam werden.

Ein Benutzer muss mindestens einer Access Manager-Benutzerklasse angehören, um sich bei den IBM Cognos-Komponenten anmelden zu können.

Vorgehensweise

1. Konfigurieren Sie einen Series 7-Namespace.
2. Aktivieren Sie gegebenenfalls die sichere Kommunikation mit dem Verzeichnisserver, der vom IBM Cognos Series 7-Namespace verwendet wird.
3. Aktivieren Sie die Einzelanmeldung zwischen IBM Cognos Series 7 und IBM Cognos .

Konfigurieren eines IBM Cognos Series 7-Namespace

Sie können IBM Cognos so konfigurieren, dass für die Authentifizierung ein oder mehrere IBM Cognos Series 7-Namespaces verwendet werden.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration an jeder Position, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** mit der rechten Maustaste auf **Authentifizierung** und klicken Sie anschließend auf **Neue Ressource** > **Namespace**.
3. Geben Sie im Feld **Name** einen Namen für den Authentifizierungsnamespace ein.
4. Klicken Sie in der Liste **Typ** auf den entsprechenden Namespace und anschließend auf **OK**.

   Die neue Authentifizierungsprovider-Ressource wird im Fenster **Explorer** unter der Komponente **Authentifizierung** angezeigt.
5. eben Sie im Fenster **Eigenschaften** für die Eigenschaft **Namespace-ID** eine eindeutige ID für den Namespace ein.
6. Geben Sie die Werte für alle anderen erforderlichen Eigenschaften an, um sicherzustellen, dass IBM Cognos-Komponenten den vorhandenen Authentifizierungsprovider finden und verwenden können.

   Wenn Sie einen IBM Cognos Series 7-Namespace der Version 16.0 verwenden, muss die Eigenschaft **Datenverschlüsselung** auf **UTF-8** gesetzt werden. Außerdem müssen die Verzeichnisse, in denen Content Manager installiert ist, dieselbe Ländereinstellung verwenden wie die Daten im IBM Cognos Series 7-Namespace.

   Der Wert für den Host kann ein Servername oder eine IP-Adresse sein. Wenn Sie von PowerPlay Enterprise Server nach IBM Cognos Analytics publizieren, müssen Sie für die Werte dasselbe Format verwenden wie in IBM Cognos Series 7 Configuration Manager für die Position des Verzeichnisservers.

   Wenn in IBM Cognos Series 7 Configuration Manager beispielsweise der Servername verwendet wird, müssen Sie den Servernamen auch in IBM Cognos Configuration für IBM Cognos Analytics verwenden.
7. Wenn Ihre Namespace-Umgebung Version 15.2 des IBM Cognos Series 7-Namespace enthält, müssen Sie die Einstellung **Series7NamespacesAreUnicode** inaktivieren.
   - Klicken Sie im Fenster **Eigenschaften** unter **Erweiterte Eigenschaften** für den Wert auf das Bearbeitungsymbol.
   - Klicken Sie im Fenster **Wert - Erweiterte Eigenschaften** auf **Hinzufügen**.
   - Geben Sie **Series7NamespacesAreUnicode** im Feld **Name** ein.
   - Geben Sie **Falsch** im Feld **Wert** ein und klicken Sie anschließend auf **OK**.
8. Überprüfen Sie, ob im Fenster **Eigenschaften** unter **Cookieeinstellungen** die Eigenschaften **Pfad**, **Domäne** und **Ist das Sicherheitsflag aktiviert?** mit den für IBM Cognos Series 7 konfigurierten Einstellungen übereinstimmen.
9. Klicken Sie im Menü **Datei** auf **Speichern**.
10. Testen Sie die Verbindung zu einem neuen Namespace. Klicken Sie im Fenster **Explorer** unter **Authentifizierung** mit der rechten Maustaste auf die neue Authentifizierungsressource und klicken Sie auf **Test**.

Sie werden dazu aufgefordert, die Berechtigungsnachweise für einen Benutzer im Namespace einzugeben, um den Test auszuführen.

Abhängig von der Konfiguration des Namespace können Sie entweder eine gültige Benutzer-ID und ein gültiges Kennwort für einen Benutzer im Namespace eingeben oder den Wert der Eigenschaft 'Benutzer-DN und Kennwort für Bindung'.

Aktivieren der sicheren Kommunikation mit dem Verzeichnisserver, der vom IBM Cognos Series 7-Namespace verwendet wird

Wenn Sie eine SSL-Verbindung zum Verzeichnisserver verwenden, der vom IBM Cognos Series 7-Namespace verwendet wird, müssen Sie das Zertifikat vom Verzeichnisserver an jede Content Manager-Position kopieren.

Weitere Informationen finden Sie im IBM Cognos Access Manager *Administratorhandbuch* und in der Dokumentation für den Verzeichnisserver.

Aktivieren von Single Sign-on zwischen IBM Cognos Series 7 und IBM Cognos

Wenn der IBM Cognos Series 7-Namespace zum Zweck der Einzelanmeldung (Single Sign-on) für die Integration mit dem externen Authentifizierungsmechanismus konfiguriert wurde, verwendet der IBM Cognos Series 7-Provider automatisch diese Konfiguration.

Indem Sie die Einzelanmeldung konfigurieren, müssen Sie die Authentifizierungsinformationen nicht erneut eingeben, wenn Sie auf IBM Cognos-Inhalte zugreifen, die durch den IBM Cognos Series 7-Namespace gesichert sind.

Vorgehensweise

1. Stellen Sie sicher, dass IBM Cognos-Komponenten so konfiguriert werden, dass ein IBM Cognos Series 7 -Namespace als Authentifizierungsprovider verwendet wird.
2. Starten Sie Configuration Manager für IBM Cognos Series 7.
3. Klicken Sie auf **Aktuelle Konfiguration öffnen**.
4. Erweitern Sie im Fenster **Explorer** auf der Registerkarte **Komponenten** die Einträge **Services** und **Access Manager - Web-Authentifizierung** und klicken Sie auf **Cookieeinstellungen**.
5. Überprüfen Sie, ob im Fenster **Eigenschaften** die Eigenschaften **Pfad**, **Domäne** und **Ist das Sicherheitsflag aktiviert?** mit den für IBM Cognos Analytics konfigurierten Einstellungen übereinstimmen.
6. Speichern und schließen Sie Configuration Manager.
7. Wenn der IBM Cognos Series 7-Namespace das Trusted-Sign-on-Plug-in für die Einzelanmeldung verwendet, müssen Sie jetzt die Funktion SaferAPIGetTrustedSignonWithEnv definieren.

Ergebnisse

Sie können nun NewsBoxes aus IBM Cognos Upfront Series 7 in IBM Cognos Analytics hinzufügen.

IBM Cognos Series 7-Namespaces und IBM Cognos Series 7-Trusted-Signon-Plug-in

Wenn der IBM Cognos Series 7-Namespace das Trusted-Sign-on-Plug-in für das Single Sign-on verwendet, müssen Sie die Funktion 'SaferAPIGetTrustedSignonWithEnv' in Ihrem Plug-in definieren. Anschließend müssen Sie die Bibliothek neu kompilieren und erneut bereitstellen, damit das Single-Sign-on für IBM Cognos-Komponenten und den Authentifizierungsmechanismus verfügbar ist.

Bei der Funktion 'SaferAPIGetTrustedSignonWithEnv' handelt es sich um eine aktualisierte Version der Funktion 'SaferAPIGetTrustedSignon'. Diese Aktualisierung ist erforderlich, da die IBM Cognos-Anmeldung nicht wie bei IBM Cognos Series 7-Anwendungen am Web-Server ausgeführt wird. Daher kann

das Plug-in keinen API-Aufruf 'getenv( )' zum Abrufen von Web-Server-Umgebungsvariablen ausführen. Möglicherweise ist es für das Plug-in erforderlich, dass bestimmte Umgebungsvariablen vom Web-Server mit der Funktion 'SaferAPIGetTrustedSignonWithEnv' entfernt werden.

Wenn Sie sowohl IBM Cognos Series 7 und IBM Cognos-Produkte mit demselben Plug-in ausführen, sind die Funktionen 'SaferAPIGetTrustedSignonWithEnv' und 'SaferAPIGetTrustedSignon' erforderlich. Weitere Informationen zur Funktion 'SaferAPIGetTrustedSignon' finden Sie in der IBM Cognos Series 7-Dokumentation.

Funktion SaferAPIGetTrustedSignonWithEnv

Damit Benutzer von Access Manager erfolgreich authentifiziert werden, müssen BS-Anmeldungen vorhanden sein und im aktuellen Namespace aktiviert sein.

Der Speicherplatz für die zurückgegebenen Werte für trustedSignonName und trustedDomainName wird intern in dieser API zugeordnet. Wenn die Funktion SAFER_SUCCESS zurückgibt, ruft Access Manager SaferAPIFreeTrustedSignon auf, um den zugeordneten Speicherplatz freizugeben.

Der Speicherplatz für den zurückgegebenen Wert für reqEnvVarList wird intern in dieser API zugeordnet. Wenn die Funktion SAFER_INFO_REQUIRED zurückgibt, ruft Access Manager SaferAPIFreeBuffer() auf, um den zugeordneten Speicherplatz freizugeben.

Wenn SaferAPIGetTrustedSignonWithEnv implementiert ist, müssen Sie sowohl die Funktion SaferAPIGetTrustedSignon als auch die Funktion SaferAPIFreeBuffer implementieren, um die Bibliothek erfolgreich zu registrieren. Die Funktion SaferAPIGetError ist nur erforderlich, wenn das Plug-in bestimmte Fehlernachrichten zurückgeben soll.

Syntax

```
SaferAPIGetTrustedSignonWithEnv(

   EnvVar             envVar[],                  /*[IN]*/

   char               **reqEnvVarList,           /*[OUT]*/

   void               **trustedSignonName,       /*[OUT]*/

   unsigned long      *trustedSignonNameLength,  /*[OUT]*/

   void               **trustedDomainName,       /*[OUT]*/

   unsigned long      *trustedDomainNameLength,  /*[OUT]*/

   SAFER_USER_TYPE    *userType,                 /*[OUT]*/

   void               **implementerData);        /*[IN/OUT]*/
```

Parameter für die Funktion SaferAPIGetTrustedSignonWithEnv

Tabelle 37. Parameter und Beschreibung für die Funktion SaferAPIGetTrustedSignonWithEnv

Parameter	Beschreibung
[in] envVar	Ein Array aus Umgebungsvariablennamen und -werten, die vom Web-Server abgerufen wurden. Das Ende des Array wird durch einen Eintrag mit einem Nullwert für "envVarName" und "envVarValue" dargestellt. Wenn diese API zum ersten Mal aufgerufen wird, enthält das Array "envVar" nur den Datenpunkt für das Ende des Arrays.

Tabelle 37. Parameter und Beschreibung für die Funktion SaferAPIGetTrustedSignonWithEnv (Forts.)	
Parameter	**Beschreibung**
[in] reqEnvVarList	Eine Zeichenfolge mit einer durch Kommas getrennten Liste der Umgebungsvariablennamen und -werte, die für die Implementierung von "Safer" erforderlich sind. Die Liste muss am Ende eine Null enthalten.
[out] trustedSignonName	Eine Reihenfolge von Bytes, durch die der derzeit authentifizierte Benutzer identifiziert wird. Für diesen Wert ist keine Null am Ende erforderlich. Dieser Wert ist obligatorisch.
[out] trustedSignonNameLength	Ein Ganzzahlwert, der die Länge von "trustedSignonName" angibt. Die gegebenenfalls vorhandene abschließende Null sollte in dieser Länge nicht eingeschlossen sein. Dieser Wert ist obligatorisch.
[out] trustedDomainName	Eine Reihenfolge von Bytes, durch die die Domäne des derzeit authentifizierten Benutzers identifiziert wird. Dieser Wert muss nicht null-terminiert werden. Wenn kein Element "trustedDomainName" vorhanden ist, wird null zurückgegeben. Dieser Wert ist optional.
[out] trustedDomainNameLength	Ein Ganzzahlwert, der die Länge von "trustedDomainName" angibt. Die gegebenenfalls vorhandene abschließende Null sollte in dieser Länge nicht eingeschlossen sein. Dieser Wert ist obligatorisch und muss auf null zurückgesetzt werden, wenn kein Element "trustedDomainName" vorhanden ist.
[out] userType	Ein Wert, der den von Access Manager zu authentifizierenden Benutzertyp angibt. Dieser Wert ist obligatorisch. Die Rückgabe folgender Werte wird für Access Manager benötigt, um Benutzer erfolgreich zu authentifizieren: **SAFER_NORMAL_USER** Ein benannter Benutzer. BS-Anmeldungen müssen vorhanden und im aktuellen Namespace aktiviert sein. **SAFER_GUEST_USER** Ein Gastbenutzer. Es muss ein Benutzerkonto für Gastbenutzer vorhanden und im aktuellen Namespace aktiviert sein. **SAFER_ANONYMOUS_USER** Ein anonymer Benutzer. Es muss ein Benutzerkonto für anonyme Benutzer vorhanden und im aktuellen Namespace aktiviert sein.
[in/out] implementerData	Ein Verweis zum Schutz von implementierungsspezifischen Daten zwischen den einzelnen Initialisierungen. Eine Initialisierung wird jedes Mal ausgeführt, wenn Access Manager das Trusted-Sign-on-Plug-in aufruft. Dieser Wert ist nur gültig, wenn das Plug-in "Trusted Sign-on" initialisiert wurde und Sie für das Plug-in einen Wert festgelegt haben.

Konfigurieren von IBM Cognos-Komponenten für die Verwendung von LDAP

Sie können IBM Cognos-Komponenten so konfigurieren, dass ein LDAP-Namespace als Authentifizierungsprovider verwendet wird. Sie können für Benutzer, die in einem LDAP-Benutzerverzeichnis, in Active

Directory Server, IBM Directory Server, Novell Directory Server oder Oracle Directory Server gespeichert sind, einen LDAP-Namespace verwenden.

Darüber hinaus können Sie die LDAP-Authentifizierung mit IBM Db2- und Essbase-OLAP-Datenquellen verwenden, indem Sie beim Einrichten der Datenquellenverbindung den LDAP-Namespace angeben. Weitere Informationen finden Sie in der Veröffentlichung *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Sie können auch angepasste Benutzereigenschaften des LDAP-Namespace in IBM Cognos-Komponenten zur Verfügung stellen.

Informationen dazu, wie Sie Benutzer an den LDAP-Server binden, finden Sie in „LDAP-Zuordnung” auf Seite 281.

Vorgehensweise

1. „Konfigurieren eines LDAP-Namespace” auf Seite 282
2. Stellen Sie gegebenenfalls benutzerdefinierte Benutzereigenschaften in IBM Cognos-Komponenten zur Verfügung.
3. Aktivieren Sie gegebenenfalls die sichere Kommunikation mit dem LDAP-Server, falls erforderlich.
4. Aktivieren Sie die Einzelanmeldung für LDAP und IBM Cognos-Komponenten, falls erforderlich.

LDAP-Zuordnung

Um einen Benutzer an den LDAP-Server zu binden, muss der LDAP-Authentifizierungsprovider den DN (Distinguished Name) erstellen. Wenn die Eigenschaft 'Externe Identität verwenden' auf 'Wahr' gesetzt ist, wird der DN des Benutzers mithilfe der Eigenschaft 'Externer Identitätsabgleich' aufgelöst. Wenn der Authentifizierungsprovider die Umgebungsvariable oder den DN nicht auf dem LDAP-Server finden kann, versucht er, den DN mithilfe der Eigenschaft **Benutzersuche** zu erstellen.

Wenn die Benutzer in einer hierarchischen Struktur im Verzeichnisserver gespeichert sind, können Sie die Eigenschaften 'Benutzersuche' und 'Externer Identitätsabgleich' für die Verwendung von Suchfiltern konfigurieren. Wenn der LDAP-Authentifizierungsprovider einen Suchlauf durchführt, verwendet er die Filter, die Sie für die Eigenschaften 'Benutzersuche' und 'Externer Identitätsabgleich' angeben. Darüber hinaus stellt er eine Bildung zum Verzeichnisserver her. Dabei verwendet er den Wert, den Sie für die Eigenschaft 'Benutzer-DN und Kennwort für Bindung' angeben, oder 'anonym', wenn kein Wert angegeben wird.

Wenn ein LDAP-Namespace so konfiguriert ist, dass er die Eigenschaft 'Externer Identitätsabgleich' zur Authentifizierung verwendet, stellt der LDAP-Provider eine Bindung zum Verzeichnisserver her, bei der er den Wert der Eigenschaft 'Benutzer-DN und Kennwort für Bindung' verwendet bzw. 'anonym', wenn kein Wert angegeben wird. Alle Benutzer, die sich mithilfe des externen Identitätsabgleichs bei IBM Cognos anmelden, sehen die gleichen Benutzer, Gruppen und Ordner wie die Bindungsbenutzer.

Wenn Sie keinen externen Identitätsabgleich verwenden, können Sie angeben, ob Sie mithilfe von Bindungsberechtigungsnachweisen durch Konfigurieren der Eigenschaft **Bindungsberechtigungsnachweise für die Suche verwenden** nach dem LDAP-Verzeichnisserver suchen möchten. Wenn die Eigenschaft aktiviert ist, werden Suchvorgänge entweder unter Verwendung der Bindungsberechtigungsnachweise des Benutzers durchgeführt oder anonym, falls kein Wert angegeben ist. Ist die Eigenschaft inaktiviert (Standardeinstellung), werden Suchvorgänge mithilfe der Berechtigungsnachweise des angemeldeten Benutzers durchgeführt. Der Vorteil von Bindungsberechtigungsnachweise ist, dass Sie die administrativen Rechte nur für den Bindungsbenutzer ändern können und nicht für mehrere Benutzer gleichzeitig ändern müssen.

Anmerkung: Wenn Sie eine DN-Syntax wie z. B. `uid=${Benutzer-ID}, ou=meine Firma.com` für die Eigenschaften **Benutzersuche**, **Externer Identitätsabgleich** oder **Benutzer-DN und Kennwort für Bindung** verwenden, müssen Sie alle im DN verwendeten Sonderzeichen mit Escapezeichen versehen. Wenn Sie eine Suchsyntax wie z. B. `(uid=${Benutzer-ID})` für die Eigenschaften **Benutzersuche** oder **Externer Identitätsabgleich** verwenden, müssen die im DN verwendeten Sonderzeichen nicht mit Escapezeichen versehen werden.

Konfigurieren eines LDAP-Namespace

Sie können IBM Cognos-Komponenten zur Verwendung eines LDAP-Namespace konfigurieren, wenn die Benutzer in einem LDAP-Benutzerverzeichnis gespeichert sind. Auf das LDAP-Benutzerverzeichnis kann auch von einer anderen Serverumgebung aus, wie Active Directory Server oder SiteMinder, zugegriffen werden.

Wenn Sie einen LDAP-Namespace für einen anderen Verzeichnisserver als LDAP konfigurieren, informieren Sie sich im entsprechenden Abschnitt:

- Informationen zu Active Directory Server finden Sie in Konfigurieren eines LDAP-Namespace für Active Directory Server.
- Informationen zu IBM Directory Server finden Sie in Konfigurieren eines LDAP-Namespace für IBM Directory Server.
- Informationen zu Novell Directory Server finden Sie in Konfigurieren eines LDAP-Namespace für Novell Directory Server.
- Informationen zu Oracle Directory Server finden Sie in Konfigurieren eines LDAP-Namespace für Oracle Directory Server.

Darüber hinaus können Sie die LDAP-Authentifizierung mit IBM Db2- und Essbase-OLAP-Datenquellen verwenden, indem Sie beim Einrichten der Datenquellenverbindung den LDAP-Namespace angeben. Weitere Informationen finden Sie in der Veröffentlichung *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration an jeder Position, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** mit der rechten Maustaste auf **Authentifizierung** und klicken Sie anschließend auf **Neue Ressource** > **Namespace**.
3. Geben Sie im Feld **Name** einen Namen für den Authentifizierungsnamespace ein.
4. Klicken Sie in der Liste **Typ** auf den entsprechenden Namespace und anschließend auf **OK**.

   Die neue Authentifizierungsprovider-Ressource wird im Fenster **Explorer** unter der Komponente **Authentifizierung** angezeigt.
5. eben Sie im Fenster **Eigenschaften** für die Eigenschaft **Namespace-ID** eine eindeutige ID für den Namespace ein.
6. Geben Sie die Werte für alle anderen erforderlichen Eigenschaften an, um sicherzustellen, dass IBM Cognos-Komponenten den vorhandenen Authentifizierungsprovider lokalisieren und verwenden können.
7. Falls der LDAP-Authentifizierungsprovider mithilfe der Eigenschaft **Benutzer-DN und Kennwort für Bindung** eine Bindung zum Verzeichnisserver herstellen soll, wenn Sie Suchvorgänge durchführen, geben Sie diese Werte an.

   Wenn keine Werte angegeben werden, stellt der LDAP-Authentifizierungsprovider eine anonyme Bindung her.

   Wenn der externe Identitätsabgleich aktiviert ist, wird **Benutzer-DN und Kennwort für Bindung** grundsätzlich für den Zugriff auf LDAP verwendet. Wenn der externe Identitätsabgleich nicht aktiviert ist, wird die Option **Benutzer-DN und Kennwort für Bindung** nur verwendet, wenn für die Eigenschaft **Benutzersuche** ein Suchfilter angegeben ist. In diesem Fall werden, sobald der Benutzer-DN vorliegt, nachfolgende Anforderungen an den LDAP-Server unter dem Authentifizierungskontext des Benutzers ausgeführt.
8. Wenn Sie keinen externen Identitätsabgleich verwenden, suchen Sie mithilfe von Bindungsberechtigungsnachweisen nach dem LDAP-Verzeichnisserver, indem Sie die folgende Schritte ausführen:
   - Stellen Sie sicher, dass die Eigenschaft **Externe Identität verwenden** auf **Falsch** eingestellt ist.
   - Legen Sie für die Eigenschaft **Bindungsberechtigungsnachweise für die Suche verwenden** den Wert **True** fest.
   - Geben Sie für **Benutzer-DN und Kennwort für Bindung** die Benutzer-ID und das Kennwort an.

Wenn Benutzer-ID und Kennwort nicht angeben werden und der anonyme Zugriff aktiviert ist, wird der Suchvorgang anonym ausgeführt.

9. Überprüfen Sie die Zuordnungseinstellungen für die erforderlichen Objekte und Attribute.

   Je nach LDAP-Konfiguration müssen Sie gegebenenfalls einige Standardwerte ändern, um eine erfolgreiche Kommunikation zwischen IBM Cognos-Komponenten und dem LDAP-Server sicherzustellen.

   Auf LDAP-Attribute, die in **Ordnerzuordnungen**, **Gruppenzuordnungen** oder **Kontozuordnungen** der Eigenschaft **Name** zugeordnet sind, müssen alle authentifizierten Benutzer zugreifen können. Die Eigenschaft **Name** darf außerdem nicht leer sein.
10. Klicken Sie im Menü **Datei** auf **Speichern**.
11. Testen Sie die Verbindung zu einem neuen Namespace. Klicken Sie im Fenster **Explorer** unter **Authentifizierung** mit der rechten Maustaste auf die neue Authentifizierungsressource und klicken Sie auf **Test**.

    Sie werden dazu aufgefordert, die Berechtigungsnachweise für einen Benutzer im Namespace einzugeben, um den Test auszuführen.

    Abhängig von der Konfiguration des Namespace können Sie entweder eine gültige Benutzer-ID und ein gültiges Kennwort für einen Benutzer im Namespace eingeben oder den Wert der Eigenschaft 'Benutzer-DN und Kennwort für Bindung'.

Ergebnisse

IBM Cognos lädt, initialisiert und konfiguriert die Providerbibliotheken für den Namespace.

Konfigurieren eines LDAP-Namespace für Active Directory Server

Wenn Sie einen neuen LDAP-Namespace zur Verwendung mit einem Active Directory Server konfigurieren, werden die Werte vom Programm generiert.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration an jeder Position, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** mit der rechten Maustaste auf **Authentifizierung** und klicken Sie dann auf **Neue Ressource** > **Namespace**.
3. Geben Sie im Feld **Name** einen Namen für den Authentifizierungsnamespace ein.
4. Wählen Sie in der Liste **Typ** die Option **LDAP - Standardwerte für Active Directory** aus und klicken Sie dann auf **OK**.

   Die neue Authentifizierungsprovider-Ressource wird im Fenster **Explorer** unter der Komponente **Authentifizierung** angezeigt. Die Standardwerte werden vom Programm generiert. Überprüfen Sie sie und nehmen Sie bei Bedarf Änderungen vor.
5. Geben Sie im Fenster **Eigenschaften** für die Eigenschaft **Namespace-ID** eine eindeutige ID für den Namespace ein.

   Tipp: Verwenden Sie keine Doppelpunkte (:) in der Eigenschaft **Namespace-ID**.
6. Geben Sie die Werte für alle anderen erforderlichen Eigenschaften an, um sicherzustellen, dass IBM Cognos-Komponenten den vorhandenen Authentifizierungsprovider finden und verwenden können.

   Beispiele für Einstellungen:

   - Für **Benutzersuche** geben Sie `(sAMAccountName=${Benutzer-ID})` ein.
   - Beim Single Sign-on setzen Sie den Wert für **Externe Identität verwenden** auf **Wahr**.
   - Beim Single Sign-on setzen Sie **Externer Identitätsabgleich** auf `(sAMAccountName=${environment("REMOTE_USER")})`.

Wenn Sie den Domänennamen aus der Variablen REMOTE_USER entfernen möchten, geben Sie `(sAMAccountName=${replace(${environment("REMOTE_USER")}, "`**`Domäne`**`\\","")})` ein.

Wichtig: Achten Sie darauf, nur die Variable REMOTE_USER zu verwenden. Die Verwendung einer anderen Variablen kann eine Sicherheitslücke verursachen.

- Für **Benutzer-DN und Kennwort für Bindung** geben Sie **`Benutzer`**`@`**`Domäne`** ein.
- Für **Eindeutige Identifizierung** geben Sie `objectGUID` ein.

7. Falls der LDAP-Authentifizierungsprovider mithilfe der Eigenschaft **Benutzer-DN und Kennwort für Bindung** eine Bindung zum Verzeichnisserver herstellen soll, wenn Sie Suchvorgänge durchführen, geben Sie diese Werte an.

   Wenn keine Werte angegeben werden, stellt der LDAP-Authentifizierungsprovider eine anonyme Bindung her.
8. Wenn Sie keinen externen Identitätsabgleich verwenden, suchen Sie mithilfe von Bindungsberechtigungsnachweisen nach dem LDAP-Verzeichnisserver, indem Sie die folgende Schritte ausführen:
   - Stellen Sie sicher, dass für die Eigenschaft **Externe Identität verwenden** der Wert **False** festgelegt ist.
   - Legen Sie für die Eigenschaft **Bindungsberechtigungsnachweise für die Suche verwenden** den Wert **True** fest.
   - Geben Sie für **Benutzer-DN und Kennwort für Bindung** die Benutzer-ID und das Kennwort an.
9. Klicken Sie im Menü **Datei** auf **Speichern**.
10. Testen Sie die Verbindung zu einem neuen Namespace. Klicken Sie im Fenster **Explorer** unter **Authentifizierung** mit der rechten Maustaste auf die neue Authentifizierungsressource und klicken Sie auf **Test**.

    Sie werden dazu aufgefordert, die Berechtigungsnachweise für einen Benutzer im Namespace einzugeben, um den Test auszuführen.

    Abhängig von der Konfiguration des Namespace können Sie entweder eine gültige Benutzer-ID und ein gültiges Kennwort für einen Benutzer im Namespace eingeben oder den Wert der Eigenschaft 'Benutzer-DN und Kennwort für Bindung'.

Ergebnisse

IBM Cognos lädt, initialisiert und konfiguriert die Providerbibliotheken für den Namespace.

Konfigurieren eines LDAP-Namespace für IBM Directory Server

Wenn Sie einen neuen LDAP-Namespace zur Verwendung mit einem IBM Directory Server konfigurieren, werden die Werte vom Programm generiert.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration an jeder Position, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** mit der rechten Maustaste auf **Authentifizierung** und klicken Sie dann auf **Neue Ressource** > **Namespace**.
3. Geben Sie im Feld **Name** einen Namen für den Authentifizierungsnamespace ein.
4. Klicken Sie in der Liste **Typ** auf **LDAP - Standardwerte für IBM Tivoli** und klicken Sie dann auf **OK**.

   Die neue Authentifizierungs-Namespace-Ressource wird im Fenster **Explorer** unter der Komponente **Authentifizierung** angezeigt. Überprüfen Sie die Werte und nehmen Sie bei Bedarf Änderungen vor.
5. Geben Sie im Fenster **Eigenschaften** für die Eigenschaft **Namespace-ID** eine eindeutige ID für den Namespace ein.

   Tipp: Verwenden Sie keine Doppelpunkte (:) in der Eigenschaft **Namespace-ID**.

6. Geben Sie die Werte für alle anderen erforderlichen Eigenschaften an, um sicherzustellen, dass IBM Cognos den vorhandenen Authentifizierungs-Namespace finden und verwenden kann.
   - Für **Benutzersuche** geben Sie `(cn=${userID})` an.
   - Für **Benutzer-DN und Kennwort für Bindung** geben Sie *cn=root* an.
7. Falls der LDAP-Authentifizierungsprovider mithilfe der Eigenschaft **Benutzer-DN und Kennwort für Bindung** eine Bindung zum Verzeichnisserver herstellen soll, wenn Sie Suchvorgänge durchführen, geben Sie diese Werte an.

   Wenn keine Werte angegeben werden, stellt der LDAP-Authentifizierungsprovider eine anonyme Bindung her.
8. Wenn Sie keinen externen Identitätsabgleich verwenden, suchen Sie mithilfe von Bindungsberechtigungsnachweisen nach dem LDAP-Verzeichnisserver, indem Sie die folgende Schritte ausführen:
   - Stellen Sie sicher, dass für die Eigenschaft **Externe Identität verwenden** der Wert **False** festgelegt ist.
   - Legen Sie für die Eigenschaft **Bindungsberechtigungsnachweise für die Suche verwenden** den Wert **True** fest.
   - Geben Sie für **Benutzer-DN und Kennwort für Bindung** die Benutzer-ID und das Kennwort an.
9. Klicken Sie im Menü **Datei** auf **Speichern**.

Konfigurieren eines LDAP-Namespace für Novell Directory Server

Wenn Sie einen neuen LDAP-Namespace zur Verwendung mit einem Novell Directory Server konfigurieren, müssen Sie die erforderlichen Einstellungen bearbeiten und die Werte für alle Eigenschaften des Novell Directory-Objekts ändern.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration an jeder Position, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** mit der rechten Maustaste auf **Authentifizierung** und klicken Sie dann auf **Neue Ressource** > **Namespace**.
3. Geben Sie im Feld **Name** einen Namen für den Authentifizierungsnamespace ein.
4. Klicken Sie in der Liste **Typ** (Gruppe) auf **LDAP**, wählen Sie in der Liste **Typ** anschließend **LDAP - Allgemeine Standardwerte** aus und klicken Sie dann auf **OK**.

   Die neue Authentifizierungs-Namespace-Ressource wird im Fenster **Explorer** unter der Komponente **Authentifizierung** angezeigt.
5. Geben Sie im Fenster **Eigenschaften** für die Eigenschaft **Namespace-Kennung** eine eindeutige Kennung für den Namespace ein.

   Tipp: Verwenden Sie keine Doppelpunkte (:) in der Eigenschaft **Namespace-ID**.
6. Geben Sie die Werte für alle anderen erforderlichen Eigenschaften an, um sicherzustellen, dass IBM Cognos den vorhandenen Authentifizierungs-Namespace finden und verwenden kann.
   - Für **Benutzersuche** geben Sie `(cn=${userID})` an.
   - Für **Benutzer-DN und Kennwort für Bindung** geben Sie den Basis-DN für einen Benutzer mit Administratorrechten an, z. B. cn=*Admin*,o=*COGNOS*.
7. Falls der LDAP-Authentifizierungsprovider mithilfe der Eigenschaft **Benutzer-DN und Kennwort für Bindung** eine Bindung zum Verzeichnisserver herstellen soll, wenn Sie Suchvorgänge durchführen, geben Sie diese Werte an.

   Wenn keine Werte angegeben werden, stellt der LDAP-Authentifizierungsprovider eine anonyme Bindung her.
8. Wenn Sie keinen externen Identitätsabgleich verwenden, suchen Sie mithilfe von Bindungsberechtigungsnachweisen nach dem LDAP-Verzeichnisserver, indem Sie die folgende Schritte ausführen:

- Stellen Sie sicher, dass für die Eigenschaft **Externe Identität verwenden** der Wert **False** festgelegt ist.
- Legen Sie für die Eigenschaft **Bindungsberechtigungsnachweise für die Suche verwenden** den Wert **True** fest.
- Geben Sie für **Benutzer-DN und Kennwort für Bindung** die Benutzer-ID und das Kennwort an.

9. Verwenden Sie zum Konfigurieren der erweiterten LDAP-Zuordnungseigenschaften für die Verwendung mit den Novell Directory Server-Objekten die in der folgenden Tabelle angegebenen Werte.

Tabelle 38. Werte für erweiterte LDAP-Zuordnung zur Verwendung mit Novell Directory Server-Objekten

Zuordnungen	**LDAP-Eigenschaft**	**LDAP-Wert**
Ordner	Objektklasse	organizationalunit,organization,container
	Beschreibung	description
	Name	ou,o,cn
Gruppe	Objektklasse	groupofnames
	Beschreibung	description
	Mitglied	member
	Name	cn
Konto	Objektklasse	inetOrgPerson
	Geschäftstelefon	telephonenumber
	Ländereinstellung für Inhalte	Sprache
	Beschreibung	description
	E-Mail	mail
	Fax/Telefon	facsimiletelephonenumber
	Vorname	givenname
	Privattelefon	homephone
	Mobiltelefon	mobile
	Name	cn
	Pager-Telefon	pager
	Kennwort	(leer)
	Adresse	postaladdress
	Produktländereinstellung	Sprache

Tabelle 38. Werte für erweiterte LDAP-Zuordnung zur Verwendung mit Novell Directory Server-Objekten (Forts.)

Zuordnungen	LDAP-Eigenschaft	LDAP-Wert
	Nachname	sn
	Benutzername	uid

Diese Zuordnungseigenschaften stellen Änderungen dar, die auf der standardmäßigen Novell Directory Server-Installation basieren. Wenn Sie das Schema ändern, müssen Sie möglicherweise weitere Zuordnungsänderungen vornehmen.

Auf LDAP-Attribute, die in **Ordnerzuordnungen**, **Gruppenzuordnungen** oder **Kontozuordnungen** der Eigenschaft **Name** zugeordnet sind, müssen alle authentifizierten Benutzer zugreifen können. Die Eigenschaft **Name** darf außerdem nicht leer sein.

Damit sich Benutzer erfolgreich bei Portal anmelden können, benötigen sie Leseberechtigung für die Attribute ou und o.

10. Klicken Sie im Menü **Datei** auf **Speichern**.

Konfigurieren eines LDAP-Namespace für Oracle Directory Server

Wenn Sie einen neuen LDAP-Namespace zur Verwendung mit einem Oracle Directory Server konfigurieren, werden die Werte vom Programm generiert.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration an jeder Position, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** mit der rechten Maustaste auf **Authentifizierung** und klicken Sie dann auf **Neue Ressource** > **Namespace**.
3. Geben Sie im Feld **Name** einen Namen für den Authentifizierungsnamespace ein.
4. Klicken Sie in der Liste **Typ** auf **LDAP - Standardwerte für Oracle Directory Server** und klicken Sie dann auf **OK**.

   Die neue Authentifizierungs-Namespace-Ressource wird im Fenster **Explorer** unter der Komponente **Authentifizierung** angezeigt. Überprüfen Sie die Werte und nehmen Sie bei Bedarf Änderungen vor.
5. Geben Sie im Fenster **Eigenschaften** für die Eigenschaft **Namespace-Kennung** eine eindeutige Kennung für den Namespace ein.

   Tipp: Verwenden Sie keine Doppelpunkte (:) in der Eigenschaft **Namespace-ID**.
6. Geben Sie die Werte für alle anderen erforderlichen Eigenschaften an, um sicherzustellen, dass IBM Cognos den vorhandenen Authentifizierungs-Namespace finden und verwenden kann.

   Beispiele für Einstellungen:

   - Für **Benutzersuche** geben Sie `(uid=${userID})` ein.
   - Beim Single Sign-on setzen Sie den Wert für **Externe Identität verwenden** auf **Wahr**.
   - Bei der Einzelanmeldung geben Sie für **Externer Identitätsabgleich** ein beliebiges Attribut an, z. B. die NT-Benutzerdomänen-ID oder die Benutzer-ID:

     ```
     (ntuserdomainid=$environment("REMOTE_USER")})
     ```

     ```
     (uid=${environment("REMOTE_USER")})
     ```

     Wichtig: Achten Sie darauf, nur die Variable REMOTE_USER zu verwenden. Die Verwendung einer anderen Variablen kann eine Sicherheitslücke verursachen.
   - Für **Eindeutige Identifizierung** geben Sie `nsuniqueid` ein.

7. Falls der LDAP-Authentifizierungsprovider mithilfe der Eigenschaft **Benutzer-DN und Kennwort für Bindung** eine Bindung zum Verzeichnisserver herstellen soll, wenn Sie Suchvorgänge durchführen, geben Sie diese Werte an.

   Wenn keine Werte angegeben werden, stellt der LDAP-Authentifizierungsprovider eine anonyme Bindung her.
8. Wenn Sie keinen externen Identitätsabgleich verwenden, suchen Sie mithilfe von Bindungsberechtigungsnachweisen nach dem LDAP-Verzeichnisserver, indem Sie die folgende Schritte ausführen:
   - Stellen Sie sicher, dass für die Eigenschaft **Externe Identität verwenden** der Wert **False** festgelegt ist.
   - Legen Sie für die Eigenschaft **Bindungsberechtigungsnachweise für die Suche verwenden** den Wert **True** fest.
   - Geben Sie für **Benutzer-DN und Kennwort für Bindung** die Benutzer-ID und das Kennwort an.
9. Klicken Sie im Menü **Datei** auf **Speichern**.

Bereitstellen von angepassten Benutzereigenschaften für LDAP für IBM Cognos-Komponenten

In IBM Cognos-Komponenten können Sie beliebige Benutzerattribute des LDAP-Authentifizierungsproviders verwenden. Zur entsprechenden Konfiguration sind diese Attribute als benutzerdefinierte Eigenschaften für den LDAP-Namespace hinzuzufügen. Die benutzerdefinierten Eigenschaften stehen als Sitzungsparameter über Framework Manager zur Verfügung.

Sie können auch die benutzerdefinierten Eigenschaften innerhalb von Befehlsblöcken verwenden, um Oracle-Sitzungen und -Verbindungen zu konfigurieren. Sie können die Befehlsblöcke mit leichten Verbindungen und virtuellen privaten Datenbanken von Oracle verwenden. Weitere Informationen finden Sie in der Veröffentlichung *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Weitere Informationen über Sitzungsparameter finden Sie im *Framework Manager User Guide*.

Vorgehensweise

1. Öffnen Sie Cognos Configuration an jeder Position, an der Content Manager installiert ist.
2. Wählen Sie im Fenster **Explorer** unter **Sicherheit** > **Authentifizierung** den LDAP-Namespace aus.
3. Klicken Sie im Fenster **Eigenschaften** auf die Spalte **Wert** für **Benutzerdefinierte Eigenschaften** und klicken Sie dann auf das Bearbeitungsymbol.
4. Klicken Sie im Fenster **Wert - Benutzerdefinierte Eigenschaften** auf **Hinzufügen**.
5. Klicken Sie auf die Spalte **Name** und geben Sie den Namen ein, der von den IBM Cognos-Komponenten für den Sitzungsparameter verwendet werden soll.
6. Klicken Sie auf die Spalte **Wert** und geben Sie den Namen des Kontoparameters in den LDAP-Authentifizierungsprovider ein.
7. Wiederholen Sie diese beiden Schritte für jeden benutzerdefinierten Parameter.
8. Klicken Sie auf **OK**.
9. Klicken Sie im Menü **Datei** auf **Speichern**.

Aktivieren der sicheren Kommunikation mit dem LDAP-Server

Die Kommunikation zwischen den Access Manager-Komponenten von Content Manager und dem Verzeichnisserver wird über Secure LDAP-Protokoll (LDAPS) verschlüsselt. LDAPS verhindert, dass geheime Informationen auf dem Verzeichnisserver und die LDAP-Berechtigungsnachweise als Klartext gesendet werden.

Um LDAPS zu aktivieren, installieren Sie ein Serverzertifikat, das von einer Zertifizierungsstelle für den Verzeichnisserver signiert wurde. Erstellen Sie anschließend eine Zertifikatsdatenbank, in der die Zertifikate abgelegt werden. Konfigurieren Sie abschließend den Verzeichnisserver und den LDAP-Namespace von IBM Cognos für die Verwendung von LDAPS.

Das Serverzertifikat muss eine Kopie von einem der folgenden Zertifikate sein:

- Vom vertrauenswürdigen Root-Zertifikat und allen anderen Zertifikaten, aus denen die Zertifikatskette des Verzeichnisserverzertifikats besteht.

  (Das vertrauenswürdige Root-Zertifikat ist das Zertifikat der Root-Zertifizierungsstelle, die das Verzeichnisserverzertifikat signiert hat.)
- Nur vom Verzeichnisserverzertifikat.

Die Zertifikate müssen im ASCII (PEM)-Format Base64-codiert sein. Alle Zertifikate, mit Ausnahme des vertrauenswürdigen Root-Zertifikats, dürfen nicht selbstsigniert sein.

Vorbereitende Schritte

IBM Cognos kann sowohl mit der Version `cert8.db` als auch mit der Version `cert7.db` der Clientzertifikatsdatenbank ausgeführt werden. Für die Erstellung der Zertifikatsdatenbank muss das Tool `certutil` von Netscape Security Services (NSS) verwendet werden. IBM Cognos akzeptiert keine anderen `cert8.db`-Dateiversionen, auch nicht die mit dem Tool `certutil`, das mit Microsoft Active Directory bereitgestellt wird, erstellten Dateien.

IBM Cognos enthält auf Plattformen, bei denen Netscape Security Services (NSS) nicht als Systemanforderung aufgelistet ist, das Tool `certutil`. Die Datei `certutil.exe` befindet sich im Verzeichnis *`Installationsposition`*`/bin64`. Sie müssen in Ihrer Umgebungsvariablen `LD_LIBRARY_PATH` das Verzeichnis `/bin64` hinzufügen.

Verwenden Sie für Plattformen, bei denen NSS als Systemvoraussetzung aufgeführt ist, die angegebene Version des Tools `certutil`.

Vorgehensweise

1. Erstellen Sie ein Verzeichnis für die Zertifikatsdatenbank.
2. Erstellen Sie die Zertifikatsdatenbank, indem Sie den folgenden Befehl eingeben:

   `certutil -N -d` *`Zertifikatsverzeichnis`*

   Dabei ist *`Zertifikatsverzeichnis`* das in Schritt 1 erstellte Verzeichnis.

   Mit diesem Befehl werden die Dateien `cert8.db` und `key3.db` im neuen Verzeichnis erstellt.
3. Fügen Sie der Zertifikatsdatenbank das Zertifikat der Zertifizierungsstelle (CA) oder das Verzeichnisserverzertifikat hinzu, indem Sie den entsprechenden Befehl für den Typ des Zertifikats eingeben:
   - Für CA-Zertifikate:

     `certutil -A -n` *`Zertifikatsname`* `-d` *`Zertifikatsverzeichnis`* `-i CA.cert -t C,C,C`
   - Für ein Verzeichnisserverzertifikat:

     `certutil -A -n` *`Zertifikatsname`* `-d` *`Zertifikatsverzeichnis`* `-i` *`Serverzertifikat`*`.cert -t P`

   Dabei ist *`Zertifikatsname`* ein von Ihnen zugewiesener Aliasname, wie z. B. der CA-Name oder der Hostname; *`Serverzertifikat`* ist das Präfix Zertifikatsdatei des Verzeichnisservers.
4. Kopieren Sie das Zertifikatsdatenbankverzeichnis in das Verzeichnis *`installationsposition`*`/configuration` jeder Speicherposition, an der Content Manager installiert ist.
5. Konfigurieren Sie den Verzeichnisserver für die Verwendung von LDAPS und starten Sie den Verzeichnisserver neu.

   Weitere Informationen finden Sie in der Dokumentation für den Verzeichnisserver.
6. Starten Sie IBM Cognos Configuration an allen Content Manager-Speicherpositionen, an denen Sie den LDAP-Namespace für die Verwendung des Verzeichnisservers konfiguriert haben.
7. Klicken Sie im Fenster **Explorer** unter **Sicherheit** > **Authentifizierung** auf den LDAP-Namespace.

8. Ändern Sie im Fenster **Eigenschaften** für die Eigenschaft **Host und Port** den Port in den sicheren LDAPS-Port.

   Geben Sie für die Eigenschaft **SSL-Zertifikatsdatenbank** den Pfad der Datei `cert7.db` an.

   Wichtig: 11.1.7 Sie können Ihren Namespace direkt konfigurieren. Das heißt, Sie müssen den Cognos Analytics-Service nicht erneut starten, nachdem Sie die Änderung konfiguriert haben. Stellen Sie in diesem Fall sicher, dass Sie für jeden Computer, auf dem der Content Manager-Service ausgeführt wird, denselben Wert konfigurieren. Andernfalls wird der Content Manager-Service auf den anderen Computern nicht gestartet. Stellen Sie außerdem sicher, dass die Datenbank auf jeden Content Manager-Computer kopiert wird.
9. Klicken Sie im Fenster **Explorer** mit der rechten Maustaste auf den LDAP-Namespace und klicken Sie auf **Test**.

   Wenn der Test fehlschlägt, ändern Sie die Eigenschaften so, dass das richtige Zertifikat verwendet wird.
10. Klicken Sie im Menü **Datei** auf **Speichern**.
11. Klicken Sie im Menü **Aktionen** auf **Neustart**.
12. Wiederholen Sie die Schritte 6 bis 11 in jedem Verzeichnis, in dem Content Manager installiert ist.

Aktivieren von Single Sign-on zwischen LDAP und IBM Cognos-Komponenten

Wenn Sie die Eigenschaft 'Externer Identitätsabgleich' konfigurieren, erhalten Sie die Möglichkeit des Single Sign-ons für die IBM Cognos-Komponenten.

Die Eigenschaft 'Externer Identitätsabgleich' kann sich auf eine CGI-Umgebungsvariable oder eine HTTP-Kopfzeilenvariable beziehen. Wenn ein Anwendungsserver-Gateway- oder Dispatchereintrag auf IBM Cognos-Komponenten verweist, kann der externe Identitätsabgleich die Sitzungsvariable `userPrincipalName` referenzieren. Der aufgelöste Wert der Zuordnungseigenschaft **Externer Identitätsabgleich** zur Laufzeit muss ein gültiger Benutzer-DN sein.

Wenn ein LDAP-Namespace so konfiguriert ist, dass er die Eigenschaft 'Externer Identitätsabgleich' zur Authentifizierung verwendet, stellt der LDAP-Provider eine Bindung zum Verzeichnisserver her, bei der er den Wert der Eigenschaft 'Benutzer-DN und Kennwort für Bindung' verwendet bzw. 'anonym', wenn kein Wert angegeben wird. Alle Benutzer, die sich mithilfe des externen Identitätsabgleichs bei IBM Cognos anmelden, sehen die gleichen Benutzer, Gruppen und Ordner wie die Bindungsbenutzer.

Wenn IBM Cognos-Komponenten mit Anwendungen funktionieren sollen, die Java oder Anwendungsserversicherheit verwenden, können Sie die Eigenschaft 'Externer Identitätsabgleich' so konfigurieren, dass die Benutzer-ID vom Java-Benutzerprincipal abgerufen wird. Schließen Sie das Token `${environment("USER_PRINCIPAL")}` in den Wert für die Eigenschaft ein. Weitere Informationen finden Sie in der Onlinehilfe für IBM Cognos Configuration.

Mit der Ersetzungsoperation können Sie in der Eigenschaft 'Externer Identitätsabgleich' begrenzte Ausdrücke bearbeiten.

Ersetzungsoperation

Die Ersetzungsoperation gibt eine Kopie der Zeichenfolge mit allen Vorkommen der alten Unterzeichenfolge zurück, die durch die neue Unterzeichenfolge ersetzt wurde.

Die folgenden Regeln gelten:

- In den Funktionsparametern wird das Zeichen \ als Escapezeichen verwendet. Für Zeichen wie \ und " sind Escapezeichen erforderlich.
- Verschachtelte Funktionsaufrufe werden nicht unterstützt.
- Sonderzeichen werden nicht unterstützt.

Syntax

```
${replace(str , old , new)}
```

Parameter für die Ersetzungsoperation

Tabelle 39. Parameter und Beschreibung für die Ersetzungsoperation

Parameter	Beschreibung
str	Die zu suchende Zeichenfolge.
old	Dei Unterzeichenfolge, die durch die neue Unterzeichenfolge ersetzt werden soll.
new	Die Unterzeichenfolge, die die alte Unterzeichenfolge ersetzt.

Beispiele

```
${replace(${environment("REMOTE_USER")},"NAMERICA\\",)}
```

```
${replace(${environment("REMOTE_USER")},"NAMERICA\\","")}
```

Konfigurieren von IBM Cognos für die Verwendung von SAP

Für die Verwendung eines SAP-Servers als Authentifizierungsprovider müssen Sie eine unterstützte SAP BW-Version verwenden.

In SAP BW können Sie Benutzer Benutzergruppen und Rollen zuweisen. Vom SAP-Authentifizierungsprovider werden nur die Rollen verwendet.

Welche Autorisierungsrechte vom SAP-Benutzer benötigt werden, hängt davon ab, ob die IBM Cognos-Komponenten von Benutzern oder von Administratoren verwendet werden.

SAP-Autorisierungseinstellungen für IBM Cognos-Benutzer

Die in der folgenden Tabelle aufgeführten Autorisierungsobjekte werden für jeden IBM Cognos-Benutzer benötigt.

Tabelle 40. SAP-Autorisierungseinstellungen für IBM Cognos-Benutzer

Autorisierungsobjekt	Feld	Wert
S_RFC Autorisierungsüberprüfung für RFC-Zugriff	Aktivität	
	Name des zu schützenden RFC	RFC1 RS_UNIFICATION, SDTX, SH3A, SU_USER, SYST, SUSO
	Typ des zu schützenden RFC	FUGR
S_USER_GRP Benutzerverwaltung: Benutzergruppen	Aktivität	03

Tabelle 40. SAP-Autorisierungseinstellungen für IBM Cognos-Benutzer (Forts.)		
Autorisierungsobjekt	**Feld**	**Wert**
	Name der Benutzergruppe	*

Einige Werte, wie zum Beispiel *, sind Standardwerte, die Sie möglicherweise für Ihre Umgebung modifizieren möchten.

SAP-Autorisierungseinstellungen für IBM Cognos-Administratoren

Wenn Benutzer administrative Aufgaben ausführen und nach Benutzern und Rollen suchen sollen, müssen dem Autorisierungsobjekt S_RFC zusätzlich zu den Werten für IBM Cognos-Benutzer die in der folgenden Tabelle aufgeführten Werte hinzugefügt werden.

Tabelle 41. SAP-Autorisierungseinstellungen für IBM Cognos-Administratoren		
Autorisierungsobjekt	**Feld**	**Wert**
S_RFC Autorisierungsüberprüfung für RFC-Zugriff	Aktivität	16
	RFC_NAME	PRGN_J2EE, SHSS, SOA3
	Typ des zu schützenden RFC-Objekts	FUGR

Einige Werte, wie zum Beispiel *, sind Standardwerte, die Sie für Ihre Umgebung modifizieren können.

Konnektivität zwischen SAP BW und IBM Cognos unter UNIX

Um zwischen SAP BW und IBM Cognos-Komponenten in einem UNIX-Betriebssystem eine Verbindung zu konfigurieren, stellen Sie sicher, dass Sie die (von SAP bereitgestellte) SAP-Datei der gemeinsam genutzten Bibliothek installieren und wie folgt zu der Bibliothekspfad-Umgebungsvariablen hinzufügen:

- AIX

  ```
  LIBPATH=$LIBPATH:<librfc.a_directory>
  ```

Konfigurieren eines SAP-Namespace

Sie können IBM Cognos-Komponenten so konfigurieren, dass ein SAP-Namespace als Authentifizierungsquelle verwendet wird.

Vorbereitende Schritte

Wenn Sie das IBM Cognos-Produkt auf einem 64-Bit-Server installiert haben, müssen Sie zudem die SAP-RFC-Bibliotheksdateien manuell in das IBM Cognos BI-Installationsverzeichnis kopieren.

Vorgehensweise

1. Bei Ausführung auf einem 64-Bit-Server gehen Sie folgendermaßen vor:
   - Wechseln Sie zu dem SAP-Installationsverzeichnis auf dem 64-Bit-Server.
   - Kopieren Sie alle 64-Bit-SAP-RFC-Bibliotheksdateien in das Verzeichnis *installationsposition*\bin64.

- Kopieren Sie alle 32-Bit-SAP-RFC-Bibliotheksdateien in das Verzeichnis *installationsposition*\bin.

2. Kopieren Sie bei Ausführung auf einem 32-Bit-Server alle 32-Bit-SAP-Bibliotheksdateien vom SAP-Installationsverzeichnis in das Verzeichnis *installationsposition*\bin64.
3. Öffnen Sie IBM Cognos Configuration in dem Verzeichnis, in dem Content Manager installiert ist.
4. Klicken Sie im Fenster **Explorer** unter **Sicherheit** mit der rechten Maustaste auf **Authentifizierung**. Klicken Sie dann auf **Neue Ressource** > **Namespace**.
5. Geben Sie im Feld **Name** einen Namen für den Authentifizierungs-Namespace ein.
6. Klicken Sie in der Liste **Typ** auf **SAP** und anschließend auf **OK**.

   Die neue Authentifizierungsprovider-Ressource wird im Fenster **Explorer** unter der Komponente **Authentifizierung** angezeigt.
7. Geben Sie im Fenster **Eigenschaften** für die Eigenschaft **Namespace-Kennung** eine eindeutige Kennung für den Namespace ein.

   Wichtig: Verwenden Sie keine Doppelpunkte (:) in der Eigenschaft 'Namespace-Kennung'.
8. Geben Sie die Werte für alle erforderlichen Eigenschaften an, um sicherzustellen, dass IBM Cognos-Komponenten den vorhandenen Authentifizierungsprovider finden und verwenden können.

   In Abhängigkeit von Ihrer Umgebung müssen Sie eventuell für die Eigenschaft **Host** dem SAP-Hostnamen die SAP Router-Zeichenfolge hinzufügen.
9. Wenn das SAP-System die Inhalte von Cookies verschlüsselt, aktivieren Sie die Funktion zum Entschlüsseln von Tickets:

   - Klicken Sie im Fenster **Eigenschaften** für **Erweiterte Eigenschaften** auf 'Wert' und dann auf das Bearbeitungssymbol.
   - Klicken Sie auf **Hinzufügen**.
   - Geben Sie den Namen `URLDecodeTickets` und den Wert `wahr` ein.
   - Klicken Sie auf **OK**.

   Vor der Herstellung einer Verbindung werden alle SAP-Anmeldetickets vom SAP-Namespace entschlüsselt.
10. Klicken Sie im Menü **Datei** auf **Speichern**.
11. Testen Sie die Verbindung zu einem neuen Namespace. Klicken Sie im Fenster **Explorer** unter **Authentifizierung** mit der rechten Maustaste auf die neue Authentifizierungsressource und klicken Sie auf **Test**.

    Sie werden dazu aufgefordert, die Berechtigungsnachweise für einen Benutzer im Namespace einzugeben, um den Test auszuführen.

    Abhängig von der Konfiguration des Namespace können Sie entweder eine gültige Benutzer-ID und ein gültiges Kennwort für einen Benutzer im Namespace eingeben oder den Wert der Eigenschaft 'Benutzer-DN und Kennwort für Bindung'.

Aktivieren der Einzelanmeldung zwischen SAP und IBM Cognos

Sie können die Einzelanmeldung (Single Sign-on) zwischen SAP Enterprise Portal und IBM Cognos-Komponenten sowie bei Verwendung der externen Namespace-Funktion der SAP BW-Datenquellenverbindungen aktivieren.

Stellen Sie für die Aktivierung sicher, dass Sie auf dem SAP BW-Server die folgenden Systemparameter festlegen:

- **login/accept_sso2_ticket = 1**
- **login/create_sso2_ticket = 1**
- **login/ticket_expiration_time = 200**

SiteMinder-Authentifizierungsprovider

Sie können IBM Cognos Analytics so konfigurieren, dass Sie einen SiteMinder-Namespace als Authentifizierungsquelle verwenden.

Der Authentifizierungsprovider verwendet das SiteMinder Software Development Kit, um einen benutzerdefinierten Agenten zu implementieren. Für die Bereitstellung von benutzerdefinierten Agenten müssen Sie in den Agenteneigenschaften der Server-Administrationskonsole für SiteMinder-Richtlinien angeben, dass Agenten der Version 4.x unterstützt werden.

SiteMinder - Konfigurationsanforderungen

Konfigurieren Sie die folgenden Elemente im CA SiteMinder-Richtlinienserver:

- Cognos Analytics 11.1.7 müssen einige Sonderzeichen und Zeichenfolgen in der Cognos Analytics-Server-URL zugelassen werden. Entfernen Sie zum Vermeiden von Fehlern die Anführungszeichen " (oder als %22 codiert) in den POST-Methoden aus der Liste im Parameter **BadURLChars** für das Agentenkonfigurationsobjekt im CA SiteMinder-Richtlinienserver. Dieses Zeichen ist für die GET-Methoden richtig codiert.

  Tipp: Kunden, die URLs in ihre Berichte integrieren, müssen die in den URL-Parametern übergebenen Zeichen überprüfen und sicherstellen, dass CA SiteMinder diese Zeichen nicht als **BadURLChars** oder **BadCSSChars** behandelt. Weitere Informationen finden Sie in der CA SiteMinder-Dokumentation.
- Cognos Analytics benötigt die Verben GET und POST für seine Funktionalität. Aktivieren Sie diese Verben im CA SiteMinder Policy Server.
- Aktivieren Sie die Codierung von Zeichen oder die Maskierung von Methoden, indem Sie die Eigenschaft **Ist Überprüfung einer möglichen XSS-Ausführung durch Drittanbieter aktiviert?** in Cognos Configuration auf 'True' setzen. Weitere Informationen finden Sie im Abschnitt „Konfigurieren von IBM Cognos-Komponenten für die Verwendung von IBM Cognos Application Firewall" auf Seite 182.

SiteMinder - konfiguriert für mehrere Benutzerverzeichnisse

Wenn Ihre SiteMinder-Umgebung für mehrere Benutzerverzeichnisse konfiguriert ist, müssen Sie in IBM Cognos Configuration den Namespace-Typ **SiteMinder** angeben.

Nach der Konfiguration des SiteMinder-Namespace in IBM Cognos Configuration müssen Sie IBM Cognos Configuration für jedes in SiteMinder definierte Benutzerverzeichnis auch einen entsprechenden LDAP- oder Active Directory Server-Namespace hinzufügen.

Bei der Konfiguration eines entsprechenden LDAP-Namespace müssen Sie sicherstellen, dass die Eigenschaft **Externer Identitätsabgleich** aktiviert und das Token **REMOTE_USER** im Eigenschaftswert enthalten ist. Dies bedeutet nicht, dass SiteMinder so konfiguriert werden muss, dass **REMOTE_USER** festgelegt werden muss.

Bei der Konfiguration eines entsprechenden Active Directory-Namespace müssen Sie sicherstellen, dass die Eigenschaft **singleSignonOption** auf **IdentityMapping** gesetzt ist.

Der **SiteMinder**-Namespace leitet Benutzerinformationen mithilfe der Umgebungsvariablen **REMOTE_USER** intern an den entsprechenden LDAP-Namespace weiter, sobald er eine erfolgreiche Benutzeridentifikation von der SiteMinder-Umgebung empfängt.

Weitere Informationen finden Sie im Abschnitt „Aktivieren der Einzelanmeldung zwischen Active Directory Server und IBM Cognos-Komponenten mit REMOTE_USER" auf Seite 268.

Wichtig: Achten Sie darauf, nur die Variable **REMOTE_USER** zu verwenden. Die Verwendung einer anderen Variablen kann eine Sicherheitslücke verursachen.

SiteMinder - konfiguriert für nur ein Benutzerverzeichnis

Wenn Ihre SiteMinder-Umgebung nur für ein Benutzerverzeichnis konfiguriert ist, brauchen Sie den Namespace-Typ **SiteMinder** nicht in IBM Cognos Configuration anzugeben.

In diesem Fall können Sie das Benutzerverzeichnis als Authentifizierungsquelle verwenden, indem Sie den passenden Namespace konfigurieren, oder Sie können den **SiteMinder**-Provider mit einem Benutzerverzeichnis konfigurieren. Wenn das SiteMinder-Benutzerverzeichnis beispielsweise LDAP ist, können Sie IBM Cognos-Komponenten mit einem LDAP-Namespace konfigurieren, aber auch mit einem **SiteMinder**-Namespace, der sich auf ein Benutzerverzeichnis bezieht, bei dem es sich um einen LDAP-Namespace handelt.

Wenn es sich beim SiteMinder-Benutzerverzeichnis um Active Directory handelt, können Sie einen Active Directory- oder einen LDAP-Namespace verwenden, der für die Verwendung mit Active Directory konfiguriert ist.

Wenn Sie das Benutzerverzeichnis direkt als Authentifizierungsquelle verwenden möchten, statt einen **SiteMinder**-Namespace festzulegen, können Sie den entsprechenden LDAP- oder Active Directory-Namespace konfigurieren. In diesem Fall sind die Agenten-Konfigurationsobjekt-Eigenschaften im SiteMinder-Richtlinienserver zu überprüfen. Stellen Sie sicher, dass **`SetRemoteUser`** aktiviert ist.

Bei der Konfiguration des Active Directory-Namespace müssen Sie sicherstellen, dass die Eigenschaft **`singleSignonOption`** auf **`IdentityMapping`** gesetzt ist.

Bei der Konfiguration eines entsprechenden LDAP-Namespace müssen Sie sicherstellen, dass die Eigenschaft **Externer Identitätsabgleich** aktiviert und das Token **`REMOTE_USER`** im Eigenschaftswert enthalten ist.

Weitere Informationen finden Sie im Abschnitt „Aktivieren der Einzelanmeldung zwischen Active Directory Server und IBM Cognos-Komponenten mit REMOTE_USER” auf Seite 268.

Wichtig: Achten Sie darauf, nur die Variable **`REMOTE_USER`** zu verwenden. Die Verwendung einer anderen Variablen kann eine Sicherheitslücke verursachen.

Konfigurieren eines SiteMinder-Namespace

Wenn Sie SiteMinder für mehrere Benutzerverzeichnisse konfiguriert haben, müssen Sie in IBM Cognos Configuration den Namespace-Typ **SiteMinder** angeben. Nach dem Hinzufügen des SiteMinder-Namespace, müssen Sie für jedes Benutzerverzeichnis in Ihrer SiteMinder-Umgebung auch einen entsprechenden LDAP-Namespace hinzufügen.

Den Namespace-Typ **SiteMinder** können Sie auch verwenden, wenn Ihre Benutzer auf einem LDAP- oder Active Directory-Server gespeichert sind.

Sie können den Namespace von Benutzern während der Anmeldung ausblenden. Dies ermöglicht Trusted-Sign-on-Namespaces (vertrauenswürdige Anmeldenamespaces), die nicht in der Namespace-Auswahlliste angezeigt werden, wenn sich Benutzer anmelden. Sie können zum Beispiel die Einzelanmeldung systemübergreifend integrieren, aber Ihren Kunden weiterhin die Möglichkeit geben, sich direkt bei IBM Cognos zu authentifizieren, ohne zur Auswahl eines Namespace aufgefordert zu werden.

Vorbereitende Schritte

Zur Verwendung des **SiteMinder**-Namespace benötigen Sie die nachfolgend aufgeführten Bibliotheksdateien von SiteMinder. Diese müssen Sie abrufen und dem Bibliothekspfad Ihres Betriebssystems hinzufügen.

Tabelle 42. SiteMinder-Bibliotheksdateien

Betriebssystem	**SiteMinder-Bibliotheksdatei**
AIX	`libsmagentapi.so`
Microsoft Windows 64-Bit	`smagentapi.dll` `smerrlog.dll`

Vorgehensweise

1. Fügen Sie auf dem Computer, auf dem Content Manager installiert ist, das Verzeichnis mit der SiteMinder-Bibliotheksdatei zur jeweiligen Umgebungsvariablen für den Bibliothekspfad hinzu.
   - Unter AIX: **LIBPATH**
   - Unter Microsoft Windows: **PATH**
2. Öffnen Sie IBM Cognos Configuration.
3. Klicken Sie im Fenster **Explorer** unter **Sicherheit** mit der rechten Maustaste auf **Authentifizierung** und klicken Sie dann auf **Neue Ressource** > **Namespace**.
4. Geben Sie im Feld **Name** einen Namen für den Authentifizierungs-Namespace ein.
5. Wählen Sie in der Liste **Typ** die Option **SiteMinder** und klicken Sie dann auf **OK**.
6. Wählen Sie den von Ihnen hinzugefügten Namespace aus.
7. Geben Sie für die Eigenschaft **Namespace-Kennung** eine eindeutige Kennung für den Namespace an.

   Tipp: Verwenden Sie in der Kennung keine Doppelpunkte (:).
8. Legen Sie auch die anderen erforderlichen Eigenschaften fest.

   Tipp: Wenn Sie nicht möchten, dass Benutzern beim Anmelden der Namespacename angezeigt wird, legen Sie für die Eigenschaft **Zur Authentifizierung auswählbar?** den Wert **Falsch** fest.
9. Klicken Sie im Fenster **Explorer** unter **Sicherheit** > **Authentifizierung** mit der rechten Maustaste auf den von Ihnen hinzugefügten Namespace und wählen Sie **Neue Ressource** > **SiteMinder-Richtlinienserver** aus.
10. Geben Sie in das Feld **Name** einen Namen für den Richtlinienserver ein und klicken Sie auf **OK**.
11. Legen Sie im Fenster **Eigenschaften** die Eigenschaft **Host** und alle anderen Eigenschaftswerte fest, die Sie ändern möchten.
12. Klicken Sie im Fenster **Explorer** mit der rechten Maustaste auf den von Ihnen hinzugefügten SiteMinder-Richtlinienserver und wählen Sie **Neue Ressource** > **Benutzerverzeichnis** aus.
13. Geben Sie in das Feld **Name** einen Namen für das Benutzerverzeichnis ein und klicken Sie auf **OK**.

    Wichtig: Der Name muss mit dem Namen des Benutzerverzeichnisses übereinstimmen, das auf dem Richtlinienserver vorhanden ist.
14. Geben Sie im Fenster **Eigenschaften** einen Wert für die Eigenschaft **Verweis auf Namespace-ID** ein.
15. Konfigurieren Sie für jedes Benutzerverzeichnis auf dem SiteMinder-Richtlinienserver ein Benutzerverzeichnis.
16. Klicken Sie auf **Datei** > **Speichern**.
17. Testen Sie die Verbindung zu einem neuen Namespace. Klicken Sie im Fenster **Explorer** unter **Authentifizierung** mit der rechten Maustaste auf die neue Authentifizierungsressource und klicken Sie auf **Test**.

    Sie werden dazu aufgefordert, die Berechtigungsnachweise für einen Benutzer im Namespace einzugeben, um den Test auszuführen.

    Abhängig von der Konfiguration des Namespace können Sie entweder eine gültige Benutzer-ID und ein gültiges Kennwort für einen Benutzer im Namespace eingeben oder den Wert der Eigenschaft 'Benutzer-DN und Kennwort für Bindung'.
18. Konfigurieren Sie für jedes Benutzerverzeichnis einen entsprechenden LDAP- oder Active Directory-Namespace.

    Stellen Sie sicher, dass Sie für die Eigenschaft **Namespace-Kennung** denselben Wert wie für die Eigenschaft **Namespace-Kennung** des SiteMinder-Namespace verwenden.

Löschen eines Authentifizierungsproviders

Sie können nicht mehr benötigte Namespaces löschen, die Sie hinzugefügt haben, oder Namespaces dekonfigurieren, die von IBM Cognos-Komponenten gefunden wurden.

Der Cognos-Namespace darf nicht gelöscht werden. Er enthält Authentifizierungsdaten, die für alle Benutzer gelten, und wird für die Speicherung der Konfiguration benötigt.

Nach dem Löschen eines Namespace können Sie sich nicht mehr bei diesem Namespace anmelden. Sicherheitsdaten für den Namespace verbleiben in Content Manager, bis Sie ihn dauerhaft aus dem Portal löschen. Weitere Informationen finden Sie in der Veröffentlichung *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Vorgehensweise

1. Öffnen Sie Cognos Configuration an jeder Position, an der Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Sicherheit** > **Authentifizierung** mit der rechten Maustaste auf den Namespace und klicken Sie dann auf **Löschen**.
3. Klicken Sie zur Bestätigung auf **Ja**.

   Der Namespace wird nicht mehr im Fenster **Explorer** angezeigt und Sie können sich in diesem Verzeichnis nicht mehr bei dem Namespace anmelden.
4. Klicken Sie im Menü **Datei** auf **Speichern**.
5. Wiederholen Sie die Schritte 1 bis 4 für jedes Verzeichnis, in dem Content Manager installiert ist.

   Sie müssen sich nun beim Portal anmelden und die Daten für den Namespace dauerhaft löschen. Weitere Informationen finden Sie im Handbuch *IBM Cognos AnalyticsVerwaltung und Sicherheit*.

Ergebnisse

Nach dem Löschen eines Namespace wird er im Portal als inaktiv angezeigt.

Kapitel 14. Verwalten der Leistung

In diesem Abschnitt wird die Verwendung von Tools und Metriken von IBM Cognos Analytics und anderen Anbietern beschrieben, mit denen Sie die Leistung Ihrer IBM Cognos Analytics-Umgebung verwalten können.

Systemleistungsmetriken

IBM Cognos Analytics stellt Systemmetriken bereit, mit denen Sie den Zustand des gesamten Systems, einschließlich aller einzelnen Server, Dispatcher und Services, überwachen können. Sie können auch die Schwellenwerte für die Metrikbewertungen festlegen. Systemleistungsmetriken sind z. B. die Anzahl der Sitzungen in Ihrem System, die Verweildauer von Berichten in Warteschlangen, die Ausführungsdauer einer Java Virtual Machine (JVM) und die Anzahl von Anforderungen und Prozessen im System.

Systemleistungsmetriken befinden sich zwar in der Java-Umgebung, können jedoch über das Portal in IBM Cognos Administration überwacht werden. Weitere Informationen zum Überwachen von Systemleistungsmetriken finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Sie können eine Momentaufnahme der aktuellen Systemmetriken erfassen, sodass Sie Trends über einen bestimmten Zeitraum verfolgen oder Details zum Systemstatus zu einem bestimmten Zeitpunkt überprüfen können. Weitere Informationen finden Sie im Abschnitt zur Metric-Dump-Datei im Handbuch *IBM Cognos Analytics Fehlerbehebung*.

Sie haben auch die Möglichkeit, außerhalb von IBM Cognos Administration Systemmetriken extern zu überwachen, indem Sie Java Management Extensions (JMX) nutzen. JMX ist eine Technologie, die Tools zum Verwalten und Überwachen von Anwendungen und serviceorientierten Netzen bereitstellt.

Externes Überwachen von Systemmetriken

Sie haben die Möglichkeit, mithilfe des Branchenstandards Java Management Extensions (JMX) Systemmetriken außerhalb von IBM Cognos Administration zu überwachen. Als Erstes konfigurieren Sie zwei JMX-Eigenschaften in IBM Cognos Configuration, um einen sicheren Zugriff auf Metriken in der Java-Umgebung zu ermöglichen. Dann stellen Sie mit einer sicheren Benutzer-ID und einem sicheren Kennwort über ein JMX-Verbindungstool eine Verbindung mit den Metriken her.

Vorbereitende Schritte

Sie müssen Oracle Java SE Development Kit oder das Java Software Development Kit von IBM installieren, um die Funktion für die externe Überwachung verwenden zu können.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration in dem Verzeichnis, in dem Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
3. Klicken Sie im Fenster **Eigenschaften** unter **Dispatcher-Einstellungen** auf **Externer JMX-Port**.
4. Geben Sie in der Spalte **Wert** eine verfügbare Portnummer ein.
5. Klicken Sie auf **Externer JMX-Berechtigungsnachweis**.
6. Klicken Sie in der Spalte **Wert** auf das Symbol **Bearbeiten**, geben Sie eine Benutzer-ID und ein Kennwort ein und klicken Sie auf **OK**.

   Benutzer-ID und Kennwort sorgen dafür, dass nur autorisierte Benutzer über den Port, der unter **Externer JMX-Port** festgelegt wurde, eine Verbindung zu der Java-Umgebung herstellen können, um die zu protokollierenden Benutzer festzulegen.
7. Speichern Sie die Änderungen und starten Sie den Service neu.
8. Um auf die Systemmetrikdaten zuzugreifen, geben Sie im JMX-Verbindungstool die folgenden Informationen an:

- den URL für die Verbindung mit den Systemmetrikdaten

  Zum Beispiel

  `service:jmx:rmi://Content_Manager_Server/jndi/rmi://Überwachungsserver:<JMXPort>/Proxyserver`

  wobei *JMXPort* der Wert ist, den Sie für **Externer JMX-Port** eingegeben haben, und *Content_Manager_Server* und *Überwachungsserver* Computernamen sind. Verwenden Sie nicht localhost, auch, wenn Sie lokal eine Verbindung herstellen.
- die Benutzer-ID und das Kennwort, um die Verbindung zu schützen

  Verwenden Sie die gleichen Werte, die Sie für **Externe JMX-Berechtigungsnachweis** konfiguriert haben.

Aktivieren von erforderlichen Services

Wenn Sie einige IBM Cognos Analytics-Services in Ihrer Umgebung nicht benötigen, können Sie diese inaktivieren, um die Leistung der anderen Services zu verbessern.

Um beispielsweise einen Computer für die Ausführung und Verteilung von Berichten abzustellen, können Sie den Präsentationsservice auf einem Computer mit Komponenten der Anwendungsebene inaktivieren. Wenn Sie diesen Service inaktivieren, verbessert sich die Leistung der Komponenten der Anwendungsebene.

Anmerkung:

- Der Präsentationsservice muss auf mindestens einem Computer in Ihrer IBM Cognos Analytics-Umgebung aktiviert bleiben.
- Wenn Sie Query Studio verwenden möchten, müssen Sie den Präsentationsservice aktivieren.
- Wenn Sie Analysis Studio verwenden möchten, müssen Sie den Berichtsservice aktivieren.
- Falls einige IBM Cognos Analytics-Komponenten nicht auf einem Computer installiert sind, sollten Sie die den fehlenden Komponenten zugeordneten Services inaktivieren. Andernfalls können bei der Ausführung der IBM Cognos Analytics-Komponenten ohne erkennbaren Grund Fehler auftreten.

IBM Cognos services

Nachdem Sie IBM Cognos Analyticsinstalliert und konfiguriert haben, ist ein Dispatcher standardmäßig auf jedem Computer verfügbar. Jeder Dispatcher verfügt über eine Gruppe zugehöriger Services, die in der folgenden Tabelle aufgelistet sind.

Tabelle 43. IBM Cognos services

Service	**Zweck**
Agentenservice	Führt Agenten aus. Wenn die Bedingungen für einen Agenten beim Ausführen des Agenten erfüllt werden, fordert der Agentenservice den Überwachungsservice auf, die Tasks auszuführen.
Anmerkungsservice	Ermöglicht die Hinzufügung von Kommentaren zu Berichten über den Arbeitsbereich von IBM Cognos . Diese Kommentare bleiben in allen Versionen des Berichts bestehen.
Stapelberichtsservice	Verwaltet Hintergrundanforderungen zum Ausführen von Berichten und stellt die Ausgabe für den Monitor-Service bereit.

Tabelle 43. IBM Cognos services (Forts.)	
Service	**Zweck**
Content Manager-Cacheservice	Verbessert die Gesamtsystemleistung und die Content Manager-Skalierbarkeit, indem häufige Abfrageergebnisse in den einzelnen Dispatchern zwischengespeichert werden.
Content Manager-Service	• Führt Objektbearbeitungsfunktionen im Content-Store aus, wie z. B. Hinzufügen, Abfragen, Aktualisieren, Löschen, Verschieben und Kopieren • Führt Content-Store-Management-Funktionen aus, z. B. Import und Export
Lieferservice	Sendet E-Mails an einen externen SMTP-Server im Namen anderer Services, wie z. B. den Berichtsservice, den Jobservice oder den Agentenservice.
Ereignisverwaltungsservice	Erstellt, Zeitpläne und verwaltet Ereignisobjekte, die Berichte, Jobs, Agenten, Wartungs-und Implementierungsimporte und -exporte darstellen.
Grafikservice	Erstellt Grafiken im Namen des Berichtsservice. Grafiken können in vier verschiedenen Formaten erzeugt werden: Raster, Vektor, Microsoft Excel XML oder PDF.
Benutzertaskservice	Ermöglicht die Erstellung und Verwaltung von Benutzertasks. Eine Benutzertask, wie z. B. die Genehmigung von Berichten, kann Einzelpersonen oder Gruppen auf einer Ad-hoc-Basis oder durch eine der anderen Services zugewiesen werden.
Interaktiven Erkennungsvisualisierungsservice	Wird von Cognos Workspace verwendet, um Visualisierungsempfehlungen bereitzustellen.
Jobservice	Führt Jobs aus, indem der Überwachungsservice signalisiert, dass Jobschritte im Hintergrund ausgeführt werden. Zu den Schritten gehören Berichte, andere Jobs, Import, Export usw.

Tabelle 43. IBM Cognos services (Forts.)

Service	**Zweck**
Protokollservice	Zeichnet Protokollnachrichten auf, die vom Dispatcher und anderen Services generiert werden. Der Protokollservice kann so konfiguriert werden, dass Protokollinformationen in einer Datei, einer Datenbank, einem fernen Protokollserver, einer Fenster Ereignisanzeige oder einem UNIX -Systemprotokoll aufgezeichnet werden. Die Protokollinformationen können anschließend von Kunden oder von Cognos Software Services analysiert werden, einschließlich: • Sicherheitsereignisse • System-und Anwendungsfehlerinformationen • ausgewählte Diagnoseinformationen
Metadatenservice	Stellt Unterstützung für Datenabstammungsinformationen bereit, die in Cognos Viewer, Reporting, Query Studio und Analysis Studio angezeigt werden. Abstammungsinformationen umfassen Informationen, wie z. B. Datenquellen und Berechnungsausdrücke.
Migrationsservice	Verwaltet die Migration von IBM Cognos Series 7 auf IBM Cognos Analytics.
Mobiler Service	Verwaltet Aktivitäten, die sich auf den IBM Cognos Analytics Mobile Reports -Client beziehen: • Transformiert Berichte und Analysen für den mobilen Verbrauch. • Komprimiert Berichts-und Analyseinhalte für die schnelle Verteilung von Luft auf die mobilen Geräte und den Zugriff von diesen Geräten. • Schiebt den Bericht und den Analyseinhalt auf die mobilen Geräte. • Ermöglicht eingehende und ausgehende berichtsbezogene und analysebezogene Anforderungen zwischen dem mobilen Gerät und der Umgebung, um Berichte zu durchsuchen, zu durchsuchen oder auszuführen. • Synchronisiert den mobilen Content-Store auf dem Server mit der mobilen Datenbank auf dem mobilen Gerät. • Übersetzt SOAP-Nachrichten (Simple Object Access Protocol) in drahtlos-freundliche Nachrichten. • Kommuniziert mit dem mobilen Gerät.

Tabelle 43. IBM Cognos services (Forts.)	
Service	**Zweck**
Überwachungsservice	• Verwaltet die Überwachung und Ausführung von Tasks, die terminiert, für die Ausführung zu einem späteren Zeitpunkt übergeben werden oder als Hintergrundtask ausgeführt werden. • Weist einen Zielservice für die Verarbeitung einer geplanten Task zu. Der Überwachungsservice kann beispielsweise den Stapelberichtsservice bitten, einen Bericht auszuführen, den Jobservice für die Ausführung eines Jobs oder den Agentenservice für die Ausführung eines Agenten. • Erstellt Protokollobjekte im Content Manager und verwaltet Failover und Wiederherstellung für die Ausführung von Einträgen.
PowerPlay -Service	Verwaltet Anforderungen zum Ausführen von PowerPlay -Berichten.
Präsentationsservice	• Konvertiert generische XML-Antworten von einem anderen Service in Ausgabeformat, wie z. B. HTML oder PDF • Stellt Anzeige-, Navigations-und Verwaltungsfunktionen bereit
Abfrageservice	Verwaltet dynamische Abfrageanforderungen und gibt das Ergebnis an den anfordernden Stapel-oder Berichtsservice zurück.
Service für relationale Metadaten	Wird von Framework Manager und CubeDesigner verwendet, um Metadaten aus relationalen Datenbanken zu importieren. Sie kann auch von Dynamic Query Analyzer zur Laufzeit verwendet werden.
Berichtsdatenservice	Manages the transfer of report data between IBM Cognos Analytics and applications that consume the data, such as IBM Cognos for Microsoft Office and IBM Cognos Analytics Mobile Reports.
Berichtsservice	Verwaltet interaktive Anforderungen zum Ausführen von Berichten und stellt die Ausgabe für einen Benutzer bereit.
Repository-Service	Verwaltet Anforderungen, um archivierte Berichtsausgaben aus einem Archivrepository oder Objektspeicher abzurufen.

Optimieren eines IBM Db2-Content Store

Wenn Sie als Content Store eine Db2-Datenbank verwenden, können Sie die Verarbeitungsgeschwindigkeit bei Anforderungen gezielt verbessern.

In Db2 werden Tabellen mit großen Objekten (Large Objects - LOBS) standardmäßig einem durch die Datenbank verwalteten Tabellenbereich zugewiesen. Die großen Objekte (LOBS) werden also nicht von den Db2-Pufferpools verwaltet. Dadurch werden direkte E/A-Anforderungen zu den LOBs generiert, was sich auf die Leistung auswirkt. Indem Sie Tabellen mit LOBs einem vom System verwalteten Tabellenbereich neu zuweisen, können Sie die Anzahl der direkten E/A-Anforderungen reduzieren.

Bevor Sie Änderungen an einem Db2-Content Store vornehmen, müssen Sie zur Umstrukturierung der Datenbank ausreichend Protokollspeicherbereich zuordnen.

Führen Sie die folgenden Schritte zum Neukonfigurieren des Db2-Content Store aus:

- Exportieren Sie die Daten aus den Tabellen, die mindestens ein LOB enthalten.
- Erstellen Sie die Tabellen in einem vom System verwalteten Tabellenbereich.
- Importieren Sie die Daten in die Tabellen.

Anpassen der Speicherressourcen für den IBM Cognos-Service

Um die Leistung in einer verteilten Umgebung zu verbessern, können Sie die Menge der vom IBM Cognos-Service verwendeten Ressourcen anpassen.

Standardmäßig ist der IBM Cognos-Service so konfiguriert, dass möglichst wenig Ressourcen beansprucht werden und die Startzeit so gering wie möglich ist.

Die Konfigurationseinstellungen für den IBM Cognos-Service sind nur für den Anwendungsserver gültig, den IBM Cognos Analytics standardmäßig verwendet. Wenn Sie IBM Cognos Analytics so konfigurieren möchten, dass die Anwendung auf einem anderen Anwendungsserver ausgeführt wird, dürfen Sie bei der Konfiguration der Ressourcen nicht IBM Cognos Configuration verwenden. Konfigurieren Sie stattdessen die Ressourcen innerhalb dieser Anwendungsserverumgebung.

Der IBM Cognos-Service steht nur auf Computern zur Verfügung, auf denen Content Manager oder die Komponenten der Anwendungsebene installiert sind.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration.
2. Erweitern Sie im Fenster **Explorer** die Optionen **Umgebung** > **IBM Cognos-Services** und klicken Sie dann auf **IBM Cognos**.
3. Ändern Sie im Fenster **Eigenschaften** den Wert für **Maximaler Speicher in MB**.
   - Wenn Sie die Startzeit, den Speicherbedarf und die verwendeten Ressourcen reduzieren möchten, verwenden Sie die Standardeinstellung 4096.
   - Dieser Wert kann auf der Basis der verfügbaren Systemressourcen angepasst werden.
4. Klicken Sie im Menü **Datei** auf **Speichern**.

Reduzieren der Zustellzeit für Berichte in einem Netz

Global versandte Berichte lassen sich an fernen Standorten langsamer öffnen als lokal. Außerdem lassen sich Berichte im HTML-Format langsamer öffnen als Berichte im PDF-Format, da für HTML-Berichte mehr Anforderungen bearbeitet werden.

Es gibt zwei Möglichkeiten, die Zustellzeiten von Berichten an fernen Standorten zu reduzieren. Sie können die Anzahl der Anforderungen zwischen Browser und Server reduzieren, indem Sie den Bericht im PDF-Format ausführen. Sind HTML-Berichte erforderlich, kann die Zustellung beschleunigt werden, indem an manchen der fernen Standorte zusätzliche Gateways konfiguriert werden. Statische Inhalte, wie z. B. Grafiken und Style-Sheets, werden dann schneller zugestellt.

Verlängern des asynchronen Zeitlimits in Umgebungen mit hoher Benutzerlast

Bei einer hohen Benutzerlast (über 165 Benutzer) und einer fortlaufenden Ausführung von Berichten in einer verteilten Umgebung kann es erforderlich sein, die Einstellung für das asynchrone Zeitlimit zu verlängern, um Fehlernachrichten zu vermeiden. Der Standardwert ist 30000.

Sie können zudem die Einstellung für das Warteschlangenzeitlimit auf den Wert 360 setzen. Informationen finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Um dieses Problem zu lösen, verlängern Sie das Warte-Zeitlimit.

Vorgehensweise

1. Wechseln Sie zum folgenden Verzeichnis:

   *installationsposition*webapps/p2pd/WEB-INF/services/.
2. Öffnen Sie die Datei reportservice.xml in einem Texteditor.
3. Ändern Sie den Parameter async_wait_timeout_ms parameter in 120000.
4. Speichern Sie die Datei.
5. Starten Sie den Service neu.

Kapitel 15. Manuelles Konfigurieren von IBM Cognos Analytics unter UNIX- und Linux-Betriebssystemen

An den UNIX- oder Linux-Computer, auf dem IBM Cognos Analytics installiert werden soll, ist möglicherweise eine Konsole angeschlossen, die keine Java-basierte grafische Benutzeroberfläche unterstützt.

Sie müssen die folgenden Aufgaben manuell ausführen:

__ • Ändern Sie die Standardkonfigurationseinstellungen durch Bearbeiten der Datei `cogstartup.xml` im Verzeichnis *installationsposition*`/configuration`.

__ • Ändern Sie die Sprach- oder Währungsunterstützung durch Bearbeiten der Datei `coglocale.xml` im Verzeichnis *install_location*`/configuration`.

__ • Wenden Sie die Konfiguration und die Ländereinstellungen auf Ihren Computer durch Ausführen von IBM Cognos Configuration im Hintergrundmodus an.

Bei jeder Installation müssen einige Konfigurationsschritte ausgeführt werden, damit IBM Cognos Analytics in Ihrer Umgebung funktioniert. Wenn Sie IBM Cognos Analytics-Komponenten auf mehrere Computer verteilen, müssen Sie die Reihenfolge beachten, in der die Computer konfiguriert und gestartet werden.

Andere Konfigurationsaufgaben sind optional und hängen von Ihrer jeweiligen Berichtsumgebung ab. Sie können das Standardverhalten von IBM Cognos Analytics ändern, indem Sie Eigenschaftswerte in der Datei `cogstartup.xml` bearbeiten. Weiterhin können Sie Beispieldateien verwenden, die es IBM Cognos Analytics ermöglichen, bereits in Ihrer Umgebung vorhandene Ressourcen zu nutzen.

Manuelles Ändern von Standardkonfigurationseinstellungen

Wenn die an Ihren UNIX- oder Linux-Computer angeschlossene Konsole keine Java-basierte grafische Benutzeroberfläche unterstützt, müssen Sie die Datei `cogstartup.xml` bearbeiten, um IBM Cognos Analytics so zu konfigurieren, dass das Programm in Ihrer Umgebung funktioniert.

Wichtig: Einige Konfigurationseinstellungen werden nur dann in der Datei `cogstartup.xml` gespeichert, wenn Sie diese über eine grafische Benutzeroberfläche vornehmen. Die Zeitzone für den Server wird beispielsweise für Ihre IBM Cognos-Komponenten nicht festgelegt, wenn Sie die Datei `cogstartup.xml` direkt ändern und anschließend IBM Cognos Configuration im Hintergrundmodus ausführen. In diesem Fall funktionieren andere Benutzereinstellungen, die auf der Zeitzone des Servers basieren, u. U. nicht mehr erwartungsgemäß.

Wenn IBM Cognos Analytics bereits in Ihrer Umgebung vorhandene Ressourcen wie beispielsweise einen Authentifizierungsprovider nutzen soll, können Sie der Konfiguration eine Komponente hinzufügen. Hierzu kopieren Sie den erforderlichen XML-Code aus den Beispieldateien in die Datei `cogstartup.xml` und passen dann die Werte an Ihre Umgebung an.

Standardmäßig wird die Datei `cogstartup.xml` mit UTF-8 codiert. Stellen Sie beim Speichern der Datei `cogstartup.xml` sicher, dass Sie die Codierung Ihrer Ländereinstellung an die verwendete Codierung anpassen. Die Codierung Ihrer Benutzerländereinstellung wird durch Ihre Umgebungsvariablen festgelegt.

Denken Sie bei der Bearbeitung der Datei `cogstartup.xml` daran, dass bei XML-Code zwischen Groß- und Kleinschreibung unterschieden wird. Dies gilt für alle Verwendungsarten von Text, auch Element- und Attributbeschriftungen sowie Elemente und Werte.

Bevor Sie die Datei `cogstartup.xml` bearbeiten, müssen Sie folgende Schritte ausführen:

- Erstellen Sie eine Sicherungskopie.
- Erstellen Sie einen Content Store auf einem verfügbaren Computer in Ihrem Netz.
- Überprüfen Sie die Konfigurationsanforderungen für Ihren Installationstyp.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *Installationsposition*/configuration.
2. Öffnen Sie die Datei cogstartup.xml in einem Editor.
3. Sie finden die Konfigurationseinstellung, die geändert werden soll, anhand der Hilfe- und Beschreibungskommentare, die vor dem Starttag der Elemente des Typs <crn:parameter> angezeigt werden.
4. Ändern Sie den Wert des Elements <crn:value> entsprechend Ihrer Umgebung.

   Tipp: Verwenden Sie das Attribut type, um den Datentyp für die Konfigurationseigenschaft zu bestimmen.
5. Wiederholen Sie die Schritte 3 bis 4, bis die Konfigurationswerte Ihrer Umgebung entsprechen.
6. Speichern Sie die Datei und schließen Sie sie.

Ergebnisse

Verwenden Sie einen überprüfenden XML-Editor, um sicherzustellen, dass Ihre Änderungen den Regeln in der Datei cogstartup.xsd entsprechen, die unter *installationsposition*/configuration gespeichert ist.

Hinzufügen von Komponenten zur Konfiguration

Die Datei cogstartup.xml enthält Konfigurationseinstellungen, die von IBM Cognos Analytics und Standardkomponenten verwendet werden. Sie können die von IBM Cognos Analytics verwendeten Komponenten ändern, indem Sie XML-Elemente aus Beispieldateien in die Datei cogstartup.xml kopieren. Anschließend können Sie die Konfigurationswerte bearbeiten, um sie an Ihre Umgebung anzupassen.

Wenn Sie zum Beispiel als Content Store eine Oracle-Datenbank verwenden möchten, können Sie die Beispieldatei ContentManager_*Sprachcode*.xml verwenden, um die Informationen zur Standard-Datenbankverbindung zu ersetzen.

IBM Cognos Analytics kann von den folgenden Elementen nur jeweils eine Instanz verwenden:

- Die für den Content Store angelegte Datenbank
- Einen Verschlüsselungsprovider
- Eine Konfigurationsvorlage für den IBM Cognos-Service

Sie sollten mit der Struktur von XML-Dateien vertraut sein, bevor Sie diese Dateien bearbeiten.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *installationsposition*/configuration/samples.
2. Wählen Sie eine Beispieldatei aus, die Sie in einem Editor öffnen möchten:
   - Zum Verwenden eines Oracle- oder IBM Db2-Content Store öffnen Sie die Datei ContentManager_*Sprachencode*.xml.
   - Um einen Authentifizierungsprovider zu verwenden, öffnen Sie die Datei Authentication_*Sprachcode*.xml.
   - Um einen Verschlüsselungsanbieter zu verwenden, öffnen Sie die Datei Cryptography_*Sprachcode*.xml.
   - Um Protokollnachrichten nicht in einer Datei zu speichern, sondern an ein anderes Ziel zu senden, öffnen Sie die Datei Logging_*Sprachcode*.xml.
   - Zum Verwenden einer mittleren oder großen Vorlage für die vom IBM Cognos Analytics-Prozess verwendeten Ressourcen öffnen Sie die Datei CognosService_*Sprachcode*.xml.
3. Kopieren Sie die benötigten Elemente.

   Tipp: Kopieren Sie den Code einschließlich der Start- und Endtags für das Element des Typs <crn:instance>.

Suchen Sie beispielsweise nach den Kommentaren (`Begin of`) und (`End of`):

```
<!--
(Begin of) Db2 template
-->
<crn:instance ...>
...
</crn:instance>
<!--
End of) Db2 template
-->
```

4. Wechseln Sie in das Verzeichnis *Installationsposition*`/configuration`.
5. Öffnen Sie die Datei `cogstartup.xml` in einem Editor.
6. Fügen Sie den Code aus der Beispieldatei in die Datei `cogstartup.xml` ein und ersetzen Sie das entsprechende Element des Typs `<crn:instance>`.
7. Ändern Sie die Werte dieser neuen Elemente entsprechend Ihrer Umgebung.

   Ändern Sie nicht das Klassenattribut für das Element `<crn:instance>`. Das Attribut "name" kann an die Umgebung angepasst werden.

   Wenn Sie beispielsweise eine Oracle-Datenbank als Content Store verwenden, ändern Sie lediglich das Attribut "name" entsprechend Ihrer Umgebung.

   ```
   <crn:instance class="Oracle" name="MyContentStore">
   ```
8. Speichern Sie die Datei und schließen Sie sie.
9. Führen Sie IBM Cognos Configuration im Hintergrundmodus aus, indem Sie den folgenden Befehl eingeben:

   ```
   ./cogconfig.sh -s
   ```

   Hiermit wird sichergestellt, dass die Datei gültig ist und die Kennwörter verschlüsselt werden.

Manuelles Ändern verschlüsselter Einstellungen

In der Datei `cogstartup.xml` können Sie verschlüsselte Einstellungen manuell ändern, zum Beispiel Kennwörter und Benutzerberechtigungsnachweise.

Wenn Sie den Wert für das Verschlüsselungsflag auf "false" setzen, wird in IBM Cognos Configuration eine Eingabeaufforderung angezeigt, um eine verschlüsselte Einstellung zu speichern.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *Installationsposition*`/configuration`.
2. Öffnen Sie die Datei `cogstartup.xml` in einem Editor.
3. Sie finden die verschlüsselte Einstellung, die geändert werden soll, anhand der Hilfe- und Beschreibungskommentare, die vor dem Starttag der Elemente des Typs `<crn:parameter>` angezeigt werden.
4. Ändern Sie den Wert des Elements `<crn:value>` entsprechend Ihrer Umgebung.

   Tipp: Verwenden Sie das Attribut "type", um den Datentyp für die Konfigurationseigenschaft zu bestimmen.
5. Ändern Sie den Verschlüsselungswert in "false".

   Zum Beispiel

   ```
   <crn:value encrypted="false">
   ```
6. Wiederholen Sie die Schritte 3 bis 5, bis die Konfigurationswerte Ihrer Umgebung entsprechen.
7. Speichern Sie die Datei und schließen Sie sie.
8. Geben Sie den folgenden Konfigurationsbefehl ein:

   ```
   ./cogconfig.sh -s
   ```

Ergebnisse

Die neuen Einstellungen werden gespeichert und verschlüsselt.

Globale Einstellungen unter UNIX- und Linux-Betriebssystemen

Wenn die an Ihren UNIX- oder Linux-Computer angeschlossene Konsole keine Java-basierte grafische Benutzeroberfläche unterstützt, müssen Sie die Datei `coglocale.xml` manuell bearbeiten.

Sie können globale Einstellungen ändern, ...

- ... um die für die Benutzeroberfläche verwendete Sprache anzugeben, wenn die Sprache in der Ländereinstellung des Benutzers nicht verfügbar ist
- ... um die in Berichten verwendete Ländereinstellung anzugeben, wenn die Ländereinstellung des Benutzers nicht verfügbar ist
- ... um Währungs- oder Ländereinstellungsunterstützung für die Daten- und Metadatenberichterstellung hinzuzufügen
- ... um Sprachunterstützung zur Benutzeroberfläche hinzuzufügen

Die IBM Cognos Analytics-Komponenten stellen standardmäßig sicher, dass für alle Ländereinstellungen, die aus unterschiedlichen Quellen stammen und in verschiedenen Formaten vorliegen können, ein normalisiertes Format verwendet wird. Dies bedeutet, dass alle erweiterten Ländereinstellungen den Einstellungen für eine Sprache und einen regionalen Code entsprechen.

Bevor Sie der Benutzeroberfläche Sprachunterstützung hinzufügen können, müssen Sie die Sprachdateien auf allen Computern in der verteilten Installation installieren. Weitere Informationen erhalten Sie bei Ihrem Supportmitarbeiter.

Beispiel 1

Ein Bericht steht in Content Manager in zwei Ländereinstellungen zur Verfügung, z.B. en-us (Englisch-USA) und fr-fr (Französisch-Frankreich), die Ländereinstellung des Benutzers ist jedoch auf fr-ca (Französisch-Kanada) festgelegt. IBM Cognos verwendet die Ländereinstellungszuordnung, um zu ermitteln, welcher Bericht dem Benutzer angezeigt wird.

IBM Cognos überprüft zunächst, ob der Bericht in Content Manager für die Ländereinstellung des Benutzers verfügbar ist. Wenn dies nicht der Fall ist, ordnet IBM Cognos die Ländereinstellung des Benutzers einer normalisierten Ländereinstellung zu, die auf der Registerkarte "Inhaltsländereinstellungszuordnungen" konfiguriert ist. Da die Ländereinstellung des Benutzers fr-ca lautet, wird sie der Ländereinstellung fr zugeordnet. IBM Cognos kann anhand dieser Zuordnung überprüfen, ob der Bericht in fr verfügbar ist. Im vorliegenden Fall ist der Bericht nur in en-us und fr-fr, nicht aber in fr verfügbar.

Als Nächstes ordnet IBM Cognos allen verfügbaren Berichten eine normalisierte Ländereinstellung zu. Auf diese Weise wird en-us zu en und fr-fr zu fr.

Da sowohl die Berichts- als auch die Benutzerländereinstellung dem Wert fr zugeordnet sind, wird der Bericht für den Benutzer mit der Ländereinstellung fr-ca mit der Ländereinstellung fr-fr gespeichert.

Beispiel 2

Die Ländereinstellung des Benutzers und die Berichtsländereinstellungen sind derselben Sprache zugeordnet. IBM Cognos entscheidet, welche Ländereinstellung verwendet wird. Wenn die Ländereinstellung eines Benutzers beispielsweise en-ca (Englisch-Kanada) lautet und die Berichte in en-us (Englisch-USA) sowie en-gb (Englisch-Großbritannien) zur Verfügung stehen, ordnet IBM Cognos jede Ländereinstellung dem Wert en zu. Der Bericht wird dem Benutzer mit denjenigen Ländereinstellungen angezeigt, die IBM Cognos auswählt.

Beispiel 3

Der Bericht und die Benutzerländereinstellungen sind keiner gemeinsamen Sprache zugeordnet. IBM Cognos wählt die Sprache aus. In diesem Fall müssen Sie eine Zuordnung konfigurieren. Wenn ein

Bericht beispielsweise in en-us (Englisch-USA) und fr-fr (Französisch-Frankreich) zur Verfügung steht, als Ländereinstellung des Benutzers jedoch es-es (Spanisch-Spanien) festgelegt ist, wählt IBM Cognos die Sprache aus.

Manuelles Ändern der globalen Einstellungen unter UNIX- und Linux-Betriebssystemen

Führen Sie die folgenden Schritte durch, um die globalen Einstellungen mithilfe der Datei `coglocale` unter UNIX und Linux zu ändern.

Vorgehensweise

1. Navigieren Sie auf allen Computern, auf denen Content Manager installiert ist, zum Verzeichnis *`installationsposition`*`/configuration`.
2. Öffnen Sie die Datei `coglocale.xml` in einem Editor.
3. Ergänzen oder ändern Sie das erforderliche Element und Attribut zwischen den entsprechenden Start- und Endtags.

   Die Elemente und Attribute sowie die Start- und Endtags sind in der folgenden Tabelle aufgeführt:

Tabelle 44. Tags für globale Einstellungen

Elementtyp	**Starttag**	**Endtag**
Sprache	<supportedProductLocales>	</supportedProductLocales>
Inhaltsländereinstellungen	<supportedContentLocales>	</supportedContentLocales>
Währung	<supportedCurrencies>	</supportedCurrencies>
Produktländereinstellungszuordnung	<productLocaleMap>	</productLocaleMap>
Inhaltsländereinstellungszuordnung	<contentLocaleMap>	</contentLocaleMap>
Schriftarten	<supportedFonts>	</supportedFonts>
Cookieeinstellungen, Archivverzeichnis für Berichte	<parameter name="*Einstellung*">	</parameter>

   Tipp: Löschen Sie zur Aufhebung der Unterstützung das Element.
4. Speichern Sie die Datei und schließen Sie sie.

Ergebnisse

Tipp: Verwenden Sie einen überprüfenden XML-Editor, um sicherstellen, dass Ihre Änderungen den Regeln in der Datei `cogstartup.xsd` entsprechen, die unter *`installationsposition`*`/configuration` gespeichert ist.

Wenn Sie einen Währungscode hinzufügen, der nicht unterstützt wird, müssen Sie ihn manuell der Datei `i18n_res.xml` im Verzeichnis *`installationsposition`*`/bin/` hinzufügen. Kopieren Sie diese Datei auf alle IBM Cognos-Computer Ihrer Installation.

Starten und Stoppen von Cognos Analytics im Hintergrundmodus unter UNIX und Linux

IBM Cognos Configuration wird im Hintergrundmodus ausgeführt, um auf UNIX- oder Linux-Computern, die keine Java-basierte grafische Benutzerschnittstelle unterstützen, Konfigurationseinstellungen anzuwenden und Services zu starten.

Bevor Sie das Konfigurationstool im Hintergrundmodus ausführen, sollten Sie sicherstellen, dass die Datei `cogstartup.xml` den in der Datei `cogstartup.xsd` definierten Regeln entsprechend gültig ist. Die Datei `cogstartup.xsd` befindet sich im Verzeichnis *installationsposition*`/configuration`.

Starten von Cognos Analytics im Hintergrundmodus unter den Betriebssystemen UNIX und Linux

Führen Sie die nachfolgenden Schritte aus, um die IBM Cognos Analytics-Software im Hintergrundmodus zu starten.

Vorgehensweise

1. Stellen Sie sicher, dass die Datei `cogstartup.xml`, die sich im Verzeichnis *installationsposition*`/configuration` befindet, für Ihre Umgebung geändert wurde.

   Weitere Informationen finden Sie im Abschnitt „Manuelles Ändern von Standardkonfigurationseinstellungen” auf Seite 307.
2. Wechseln Sie in das Verzeichnis *installationsposition*`/bin64`.
3. Geben Sie den folgenden Befehl ein:

   ```
   ./cogconfig.sh -s
   ```

   Tipp: Um Protokollnachrichten anzuzeigen, die während einer unbeaufsichtigten Konfiguration generiert wurden, öffnen Sie die Datei `cogconfig_response.csv` im Verzeichnis *installationsposition*`/logs`.

Ergebnisse

IBM Cognos Configuration wendet die in der Datei `cogstartup.xml` angegebenen Konfigurationseinstellungen an, verschlüsselt Berechtigungsnachweise, generiert digitale Zertifikate und startet gegebenenfalls den Cognos-Service oder -Prozess.

Stoppen von Cognos Analytics im Hintergrundmodus unter den Betriebssystemen UNIX und Linux

Führen Sie die nachfolgenden Schritte aus, um die IBM Cognos Analytics-Software im Hintergrundmodus zu beenden.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *installationsposition*`/bin64`.
2. Geben Sie den folgenden Befehl ein:

   ```
   ./cogconfig.sh -stop
   ```

Kapitel 16. Deinstallieren von IBM Cognos Analytics

Sie müssen Programme ordnungsgemäß deinstallieren, damit alle Dateien und Änderungen an Systemdateien vollständig entfernt werden. Zum Deinstallieren von IBM Cognos Analytics müssen Sie die Serverkomponenten und Modellierungstools deinstallieren.

Wenn Sie IBM Cognos Analytics in einer Anwendungsserverumgebung ausführen, müssen Sie das mit dem Anwendungsserver mitgelieferte Administrationstool verwenden, um die laufende Anwendung zu stoppen und die Bereitstellung des Java-Teils der IBM Cognos Analytics-Komponenten zurückzunehmen. In vielen Anwendungsservern werden die bereitgestellten Anwendungsdateien oder Verzeichnisse beim Zurücknehmen der Bereitstellung nur unvollständig entfernt, d. h., Sie müssen diese gegebenenfalls manuell entfernen. Nachdem Sie die Bereitstellung von IBM Cognos Analytics-Komponenten zurückgenommen haben, führen Sie die in diesem Abschnitt für UNIX bzw. Microsoft Windows angegebene Schrittfolge zur Deinstallation aus.

Tipp: Wenn Überwachungstools, wie z. B. Process Explorer oder MMC (Microsoft Management Console), während der Deinstallation aktiv sind, beeinträchtigen sie das Löschen der Services. Dies gilt für alle Services im Allgemeinen. Zum Beispiel werden nach der Deinstallation von Cognos Analytics Produktservices, wie z. B. ApacheDS, IBM Cognos und Informix, nicht vollständig entfernt, sondern werden in der Serviceanzeige als gestoppt und inaktiviert angezeigt. Um dies zu vermeiden, sorgen Sie dafür, dass keine Überwachungstools während der Deinstallation aktiv sind. Wenn diese Überwachungstools nach der Deinstallation beendet werden, wird auch das Entfernen der Services abgeschlossen.

Wichtig: Löschen Sie keine Konfigurations- und Datendateien, wenn Sie auf eine neue Version von IBM Cognos Analytics aktualisieren und die Konfigurationsdateien mit der neuen Version verwenden möchten.

Wichtig: Die Anwendung und die zugehörigen Services müssen gestoppt werden, damit der Deinstallationsprozess abgeschlossen werden kann. Beachten Sie, dass das Stoppen der Services bis zu 15 Minuten in Anspruch nehmen kann.

Deinstallieren von IBM Cognos Analytics unter UNIX oder Linux

Wenn Sie IBM Cognos Analytics nicht mehr benötigen oder unter Ihrem UNIX- bzw. Linux-Betriebssystem eine Aktualisierung des Betriebssystems durchführen möchten, deinstallieren Sie IBM Cognos Analytics.

Bei der Deinstallation werden keine Dateien entfernt, die nach der Installation geändert wurden, wie zum Beispiel Konfigurations- und Benutzerdatendateien. Das Installationsverzeichnis verbleibt auf dem Computer und diese Dateien bleiben so lange erhalten, bis Sie sie manuell löschen.

Vorgehensweise

1. Wenn die an Ihren Computer angeschlossene Konsole keine Java-basierte grafische Benutzeroberfläche unterstützt, ermitteln Sie die Prozess-ID (PID) des IBM Cognos Analytics-Prozesses durch Eingabe des folgenden Befehls:

   ```
   ps -ef | grep cogbootstrapservice
   ```
2. Stoppen Sie den IBM Cognos Analytics-Prozess:
   - Wenn Sie mit XWindows arbeiten, starten Sie IBM Cognos Configuration und klicken Sie im Menü **Aktionen** auf **Stoppen**.
   - Wenn Sie nicht mit XWindows arbeiten, geben Sie Folgendes ein:

     ```
     kill -TERM pid
     ```
3. Zum Deinstallieren von IBM Cognos Analytics wechseln Sie in das Verzeichnis *install_location/uninstall* und geben Sie den entsprechenden Befehl ein:
   - Geben Sie für XWindows Folgendes ein:

     ```
     ./Uninstall_IBM_Cognos_Analytics
     ```

- Wenn Sie nicht mit XWindows arbeiten, führen Sie eine unbeaufsichtigte Deinstallation durch (siehe Verwenden einer unbeaufsichtigten Deinstallation).

4. Folgen Sie den Eingabeaufforderungen, um die Deinstallation abzuschließen.
5. Löschen Sie alle temporären Internet-Dateien aus dem Web-Browser.

Deinstallieren von Cognos Analytics unter Microsoft Windows-Betriebssystemen

Wenn Sie IBM Cognos Analytics nicht mehr benötigen oder eine aktuelle Version installieren möchten, deinstallieren Sie alle IBM Cognos Analytics-Komponenten sowie den IBM Cognos-Service.

Wenn Sie mehrere Komponenten im gleichen Pfad installiert haben, können Sie mithilfe des Deinstallationsassistenten auswählen, welche Packages deinstalliert werden sollen. Alle Komponenten des Package werden deinstalliert. Sie müssen den Deinstallationsvorgang auf jedem Computer wiederholen, auf dem IBM Cognos Analytics-Komponenten installiert sind.

Es ist nicht erforderlich, unter einem Microsoft Windows-Betriebssystem die Konfigurations- und Datendateien zu sichern. Diese Dateien bleiben bei der Deinstallation erhalten.

Schließen Sie alle Programme, bevor Sie IBM Cognos Analytics deinstallieren. Andernfalls werden möglicherweise nicht alle Dateien entfernt.

Bei der Deinstallation werden keine Dateien entfernt, die nach der Installation geändert wurden, wie zum Beispiel Konfigurations- und Benutzerdatendateien. Das Installationsverzeichnis verbleibt auf dem Computer und diese Dateien bleiben so lange erhalten, bis Sie sie löschen. Löschen Sie keine Konfigurations- und Datendateien, wenn Sie auf eine neue Version von IBM Cognos Analytics aktualisieren und die Konfigurationsdateien mit der neuen Version verwenden möchten.

Vorgehensweise

1. Suchen Sie im Menü **Start** mit der Programmliste die Anwendung IBM Cognos Analytics. Klicken Sie mit der rechten Maustaste auf den Anwendungsnamen und klicken Sie auf **Deinstallieren**.

   Wenn Sie nicht auf das Menü **Start** zugreifen können, wechseln Sie in das Verzeichnis *installationsposition*\uninstall und führen Sie das Programm Uninstall_IBM Cognos Analytics.exe aus.
2. Befolgen Sie die Anweisungen zur Deinstallation der Komponenten.

   In der Datei cognos_uninst_log.htm werden die Aktivitäten aufgezeichnet, die der Deinstallationsassistent beim Deinstallieren von Dateien durchführt.

   Tipp: Die Protokolldatei finden Sie im Verzeichnis Temp.
3. Löschen Sie alle temporären Internet-Dateien aus dem Web-Browser.

   Weitere Informationen finden Sie in Ihrer Web-Browser-Dokumentation.

Wiederherstellung nach einer nicht erfolgreichen Deinstallation

Wenn eine Deinstallation nicht erfolgreich durchgeführt wurde, sind Dateien, Registry-Einträge und Services, die gelöscht werden sollten, möglicherweise noch vorhanden. Der vorliegende Abschnitt enthält Richtlinien, die sich sowohl auf Installationen des Typs "Easy Install" als auch auf benutzerdefinierte Installationen beziehen.

Vorgehensweise

1. Für Installationen des Typs "Easy Install" und Erstinstallationen:
   a) Entfernen Sie Informix, indem Sie den Informix-Deinstallationsbefehl ausführen:

   ```
   Installationsposition\informix\bin\ifxdeploy.exe -u Installationsposition\informix -delifx
   ```

a) Entfernen Sie den folgenden Registrierungsschlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Informix\Online\ol_cognoscm.

b) Entfernen Sie den Installationsordner *Installationsposition*.

c) Wenn es sich hierbei um die einzige InstallAnywhere-basierte Installation auf der Maschine handelt, können Sie die InstallAnywhere-Registry-Datei entfernen: %PROGRAM FILES%\Zero G Registry\.com.zerog.registry.xml.

2. Für alle anderen Installationen:

a) Entfernen Sie den Installationsordner *Installationsposition*.

b) Wenn es sich hierbei um die einzige InstallAnywhere-basierte Installation auf der Maschine handelt, können Sie die InstallAnywhere-Registry-Datei entfernen:

Unter Windows (verborgenes Verzeichnis): %PROGRAM FILES%\Zero G Registry\.com.zerog.registry.xml

Unter UNIX: Registry-Datei: .com.zerog.registry.xml an der folgenden Speicherposition:

- Bei einer Anmeldung als Root befindet sich die globale Registry in /var.
- Bei einer Anmeldung als Benutzer befindet sich die globale Registry im Ausgangsverzeichnis des Benutzers.

Wenn Sie den Status der InstallAnywhere-Installationen nicht genau kennen, können Sie diese Datei umbenennen und so eine Kopie davon aufbewahren.

Kapitel 17. IBM Cognos content archival

Das Speichern archivierter Inhalte in Ihrem externen Repository bietet Ihnen die Möglichkeit, die Anforderungen an die Einhaltung von Vorschriften einzuhalten und die Skalierbarkeit und Leistung von IBM Cognos -Produkten zu verbessern, indem Sie die Größe des Inhalts im Content-Store reduzieren.

The software supports an IBM FileNet Content Manager with IBM FileNet CMIS external repository. Wenn IBM Filenet CMIS Version 1 der installierten Software bereits installiert ist, müssen Sie diese Software mit Fixpack, Version 2, aktualisieren. Die Inhaltsarchivierung kann auch für die Verwendung Ihres Dateisystems konfiguriert werden.

Administratoren erstellen eine Datenquellenverbindung zu einem externen Repository, damit Inhalte aus dem Content-Store in das Repository verschoben werden können. Benutzer können dann den archivierten Inhalt im externen Repository anzeigen. Durch die Bereitstellung von Suchergebnissen für aktuelle und archivierte Inhalte können Benutzer kritische Vergleiche zwischen aktuellen Daten und historischen Daten vornehmen. Dieser effiziente Mechanismus ermöglicht es Ihrem Unternehmen, die Anforderungen von Unternehmen und Behörden zu erfüllen und gleichzeitig eine nahtlose Benutzererfahrung zu bieten.

Der Inhalt, der im externen Repository archiviert wurde, wird nicht in der IBM Cognos -Umgebung verwaltet. Wenn Sie zum Beispiel Berichte in IBM Cognos Analyticslöschen, werden die archivierten Ausgaben nicht in Ihrem externen Repository gelöscht.

Informationen zur Verwaltung Ihrer Archive finden Sie im *IBM Cognos Analytics Administration and Security Guide*.

Für die Archivierung Ihrer Inhalte gibt es zwei Workflow-Szenarien. Der erste Workflow ermöglicht es Administratoren, Pakete und Ordner nach der Installation von IBM Cognos Content Archival-Software zu archivieren. Der zweite Workflow ermöglicht es Administratoren, Repository-Verbindungen für neue Pakete und Ordner zu erstellen.

Workflow 1: Inhalt nach der Installation der Konnektivitätssoftware archivieren

Administratoren können gespeicherte Berichtsausgaben für bestimmte Pakete und Ordner oder für alle Pakete und Ordner nach der Installation oder dem Upgrade von IBM Cognos Analyticsarchivieren. Dieser Workflow muss nur einmal ausgeführt werden, da sich der gesamte Inhalt derzeit in Ihrem Content-Store befindet.

- Erstellen Sie eine Datenquellenverbindung mit dem externen Repository.
- Wählen Sie Repository-Verbindungen für die Pakete und Ordner aus, die archiviert werden müssen.
- Erstellen und führen Sie eine Task zur Verwaltung von Inhaltsarchiven aus, um Ordner und Pakete auszuwählen, die im externen Repository archiviert werden sollen.

Sobald Sie eine Repository-Verbindung für Pakete und Ordner festgelegt haben, wird jede neue Berichtsausgabe automatisch archiviert. Dies bedeutet, dass die Wartungsaufgabe für den Inhalt des Inhalts nicht erneut ausgeführt werden muss.

Workflow 2: Repository-Verbindungen für neue Pakete und Ordner erstellen

Administratoren können Repository-Verbindungen für neue Pakete und Ordner erstellen, indem sie die folgenden Tasks ausführen:

- Erstellen Sie eine Datenquellenverbindung mit dem externen Repository.
- Wählen Sie Repository-Verbindungen für die Pakete und Ordner aus, die archiviert werden müssen.

Verwaltungsaufgaben für Inhaltsarchivierung verwenden

Die Task zur Verwaltung von Inhaltsarchiven erstellt einen Verweis auf die Berichtsversionen in den Ordnern und Paketen, die Sie auswählen und konfigurieren. Durch die Auswahl von Ordnern und Paketen

wird der Inhalt innerhalb des Inhalts markiert, der im Content-Store verbleiben kann, bis er in Ihrem externen Repository archiviert wird.

Es ist wichtig zu beachten, dass diese Task Ihren Inhalt nicht aus dem Content-Store in das externe Repository verschoben hat. Sie müssen zuerst Repository-Verbindungen für Ihre Pakete und Ordner auswählen. Berichtsversionen in Ordnern und Paketen, die nicht für die Archivierung markiert sind, stehen zum Löschen aus dem Content Store zur Verfügung.

Sobald der Inhalt markiert ist, ist die Content-Archivierungstask abgeschlossen. Eine Hintergrundtask in Content Manager findet die markierten Elemente und kopiert sie und speichert sie im externen Repository.

Durch den Import von Inhalt in einen Ordner oder ein Paket, der für die Archivierung in einem externen Repository konfiguriert ist, wird der importierte Inhalt nicht automatisch in das Repository verschoben und archiviert. Ein Administrator muss für diesen Ordner oder das Paket eine Wartungstask für die Inhaltsarchivierung ausführen, um den importierten Inhalt zu archivieren.

Hintergrundtasks

Die XML-Hintergrundtasks, die zum Verschieben von Inhalt aus dem Content-Store in das externe Repository verwendet werden, sind 'archiveTask.xml' und 'deleteTask.xml'. Die Datei archiveTask.xml verschiebt den markierten Inhalt in ein externes Repository. Sie können diese Datei auch verwenden, um Thread-Ausführungszeiten und Archivierungsausgaben ausgewählter Formate festzulegen. Die Datei "deleteTask.xml" ist eine Konfigurationsdatei, die markierte Versionsobjekte aus der Warteschlange abruft und löscht. Sie sollten diese Datei nicht ändern.

Inhalt-IDs vor dem Archivieren bewahren

Falls erforderlich, können Sie die Inhalts-IDs beibehalten, bevor die Berichtsausgabe archiviert wird.

Objekte im Content-Store verfügen über Inhalts-IDs, die standardmäßig gelöscht und durch neue IDs ersetzt werden, wenn Sie eine Importimplementierung ausführen und Inhalte in eine Zielumgebung verschieben. Es kann jedoch Situationen geben, in denen Sie Inhalts-IDs beibehalten müssen, z. B. wenn die Berichtsausgabe in ein externes Berichtsrepository verschoben wird.

Inhaltsarchivierung konfigurieren

Sie müssen Ihre Umgebung für die Inhaltsarchivierung konfigurieren. Damit die Konfigurationsänderungen wirksam werden, müssen Sie die IBM Cognos -Services stoppen und starten.

Dateiposition für ein Dateisystemrepository erstellen

Wenn Sie Berichte oder Berichtsspezifikationen in einem Systemrepository des IBM Cognos -Inhaltsarchivdateisystems archivieren möchten, müssen Sie ein Aliasstammverzeichnis erstellen, das auf eine Dateiposition auf einem lokalen Laufwerk oder auf einem lokalen Netzwerk verweist.

Vorbereitende Schritte

Sie müssen ein Administrator sein und Zugriff auf die Dateiposition haben. Content Manager-Komponenten und Komponenten der Anwendungsebene müssen über eine Datei-URI auf diese Position zugreifen können.

Vorgehensweise

1. Stoppen Sie bei der Ausführung den IBM Cognos -Service.
2. Starten Sie IBM Cognos Konfiguration.
3. Klicken Sie auf **Aktionen** > **Bearbeiten Sie die globale Konfiguration.**

4. Wählen Sie auf der Registerkarte **Allgemein** die Option **Aliaswurzeln**aus, klicken Sie auf das Wertfeld, klicken Sie auf die Schaltfläche "Bearbeiten", und klicken Sie dann auf **Hinzufügen**, wenn das Dialogfeld **Wert-Alias-Roots** angezeigt wird.
5. Geben Sie in der Spalte **Alias-Stammname** einen eindeutigen Namen für das Dateisystemrepository ein.

   Anmerkung: Es gibt keine Begrenzung für die Anzahl der Aliasnamen, die Sie erstellen können.
6. Geben Sie den Pfad zu Ihrer Dateisystemposition ein, wobei file-system-path für den vollständigen Pfad zu einer vorhandenen Dateiposition steht:
   - Geben Sie in Fensterin der Spalte **windowsURI** den Typ `file:///` gefolgt vom lokalen Pfad ein, z. B. `file:///c:/file-systempfad` oder geben Sie `file://` gefolgt vom Servernamen und dem Freigabepfad ein, z. B. `file://server/share`.
   - Geben Sie in UNIX oder Linuxin der Spalte **unixURI** `file:///` gefolgt vom lokalen Pfad ein, z. B. `file:///file-systempfad`.

   Anmerkung: Relative Pfade, wie z. B. `file:/// ../file-system-path`, werden nicht unterstützt.

   In einer verteilten Installation müssen sowohl die Content Manager-als auch die Application-Tier-Komponenten-Computer über Zugriff auf die Dateiposition verfügen. Verwenden Sie beide URIs nur in einer verteilten Installation. Der UNIX -URI und der Fenster -URI in einem Aliasstammverzeichnis müssen auf dieselbe Position im Dateisystem verweisen.
7. Klicken Sie auf **OK**.
8. Starten Sie den IBM Cognos -Service erneut. Dies kann einige Minuten dauern.

Ergebnisse

Verwenden Sie diesen Namen des Dateisystemrepositorys, um eine Datenquellenverbindung zu erstellen, die mit der Cognos -Content-Archivierungs-Software verwendet werden kann. Weitere Informationen finden Sie im *IBM Cognos Administration and Security Guide.* .

Angepasste Klassen-Definitionen und -Eigenschaften in IBM FileNet Content Manager importieren

Wenn Sie die Inhaltsarchivierung von IBM Cognos verwenden möchten, müssen Sie eine Gruppe von angepassten Klassen und Eigenschaftendateien in IBM FileNet Content Manager importieren.

Zu den Definitionen und Eigenschaften von angepassten Klassen gehören FileNet -spezifische Metadaten. Sie können angepasste Klassen und Eigenschaftendateien zu jeder Zeit installieren.

Vorgehensweise

1. Wenn Sie eine FileNet-Archivierung eingerichtet haben, wechseln Sie in das Verzeichnis *Installationsposition*`/configuration/repository/filenet/upgrade/`.
2. Wenn die FileNet-Archivierung nicht bereits konfiguriert ist, wechseln Sie in das Verzeichnis *Installationsposition*`/configuration/repository/filenet/new/` .
3. Kopieren Sie die `CMECMIntegrationObjects_CEExport. _xxx.xml` -Dateien in einen lokalen Ordner auf dem FileNet -Server.
4. Öffnen Sie das FileNet Enterprise Manager-Verwaltungstool und stellen Sie eine Verbindung zur Domäne für das externe FileNet -Repository her.
5. Wählen Sie einen Zielobjektspeicher aus, und klicken Sie auf **Alle Elemente importieren** , um die Definitionen in den Objektspeicher zu importieren.
6. Klicken Sie im Teilfenster "Importoptionen" auf **Manifestdatei importieren** , und navigieren Sie zu der Position, in der sich die `CMECMIntegrationObjects_CEExport. _xxx.xml` -Dateien befinden.
7. Wählen Sie die `CMECMIntegrationObjects_CEExport_Manifest.xml` -Datei aus und klicken Sie auf **Importieren**.

8. Starten Sie die FileNet Content Engine-und FileNet -CMIS-Anwendung erneut, um die Änderungen auf Ihre Umgebung anzuwenden.

   Anmerkung: Es kann eine lange Zeit dauern, bis Änderungen an allen FileNet-Knoten aktualisiert werden.

Angepasste Klassen-Definitionen und -Eigenschaften in IBM Content Manager 8 importieren

To use IBM Cognos content archival with IBM Content Manager 8, you must import a set of custom classes and properties files. Sie müssen auch die CMIS-Konfigurationsdatei mit den Ordnertypen IBM Cognos aktualisieren.

Zu den Definitionen und Eigenschaften von angepassten Klassen gehören IBM Content Manager 8-spezifische Metadaten. Sie können angepasste Klassen und Eigenschaftendateien zu jeder Zeit installieren.

Da es keinen Ressourcenmanager gibt, der während des Installationsprozesses definiert ist, gibt es während des Importprozesses Konfliktfehlernachrichten.

Vorbereitende Schritte

Sie müssen IBM Content Manager 8 mit einem externen Repository von IBM Content Manager 8 CMIS Version 1.1 installiert haben.

Vorgehensweise

1. Öffnen Sie den Content Manager 8 **Systemverwaltungsclient**.
2. Klicken Sie im Hauptmenü auf **Werkzeuge** > **XML importieren**.
3. Im **XML-Importoptionen importieren** -Fenster wird der Abschnitt **Zu importierende Datei** :
   - Klicken Sie im Feld **Datenmodelldatei** auf **Durchsuchen**, und wählen Sie die `CMECMIntegration-Types_RMImport_Manifest.xsd` -Datei aus, aus der die Objekte importiert werden sollen.
   - Klicken Sie im Feld **Verwaltungsobjektdatei** auf **Durchsuchen**, und wählen Sie die Datei `CMEC-MIntegrationTypes_RMImport_MimeTypes.xml` aus, um die Datei mit den Verwaltungsobjekten zu importieren.

   Die Standardposition ist das Verzeichnis *`Installationsposition`*`/configuration/repository/contentManager8/Neu` .
4. Um Konflikte anzuzeigen, wählen Sie im **XML-Importoptionen importieren** -Fenster unter **Verarbeitungsoptionen**die Option **Interaktiv verarbeiten**aus.
5. Klicken Sie auf **Importieren** , um den Importprozess zu starten.
   a) Erweitern Sie im Fenster **Preprocessor-Ergebnisse importieren** den Eintrag **Elementtypen**, und klicken Sie doppelt auf einen Elementtyp, der auf einen Konflikt hinweist.
   b) Wählen Sie im Fenster **Details der Importdefinition und der Zieldefinition** in der Spalte **Resultierendes Ziel** die Namen für die **Ressourcenmanager** und die **Sammlung** aus, die erstellt wurden, als Sie Content Manager 8 installiert haben, und klicken Sie auf **Akzeptieren**.
   c) Wiederholen Sie die Schritte a und b für jeden Elementtyp, der einen Konflikt anzeigt.
6. Nachdem Sie alle Konflikte gelöst haben, klicken Sie im **Preprocessor-Ergebnisse importieren** -Fenster auf **Weiter**.
7. Klicken Sie im Fenster **Importauswahl bestätigen** auf **Importieren**.
8. Klicken Sie nach Abschluss des Imports auf **OK**.
9. Wenn Sie die CMIS-Konfigurationsdatei aktualisieren möchten, um die Ordnertypen von IBM Cognos zu ermitteln, führen Sie das Konfigurationsprogramm CMIS for Content Manager 8 aus, um ein Profil zu erstellen.
10. Öffnen Sie die `cmpathservice.properties` -Datei im Ordner IBM CMIS for Content Manager-Konfigurationsprofile.

Für UNIXlautet der Standarddateipfad: `/opt/IBM/CM_CMIS/profiles/profile1`

Für Fensterlautet der Standarddateipfad: `C:\Programmdatei\IBM\CM_CMIS \profiles\profile1`

a) Suchen Sie die `FolderTypes` -Zeile.

b) Fügen Sie die IBM Cognos -Ordner "COGNOSREPORT" und "REPORTVERSION" in Großbuchstaben hinzu. Trennen Sie die einzelnen Ordnertypen durch ein Komma voneinander.

```
For example,
folderTypes = ClbFolder,COGNOSSREPORT,REPORTVERSION
```

c) Speichern und schließen Sie die Datei.

11. Führen Sie das Konfigurationsprogramm für CMIS for Content Manager 8 aus und wählen Sie die Option zum automatischen erneuten Implementieren der CMIS-Konfigurationsdatei aus.

    Anmerkung: Weitere Informationen zur manuellen Implementierung von CMIS finden Sie unter IBM CMIS for Content Manager manuell implementieren (http://pic.dhe.ibm.com/infocenter/cmgmt/v8r4m0/topic/com.ibm.installingcmcmis.doc/cmsde001.htm).

12. Starten Sie in der Administrationskonsole von WebSphere Application Server Liberty Profile den **CMIS for Content Manager-Anwendung**erneut.

Zur Verfügung stehende Zeit für die Ausführung des Archivierungsprozesses angeben

Um eine hohe Systemleistung während der Spitzenzeiten zu gewährleisten, können Sie einen Blackoutzeitraum konfigurieren, um anzugeben, wann die Archivierungs-oder Löschtasks ausgeführt werden.

Ein Blackoutzeitraum ist ein temporärer Zeitraum, in dem die Datenversetzung verweigert wird. Ein Blackoutzeitraum ist standardmäßig nicht definiert, wenn die Software installiert ist.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *Installationsposition*`/webapps/p2pd/WEB-INF/cm/tasks/manager`.
2. Öffnen Sie die `tasksManager.xml` -Datei mithilfe eines XML-Texteditors.
3. Zum Beispiel, um eine wöchentliche Blackoutperiode von 8.00 bis 17.00 Uhr anzugeben, Dienstag bis Freitag fügen Sie das folgende `< blackoutPeriods>` -Element als untergeordnetes Element des Elements `BackgroundTasksManager` hinzu.
   - Startzeit = `< hour> 08 < /hour>`
   - Stoppzeit = `< hour> 17 < /hour>`
   - Tage =

```
<day>Tuesday</day>
<day>Wednesday</day>
<day>Thursday</day>
<day>Friday</day>
```

4. Falls erforderlich, verringern Sie die Anzahl der Threads, die für die Archivierungs-und Löschprozesse verfügbar sind. Die maximale Anzahl an Threads ist 7.
5. Speichern und schließen Sie die Datei.
6. Starten Sie Hintergrundaktivitäten für den Content Manager-Service erneut.

Threadausführungszeit angeben

Sie können Threads verwenden, um die Verarbeitungszeit des Betriebssystems zu planen.

Das Archiv und das Löschen von Hintergrundtasks verwenden Threads, um Inhalte zu verschieben. Threads sind Einheiten der Verarbeitungszeit, die vom Betriebssystem geplant werden.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *Installationsposition*/webapps/p2pd/WEB-INF/cm/tasks/config .
2. Öffnen Sie die archiveTask.xml -Datei mithilfe eines XML-Texteditors.
3. Beispiel: Um drei Threads zu konfigurieren, die von Mitternacht bis 8.00 Uhr ausgeführt werden, ein Thread, der von 8.00 Uhr bis 17.00 Uhr ausgeführt wird, keine Threads, die von 17.00 Uhr bis Mitternacht ausgeführt werden, und alle Threads, die jeden Tag der Woche ausgeführt werden, fügen Sie das folgende < executionPeriods> -XML-Element als untergeordnetes Element des Elements BackgroundTask hinzu.

```
            <executionPeriods>
        <executionPeriod>
            <threads>3</threads>
            <startTime>
                <hour>00</hour>
                <minute>00</minute>
            </startTime>
            <stopTime>
                <hour>08</hour>
                <minute>00</minute>
            </stopTime>
            <days>
                <day>Monday</day>
                <day>Tuesday</day>
                <day>Wednesday</day>
                <day>Thursday</day>
                <day>Friday</day>
                <day>Saturday</day>
                <day>Sunday</day>
            </days>
        </executionPeriod>
        <executionPeriod>
            <startTime>
                <hour>08</hour>
                <minute>00</minute>
            </startTime>
            <stopTime>
                <hour>17</hour>
                <minute>00</minute>
            </stopTime>
            <days>
                <day>Monday</day>
                <day>Tuesday</day>
                <day>Wednesday</day>
                <day>Thursday</day>
                <day>Friday</day>
                <day>Saturday</day>
                <day>Sunday</day>
            </days>
        </executionPeriod>
    </executionPeriods>
```

4. Speichern und schließen Sie die Datei.

Ausgewählte Formate von Berichtsausgaben archivieren

Sie können die Archivierung einschränken, um die Archivierung auf bestimmte Ausgabeformate zu beschränken. Standardmäßig werden Ausgaben eines beliebigen Formats, einschließlich PDF, XML, HTML und Excel, archiviert.

Sie können die Archivierung bestimmter Ausgabeformate auf das Repository beschränken.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *Installationsposition*/webapps/p2pd/WEB-INF/cm/tasks/config .
2. Öffnen Sie die archiveTask.xml -Datei mithilfe eines XML-Texteditors.

3. Wenn Sie beispielsweise die Archivierung nur von PDF-Berichtsausgabeversionen definieren möchten, fügen Sie das folgende < outputFormats> -XML-Element als untergeordnetes Element des XML-Elements RunOptions hinzu.

```
<outputFormats>
            <outputFormat>PDF</outputFormat>
        </outputFormats>
```

Sie können das vorhandene Beispielelement Ausgabeformate verwenden und die Liste so ändern, dass Ausgabeformate angegeben werden, die archiviert werden sollen.

Es ist nicht möglich, mehrere Ausgabeversionen von Dateiberichten selektiv zu archivieren, z. B. HTML mit Grafiken.

Speichern und schließen Sie die Datei.

Angeben, dass Berichtsspezifikationen nicht archiviert werden

Standardmäßig wird die Ausgabe der Berichtsspezifikation archiviert. Die Berichtsspezifikationen beschreiben, wie Daten in einem Bericht generiert wurden.

Um die Archivierung von Berichtsspezifikationen zu inaktivieren, müssen Sie zwei Dateien ändern: CM.xmlund CM_FILENET.xml oder CM_CM8.xml, je nachdem, ob Sie Ihren Inhalt in einem IBM FileNet Content Manager-Repository oder einem IBM Content Manager 8-Repository archivieren.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *Installationsposition*/webapps/p2pd/WEB-INF/repositories/config .
2. Öffnen Sie die CM.xml -Datei mithilfe eines XML-Texteditors.
3. Entfernen Sie die folgende Zeile, oder entfernen Sie die folgende Zeile: < property name="Spezifikationen " metadataPropertyName = "Spezifikation" useTempFile = "true"
4. Speichern und schließen Sie die Datei.
5. Wechseln Sie in das Verzeichnis *Installationsposition*/webapps/p2pd/WEB-INF/repositories/config .
6. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie Ihren Inhalt in FileNetarchivieren, öffnen Sie die Datei mit dem Namen CM.FILENET.xml in einem Texteditor.
   - Wenn Sie Ihren Inhalt in IBM Content Manager 8 archivieren, öffnen Sie die Datei mit dem Namen CM.xml in einem Texteditor.
7. Entfernen Sie das folgende Element oder entfernen Sie das folgende Element:

```
<property repositoryName="REPORTEXECUTIONSPECIFICATION" repositoryType="ASSOCIA
TED"
metadataPropertyName="specification">
                                <associatedObjectTypes>
                                     <objectType name="VERSIONSPECIFICATION">
                                         <properties>
                                            <property repositoryName="cmis:name"
repositoryType="STRING"
metadataPropertyName="reportVersionDefaultName"  valueHandler="com.cognos.cm.
repositoryPluginFramework.
PropertyValueAppendStringHandler" valueHandlerArgument="_specification"/>
                                             </properties>
                                        </objectType>
                                </associatedObjectTypes>
                            </property>
```

Anmerkung: In der CM.xml -Datei ist der objectType, Name -Wert < objectType name=" $t!-2_VERSIONSPECIFICATIONv-1 ">.

8. Starten Sie Hintergrundaktivitäten für den Content Manager-Service erneut. Weitere Informationen finden Sie im *IBM Cognos Analytics Administration and Security Guide*.

Anhang A. Befehlszeilenoptionen für IBM Cognos Configuration

Sie können das Verhalten von IBM Cognos Configuration beim Startvorgang ändern, indem Sie den Konfigurationsbefehl mit Befehlszeilenoptionen eingeben.

Tabelle 45. Befehlszeilenoptionen und zugehörige Beschreibungen

Option	**Beschreibung**
`-h`	Zeigt Befehle für IBM Cognos Configuration an.

`-s`	Führt IBM Cognos Configuration im Hintergrundmodus aus.
	Die in der Datei `cogstartup.xml` angegebenen Eigenschaftswerte werden zur Konfiguration der installierten Komponenten verwendet, um alle Services zu starten.
	`./cogconfig.sh -s`
	`cogconfig.bat -s`

`-stop`	Stoppt alle IBM Cognos-Services.
	`./cogconfig.sh -stop`
	`cogconfig.bat -stop`

`-startupfile` *`Pfad/Dateiname.xml`*	Führt IBM Cognos Configuration mit einer anderen Datei als der Datei `cogstartup.xml` im Verzeichnis *`installationsposition`*`/configuration` aus.

`-test`	Verwendet in der Datei `cogstartup.xml` angegebene Eigenschaftswerte zum Testen von Konfigurationseinstellungen.
	`./cogconfig.sh -test`
	`cogconfig.bat -test`

`-notest`	Startet IBM Cognos Configuration, wobei die automatischen Testaufgaben inaktiviert sind.
	`./cogconfig.sh -notest`
	`cogconfig.bat -notest`
	Diese Option sollte nicht verwendet werden, wenn das Produkt zum ersten Mal gestartet wird oder wenn Konfigurationsänderungen vorgenommen werden.

Tabelle 45. Befehlszeilenoptionen und zugehörige Beschreibungen (Forts.)	
Option	**Beschreibung**

`-utf8`	Speichert die Konfiguration in der UTF-8-Codierung.
	`./cogconfig.sh -s -utf8`
	`cogconfig.bat -s -utf8`

`-l` *Sprachen-ID*	Führt IBM Cognos Configuration in der Sprache aus, die durch die Sprachen-ID angegeben ist.
	Zum Ausführen des Konfigurationstools im Hintergrundmodus in vereinfachtem Chinesisch:
	`./cogconfig.sh -l zh-cn`
	`cogconfig.bat -l zh-cn`

`-e` *Dateiname.xml*	Exportiert die aktuellen Konfigurationseinstellungen in die angegebene Datei.
	`./cogconfig.sh -e` *Dateiname*`.xml`
	`cogconfig.bat -e` *Dateiname*`.xml`

`-log`	Erstellt die Fehlerdatei `cogconfig.`*Zeitstempel*`.log` im Verzeichnis*Cognos_Position*`/logs`.
	`./cogconfig.sh -log`
	`cogconfig.bat -log`
	11.1.2 Die Protokolldatei 'cogconfig.log' wird standardmäßig ohne die Option '-log' im Verzeichnis *cognos_location*`/logs` erstellt.

`-d`	Aktiviert die Debugprotokollierung in der Protokolldatei. Diese Option muss in Verbindung mit der Option '-log' verwendet werden. 11.1.2 Die Protokolldatei 'cogconfig.log' wird standardmäßig erstellt. Sie können die Option -d ohne die Option '-log' verwenden.

`-config`	Speichert IBM Cognos Configuration im unbeaufsichtigten Modus. Lädt Eigenschaftswerte, die in der Datei 'cogstartup.xml' für IBM Cognos Configuration angegeben wurden, und speichert sie anschließend im unbeaufsichtigten Modus, ohne dass die Services gestartet werden.
	`./cogconfig.sh -config`
	`cogconfig.bat -config`

Es können mehrere Befehlszeilenoptionen gleichzeitig verwendet werden. IBM Cognos Configuration kann beispielsweise im Hintergrundmodus ausgeführt werden und alle Fehlernachrichten in einer Protokolldatei aufzeichnen.

Anhang B. Fehlerbehebung

Diese Referenzinformationen und Lösungen zur Fehlerbehebung sollen Ihnen als Ressource bei der Lösung von bestimmten Problemen dienen, die insbesondere während oder nach der Installation von IBM Cognos-Komponenten auftreten können.

Die Probleme werden anhand der Symptome charakterisiert. Jedes Symptom kann mithilfe spezieller Tools und Techniken zur Fehlerbehebung auf eine oder mehrere Ursachen zurückgeführt werden. Nach der Ursachenermittlung werden die Probleme durch die Durchführung einer Reihe von Aktionen behoben.

Protokolldateien unterstützen Sie bei der Fehlerbehebung. Die Support Community, die über die IBM Support-Website verfügbar ist, bietet ebenfalls wertvolle Unterstützung bei der Fehlerbehebung. Die Support Community kann für alle IBM Cognos-Produkte mit Problemlösungen unterstützen.

Wenn Sie ein Problem nicht selbst lösen können, erhalten Sie Unterstützung von einem Mitarbeiter des Kundenservice. Der Kundenservicemitarbeiter benötigt für die Fehleranalyse Informationen über die Situation und die aufgetretenen Symptome. Ermitteln Sie daher die erforderlichen Daten zur Fehleranalyse, bevor Sie sich mit dem Kundenservice in Verbindung setzen.

Fehlerbehebung bei Problemen

Bei der *Fehlerbehebung* handelt es sich um einen systematischen Ansatz zum Beheben von Problemen. Das Ziel der Fehlerbehebung besteht in der Feststellung der Ursachen für einen Fehler, der dazu führt, dass Funktionen nicht wie vorgesehen arbeiten, und in der Ermittlung der geeigneten Maßnahmen zur Behebung des Problems.

Der erste Schritt innerhalb des Fehlerbehebungsprozesses besteht in der vollständigen Beschreibung des Problems. Problembeschreibungen helfen Ihnen und der technischen Unterstützungsfunktion von IBM bei der Eingrenzung der Fehlerursache. Im Rahmen dieses Schrittes sollten Sie die folgenden grundlegenden Fragen beantworten:

- Welche Fehlersymptome treten auf?
- Wo tritt der Fehler auf?
- Wann tritt der Fehler auf?
- Unter welchen Bedingungen tritt der Fehler auf?
- Kann der Fehler reproduziert werden?

Die Antworten auf diese Fragen ergeben normalerweise eine gute Beschreibung des Fehlers, die dann in eine Lösung zur Behebung des Problems umgesetzt werden kann.

Welche Fehlersymptome treten auf?

Wenn Sie mit der Fehlerbeschreibung beginnen, dann ist die naheliegendste Frage: "Was ist das Problem?" Diese Frage erscheint auf den ersten Blick zu allgemein. Allerdings können Sie sie in mehrere gezielte Teilfragen untergliedern, die ein aussagekräftigeres Bild des Problems ergeben. Diese Fragen können sich auf folgende Faktoren beziehen:

- Welche Person oder Einheit meldet den Fehler?
- Welche Fehlercodes und Nachricht wurden ausgegeben?
- Wie hat sich der Fehler auf dem System geäußert? Beispiel: Ist das Problem das Auftreten einer Schleife, einer Blockierung, eines Absturzes, eines Leistungsabfalls oder fehlerhafter Ergebnisse?

Wo tritt der Fehler auf?

Die Ermittlung der Einheit, auf die der Fehler zurückzuführen ist, ist nicht immer einfach. Es handelt sich dabei jedoch um einen der wichtigsten Schritte bei der Behebung eines Fehlers. Zahlreiche Technologieebenen können zwischen der Einheit, die den Fehler meldet, und den Komponenten liegen, auf

denen der Fehler aufgetreten ist. Netze, Platten und Treiber sind nur einige der Komponenten, die bei der Untersuchung von Fehlern berücksichtigt werden müssen.

Die folgenden Fragen helfen Ihnen bei der Isolierung der Ebene Ihres Systems, auf der der Fehler aufgetreten ist:

- Tritt der Fehler ausschließlich auf einer bestimmten Plattform oder unter einem bestimmten Betriebssystem oder bei mehreren Plattformen oder Betriebssystemen auf?
- Wird die momentan verwendete Umgebung und Konfiguration unterstützt?

Wenn auf einer Ebene ein Fehler gemeldet wird, dann ist es nicht zwingend so, dass dieser Fehler auch seinen Ursprung in dieser Ebene hat. Eine wichtige Voraussetzung zur Identifizierung einer Fehlerursache besteht in der Kenntnis der Umgebung, in der er aufgetreten ist. Nehmen Sie sich ausreichend Zeit, um die fehlerhafte Umgebung ausführlich zu beschreiben und berücksichtigen Sie dabei auch das Betriebssystem und dessen Version, alle vorhandenen Softwareprodukte sowie deren Versionen und die verwendete Hardware. Überprüfen Sie, ob die Umgebung, in der Sie arbeiten, unterstützt wird. Zahlreiche Probleme können auf nicht kompatible Softwareversionen zurückgeführt werden, die nicht zusammen eingesetzt werden sollten, oder die in Bezug auf ihren gemeinsamen Einsatz nicht ausreichend getestet wurden.

Wann tritt der Fehler auf?

Stellen Sie einen detaillierten Zeitplan der Ereignisse auf, die zu einem Fehler geführt haben. Berücksichtigen Sie dabei insbesondere Vorkommnisse, die nur einmal aufgetreten sind. Ein Zeitplan lässt sich einfach aufstellen, indem Sie die Ereignisse ausgehend vom Zeitpunkt der Fehlermeldung (möglichst exakt und wenn möglich im Millisekundenbereich) rückwärts rekonstruieren und dann die verfügbaren Protokolle und Daten zurückverfolgen. Normalerweise müssen Sie nur bis zum ersten verdächtigen Ereignis zurückgehen, das sie in einem Protokoll der Diagnoseprogramme vorfinden.

Zur Entwicklung eines detaillierten Zeitplans der Ereignisse sollten Sie die folgenden Fragen beantworten:

- Tritt das Problem nur zu einer bestimmten Tages- oder Nachtzeit auf?
- Wie oft tritt das Problem auf?
- Welche Abfolge von Ereignissen ist bis zum Zeitpunkt der Fehlermeldung aufgetreten?
- Tritt der Fehler nach einer Änderung der Umgebung (z. B. nach einem Upgrade oder einer Software- oder Hardwareinstallation) weiterhin auf?

Unter welchen Bedingungen tritt der Fehler auf?

Die Klärung der Frage, welche Systeme und Anwendungen zum Fehlerzeitpunkt ausgeführt wurden, ist ein wichtiger Faktor bei der Fehlerbehebung. Diese Fragen zu Ihrer Umgebung können Sie bei der Identifizierung der Fehlerursache unterstützten:

- Tritt der Fehler immer auf, wenn die gleiche Aufgabe ausgeführt wird?
- Stellt eine gewisse Abfolge von Ereignissen die Voraussetzung für das Auftreten des Fehlers dar?
- Tritt zum gleichen Zeitpunkt auch in anderen Anwendungen ein Fehler auf?

Die Beantwortung dieser Fragen kann Ihnen Klarheit über die Umgebung verschaffen, in der das Problem auftritt, und gibt Ihnen die Möglichkeit, Abhängigkeiten zu korrelieren. Beachten Sie dabei, dass die Tatsache, dass zu einem bestimmten Zeitpunkt mehrere Probleme aufgetreten sind, nicht unbedingt darauf hindeuten muss, dass diese Probleme miteinander in Zusammenhang stehen.

Kann der Fehler reproduziert werden?

Fehler, die sich reproduzieren lassen, sind häufig einfacher zu beheben. Allerdings bergen reproduzierbare Fehler auch einen Nachteil. Wenn der Fehler erhebliche negative Auswirkungen auf Ihren Geschäftsbetrieb hat, dann möchten Sie nicht, dass er sich wiederholt. Sofern dies möglich ist, sollten Sie den Fehler in einer Test- oder Entwicklungsumgebung reproduzieren, in der Sie normalerweise über ein höheres Maß

an Flexibilität und bessere Kontrollmöglichkeiten während der Untersuchung verfügen. Beantworten Sie die folgenden Fragen:

- Kann der Fehler auf einem Testsystem reproduziert werden?
- Tritt der Fehler bei mehreren Benutzern oder Anwendungen auf?
- Kann der Fehler durch Ausführung eines einzelnen Befehls, einer Befehlsgruppe oder einer bestimmten Anwendung reproduziert werden?

Durchsuchen von Wissensbasen

Häufig lassen sich Lösungen für Probleme finden, indem Sie die IBM Wissensbasen durchsuchen. Die Ergebnisse können anhand der verfügbaren Ressourcen, Unterstützungstools und Suchmethoden optimiert werden.

Informationen zu diesem Vorgang

Sie können nützliche Informationen finden, indem Sie das Information Center für IBM Cognos durchsuchen. Allerdings ist es in bestimmten Fällen zur Behebung eines Problems notwendig, Informationen zu suchen, die über die im Information Center enthaltenen Informationen hinausgehen.

Prozedur

Um Wissensbasen nach den benötigten Informationen zu durchsuchen, können Sie eine oder auch mehrere der folgenden Methoden verwenden:

- Suchen Sie die gewünschten Inhalte über das IBM Support Portal.

  Das IBM Support Portal bietet eine einheitliche, zentrale Ansicht aller technischen Unterstützungstools und aller Informationen für sämtliche IBM Systeme, Softwareprodukte und Services. Das IBM Support Portal ermöglicht Ihnen den zentralen Zugriff auf das gesamte Portfolio des elektronischen Supports von IBM. Sie können die Seiten anpassen, um gezielt die Informationen und Ressourcen zu nutzen, die Sie zur Vermeidung von Fehlern und zur schnelleren Fehlerbehebung benötigen. Machen Sie sich mit dem IBM Support Portal vertraut, indem Sie die Demovideos zu diesem Tool aufrufen. Diese Videos bieten Ihnen eine Einführung zum IBM Support Portal und stellen die Fehlerbehebungsressourcen und andere Ressourcen vor. Des Weiteren wird gezeigt, wie Sie die Seite anpassen können, indem Sie verschiedene Portlets verschieben, hinzufügen und löschen.
- Suchen Sie nach Inhalten zu IBM Cognos, indem Sie eine der folgenden zusätzlichen technischen Ressourcen nutzen:
  - IBM Cognos Analytics-APARs (Problemberichte)
  - IBM Cognos-Foren und -Communitys
- Suchen Sie mithilfe der IBM Kopfzeilensuche nach Inhalten.

  Sie können die IBM Kopfzeilensuche verwenden, indem Sie den Suchbegriff in das Suchfeld eingeben, das sich auf allen Seiten von ibm.com befindet.
- Suchen Sie mit einer externen Suchmaschine (z. B. Google, Yahoo oder Bing) nach den gewünschten Inhalten.

  Wenn Sie eine externe Suchmaschine verwenden, dann enthalten Ihre Ergebnisse mit einer höheren Wahrscheinlichkeit Informationen, die außerhalb der Domäne von ibm.com zu finden sind. In bestimmten Fällen können Sie jedoch nützliche Problemlösungsinformationen zu IBM Produkten in Newsgroups, Foren und Blogs finden, die sich nicht auf ibm.com befinden.

  Tipp: Schließen Sie "IBM" und den Namen des Produkts in die Suche ein, wenn Sie nach Informationen zu einem IBM Produkt suchen.

Fixes abrufen

Für die Behebung des bei Ihnen aufgetretenen Problems ist möglicherweise ein Fix verfügbar.

Vorgehensweise

Gehen Sie wie folgt vor, um Fixes zu suchen und zu installieren:

1. Stellen Sie fest, welcher Fix benötigt wird (Fix Central). Diese Seite (http://www.ibm.com/support/fixcentral/) wird in einem neuem Fenster geöffnet.
2. Laden Sie den Fix herunter. Öffnen Sie das Downloaddokument und folgen Sie dem Link im Abschnitt für das "Downloadpackage".
3. Wenden Sie den Fix an, indem Sie den Anweisungen im Abschnitt mit den "Installationsanweisungen" des Downloaddokuments folgen.
4. Führen Sie ein Abonnement durch, wenn Sie eine wöchentliche E-Mail-Benachrichtigung zu Fixes und weiteren IBM Support-Informationen erhalten möchten.

Kontaktaufnahme zum IBM Support

Der IBM Support bietet Zugriff auf eine Vielzahl von IBM Ressourcen, die Ihnen bei der Beantwortung softwarerelevanter Fragen helfen.

Vorbereitende Schritte

Nachdem Sie versucht haben, Antworten oder Lösungen mithilfe anderer Selbsthilfeoptionen wie z. B. der technischen Hinweise zu finden, können Sie Kontakt zum IBM Support aufnehmen. Um Kontakt zum IBM Support aufnehmen zu können, muss Ihr Unternehmen über einen aktiven IBM Wartungsvertrag verfügen und Sie müssen zur Einreichung von Problemen an IBM berechtigt sein. Halten Sie außerdem die folgenden Informationen bereit:

- Ihre Kundennummer
- Ihre Serviceanforderungsnummer (bei einer laufenden Serviceanforderung)
- die Telefonnummer, unter der Sie erreichbar sind
- die Version der von Ihnen verwendeten Software
- die Version der von Ihnen verwendeten Betriebssystemumgebung
- eine Beschreibung der von Ihnen beim Auftreten des Problems eingeleiteten Schritte
- die exakten Wortlaute aller aufgetretenen Fehlernachrichten
- eine Beschreibung aller Problemlösungsversuche

Informationen zu den verfügbaren Supporttypen finden Sie im Abschnitt zum Supportportfolio im *Software Support Handbook*.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um wegen eines Problems mit dem IBM Support Kontakt aufzunehmen:

1. Definieren Sie das Problem, stellen Sie Hintergrundinformationen zusammen und ermitteln Sie den Schweregrad des Problems. Weitere Informationen finden Sie im Abschnitt zum Kontaktieren von IBM Support im *Software Support Handbook*.
2. Stellen Sie Diagnoseinformationen zusammen.
3. Reichen Sie das Problem auf eine der folgenden Arten an den IBM Support ein:
   - Online über die IBM Support-Website: Sie können alle eigenen Serviceanforderungen über das Service Request-Portlet auf der Serviceanforderungsseite öffnen, aktualisieren und anzeigen.
   - Telefonisch: Die zu verwendende Telefonnummer finden Sie auf der Webseite Directory of worldwide contacts.

Ergebnisse

Wenn sich das eingereichte Problem auf einen Softwaredefekt oder auf fehlende bzw. fehlerhafte Dokumentation bezieht, dann erstellt der IBM Support einen APAR (Authorized Program Analysis Report). Der

APAR enthält eine detaillierte Beschreibung des Problems. Sofern möglich, stellt Ihnen der IBM Support eine Fehlerumgehung zur Verfügung, die Sie bis zur Bearbeitung des APARs und bis zur Bereitstellung eines entsprechenden Fixes implementieren können. IBM veröffentlicht bearbeitete APARs täglich auf der Website für den IBM Support, sodass auch andere Benutzer, bei denen das gleiche Problem auftritt, von der Lösung profitieren können.

Austauschen von Informationen mit IBM

Um ein Problem zu diagnostizieren oder zu identifizieren, müssen Sie dem IBM Support möglicherweise Daten und Informationen Ihres Systems zur Verfügung stellen. In anderen Fällen stellt Ihnen der IBM Support möglicherweise Tools oder Dienstprogramme zur Verfügung, die Sie für die Problembestimmung verwenden können.

Senden von Informationen an den IBM Support

Um den Zeitaufwand zur Behebung Ihres Problems zu reduzieren, können Sie Trace- und Diagnoseinformationen an den IBM Support senden.

Vorgehensweise

Gehen Sie wie folgt vor, um Diagnoseinformationen an den IBM Support einzureichen:

1. Öffnen Sie einen PMR (Problem Management Record). Sie können die IBM Support-Site oder das IBM Service Request-Tool verwenden.
2. Stellen Sie die benötigten Diagnosedaten zusammen. Die Diagnosedaten helfen bei der Reduzierung des Zeitaufwands für die Bearbeitung Ihres PMR. Sie können die Diagnosedaten manuell oder automatisch erfassen.
3. Komprimieren Sie die Dateien mithilfe des Programms TRSMAIN oder AMATERSE. Laden Sie das kostenlose Dienstprogramm von IBM auf das IBM Cognos Analytics-System herunter und installieren Sie das Dienstprogramm anschließend mit dem Befehl TSO RECEIVE.
4. Übertragen Sie die Dateien an IBM. Zum Übertragen der Dateien an IBM können Sie eine der folgenden Methoden verwenden:
   - Service Request-Tool
   - Standardmethoden zum Hochladen von Daten: FTP, HTTP
   - Sichere Methoden zum Hochladen von Daten: FTPS, SFTP, HTTPS
   - E-Mail

   Wenn Sie ein IBM Cognos-Produkt verwenden und zum Einreichen von PMRs ServiceLink / IBMLink verwenden, können Sie Diagnosedaten in einer E-Mail oder via FTP an den IBM Support senden.

Empfangen von Informationen vom IBM Support

In bestimmten Fällen werden Sie von einem Mitarbeiter der technischen Unterstützung von IBM gebeten, Diagnosetools oder andere Dateien herunterzuladen. Zum Herunterladen dieser Dateien können Sie FTP verwenden.

Vorbereitende Schritte

Vergewissern Sie sich, dass Ihnen der Mitarbeiter der technischen Unterstützung von IBM den bevorzugten Server für den Download der Dateien und das genaue Verzeichnis sowie die Dateinamen genannt hat, auf die zugegriffen werden muss.

Vorgehensweise

Gehen Sie wie folgt vor, um Dateien des IBM Supports herunterzuladen:

1. Stellen Sie via FTP eine Verbindung zu der Site her, die der Mitarbeiter der technischen Unterstützung von IBM angegeben hat, und melden Sie sich als anonymous an. Verwenden Sie dabei Ihre E-Mail-Adresse als Kennwort.
2. Wechseln Sie ins richtige Verzeichnis:
   a) Wechseln Sie ins Verzeichnis `/fromibm`.

   ```
   cd fromibm
   ```

   b) Wechseln Sie in das Verzeichnis, das Ihnen der Mitarbeiter der technischen Unterstützung von IBM genannt hat.

   ```
   cd Verzeichnisname
   ```
3. Aktivieren Sie für die Sitzung den binären Modus.

   ```
   binary
   ```
4. Verwenden Sie den Befehl **get**, um die Datei herunterzuladen, die der Mitarbeiter der technischen Unterstützung von IBM angebeben hat.

   ```
   get Dateiname.Erweiterung
   ```
5. Beenden Sie die FTP-Sitzung.

   ```
   quit
   ```

Abonnieren von Support-Aktualisierungen

Um in Bezug auf wichtige Informationen zu den von Ihnen verwendeten IBM Produkten auf dem neuesten Stand zu bleiben, können Sie Aktualisierungen abonnieren.

Informationen zu diesem Vorgang

Wenn Sie den Empfang von Aktualisierungen abonnieren, dann erhalten Sie wichtige technische Informationen und Aktualisierungen für spezielle Unterstützungstools und -ressourcen. Sie können die Aktualisierungen abonnieren, indem Sie eine der beiden folgenden Methoden verwenden:

RSS-/Atom-Feeds und Social Media-Abonnements
Allgemeine Informationen zu RSS einschließlich der einführenden Schritte und einer Liste der RSS-fähigen IBM Websites finden Sie auf der IBM Support-Website.

Eigene Benachrichtigungen
Mit der Funktion für eigene Benachrichtigungen (My Notifications) können Sie die Support-Aktualisierungen für alle IBM Produkte abonnieren. Sie können angeben, dass Sie E-Mail-Mitteilungen täglich oder wöchentlich erhalten wollen. Sie können angeben, welche Informationstypen Sie erhalten wollen (z. B. Veröffentlichungen, Hinweise und Tipps, Produkteinblendungen (sog. Alerts), Downloads und Treiber). Die Funktion 'My Notifications' (Eigene Benachrichtigungen) ermöglicht Ihnen das Anpassen und Kategorisieren der Produkte, über die Sie informiert werden möchten, und die Angabe der Zustellungsmethode, die optimal auf Ihre Anforderungen abgestimmt ist.

Vorgehensweise

Gehen Sie wie folgt vor, um die Support-Benachrichtigungen zu abonnieren:

1. Navigieren Sie zur IBM Support-Website.
2. Klicken Sie in der Registerkarte **Other** (Mehr) auf **My notifications** (Meine Benachrichtigungen).
3. Wenn Sie sich bereits für den 'My support' (Eigener Support) registriert haben, dann melden Sie sich an und überspringen Sie den nächsten Schritt. Wenn Sie noch nicht registriert sind, dann klicken Sie auf die Option **Register now** (Jetzt registrieren). Füllen Sie das Registrierungsformular aus und verwenden Sie dabei Ihre E-Mail-Adresse als IBMid. Klicken Sie anschließend auf **Submit** (Senden).

4. Suchen Sie nach den Produkten, die abonniert werden sollen (z. B. **Cognos Analytics**), und klicken Sie auf **Subscribe** (Abonnieren).
5. Wählen Sie im Popup-Menü die Dokumenttypen aus, z. B. **Security bulletin** (Sicherheitsbulletin).
6. Klicken Sie auf **Submit** (Senden).

Ergebnisse

Bis Sie die Vorgaben für die RSS-/Atom-Feeds und für 'My Notifications' ändern, erhalten Sie nun Benachrichtigungen zu den Aktualisierungen, die Sie angefordert haben. Sie können Ihre Vorgaben bei Bedarf (z. B. wenn Sie ein bestimmtes Produkt nicht mehr verwenden und stattdessen ein neues Produkt einsetzen) ändern.

Klicken Sie für RSS/Atom-Feeds unter der Spalte **RSS/Atom feed** Ihrer abonnierten Produkte auf **Links**.

Protokolldateien

Protokolldateien können Ihnen bei der Fehlerbehebung helfen, da sie die Aktivitäten aufzeichnen, die während der Arbeit mit einem Produkt ausgeführt werden.

Die in IBM Cognos Analytics ausgeführten Vorgänge werden zwecks Rückverfolgung in verschiedenen Protokolldateien aufgezeichnet. Wenn beispielsweise bei der Installation von IBM Cognos Analytics Fehler aufgetreten sind, enthält das Übertragungsprotokoll Informationen über die Aktivitäten des Installationsassistenten bei der Dateiübertragung.

Bevor Sie die Protokolldateien anzeigen, sollten Sie sicherstellen, dass sie die gewünschten Informationen enthalten.

Verwenden Sie IBM Cognos Administration, um die zu protokollierende Detailebene für jede Kategorie festzulegen.

Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Mit IBM Cognos Configuration können Sie die Größe, die Anzahl und den Pfad der Protokolldateien angeben sowie die Eigenschaften des Protokollservers konfigurieren.

Bei der Fehlerbehebung können Sie auf die folgenden Dateien zurückgreifen:

Übertragungsprotokolldatei

In dieser Datei werden die installierten Komponenten, Informationen über den Festplattenspeicherplatz, die in den Übertragungsdialogen ausgewählten Optionen sowie die Fehler aufgeführt, die beim Übertragen von Komponenten im Installationsassistenten aufgetreten sind. Darüber hinaus werden die Aktivitäten aufgezeichnet, die der Installationsassistent beim Übertragen von Dateien ausführt.

Die Übertragungsprotokolldatei befindet sich im Verzeichnis *`Installationsposition`*`\logs`. Der Dateiname enthält den Produktnamen und die Zeitmarke. Nachstehend finden Sie ein Beispiel für ein Dateinamenformat:

```
IBM_Cognos_Analytics_Install_04_21_2016_11_00_59.log
```

Protokolldatei der Installationskonfiguration

In dieser Protokolldatei werden sämtliche Konfigurationsaktivitäten während der Installation aufgezeichnet. Beispielsweise wird der verfügbare Port für den Dispatcher dokumentiert.

Die Fehlerauswertungs-Übertragungsprotokolldatei befindet sich im Verzeichnis *`Installationsposition`*`\logs`. Der Dateiname lautet `install_configuration.log`

Startkonfigurationsdatei

In dieser Datei werden die Konfigurationseinstellungen bei jedem Speichern der Eigenschaften aufgezeichnet. Der Dateiname lautet `cogstartup.xml`.

Wenn Sie die Konfiguration nicht speichern können oder Probleme auftreten, können Sie auf eine zuvor gespeicherte Konfigurationsdatei zurückgreifen. Die Sicherungskopien der Konfigurationsdateien befinden sich im Verzeichnis *Installationsposition*`/configuration`. Nachfolgend ist ein Beispiel für das Dateinamenformat von Sicherungskopien der Konfigurationsdateien aufgeführt:

`cogstartup_200811231540.xml`

Sperrdatei der Startkonfiguration

Diese Datei wird bei jedem Öffnen von IBM Cognos Configuration erstellt. Auf diese Weise wird verhindert, dass mehr als ein IBM Cognos Configuration-Fenster geöffnet wird.

Wenn Probleme beim Öffnen von IBM Cognos Configuration auftreten, suchen Sie im Verzeichnis *Installationsposition*`/configuration` nach der Datei `cogstartup.lock`. Wenn die Datei vorhanden ist, ohne dass IBM Cognos Configuration geöffnet ist, wurde IBM Cognos Configuration bei der letzten Verwendung nicht ordnungsgemäß beendet. Sie können die Sperrdatei löschen und anschließend IBM Cognos Configuration öffnen.

Ländereinstellungs-Konfigurationsdatei

In dieser Datei werden die Konfigurationseinstellungen aufgezeichnet, die Sie in IBM Cognos Configuration für Produkt- und Inhaltsländereinstellungen, die Ländereinstellungszuordnung und Währungsunterstützung vornehmen.

Wenn in der Benutzeroberfläche oder in Berichten Probleme mit der Sprachunterstützung auftreten, verwenden Sie diese Dateien, um die Änderungen zurückzuverfolgen. Die Sicherungskopien der Konfigurationsdateien befinden sich im Verzeichnis *Installationsposition*`/configuration`. Nachstehend finden Sie ein Beispiel für ein Dateinamenformat:

`coglocale_200811231540.xml`

Die Laufzeit-Protokolldatei

Die Standardprotokolldatei von IBM Cognos mit dem Namen `cogaudit.log` oder andere Protokolldateien, die Sie für den Empfang von Protokollnachrichten des Protokollservers konfiguriert haben, zeichnen Informationen auf, nachdem Sie den IBM Cognos Analytics-Service gestartet haben. Die betreffenden Dateien befinden sich im Verzeichnis *Installationsposition*`/logs`. Wenn Sie eine andere Position für Protokollnachrichten konfiguriert haben, überprüfen Sie die entsprechende Datei oder Datenbank.

Einige Protokollnachrichten geben an, dass Probleme vorliegen. Die meisten Nachrichten liefern nur Informationen, andere jedoch können Ihnen bei der Problemdiagnose in der Laufzeitumgebung helfen.

Gateway-Protokolldatei

Die Gateways nutzen zum Aufzeichnen von Fehlern die Gateway-Protokolldatei, die sich im Verzeichnis *Installationsposition*`/logs` befindet.

Sie können die Gateway-Protokolldatei zur Behebung von Fehlern verwenden, aufgrund derer das Gateway Anforderungen nicht verarbeiten oder keine Verschlüsselung verwenden kann. Folgende Symptome können auf diese Probleme hinweisen:

- Benutzerkennungen und Kennwörter funktionieren nicht
- Die Einzelanmeldung funktioniert nicht

- Der Dispatcher wird ausgeführt, aber die Benutzer erhalten eine Fehlernachricht, die angibt, dass der IBM Cognos Analytics-Server nicht verfügbar ist.

Die Gateway-Protokolldatei verwendet das folgende Benennungsformat, wobei *Gateway-Schnittstelle* cgi, mod2 (Apache 2.0-Modul) oder isapi entspricht.

gw*Gateway-Schnittstelle*.log (z. B. gwcgi.log)

Deinstallationsprotokolldatei

In dieser Datei werden die Aktivitäten aufgezeichnet, die der Deinstallationsassistent beim Deinstallieren von Dateien durchführt. Die Protokolldatei trägt die Bezeichnung cognos_uninst_log.htm und befindet sich im Verzeichnis "Temp". Sie können diese Protokolldatei zur Fehlerbehebung bei der Deinstallation von IBM Cognos Analytics-Komponenten verwenden.

Hintergrundmodus-Protokolldatei

In dieser Datei werden die Aktivitäten aufgezeichnet, die IBM Cognos Configuration bei der Ausführung im Hintergrundmodus durchführt. Diese Protokolldatei trägt die Bezeichnung cogconfig_response.csv und befindet sich im Verzeichnis *Installationsposition*/logs.

Anhang C. Informationen zu diesem Handbuch

Dieses Dokument ist für die Verwendung mit IBM Cognos Analytics vorgesehen. IBM Cognos Analytics ist ein Webprodukt mit integrierten Funktionen für die Berichterstellung, das Dashboarding, die Analyse und das Ereignismanagement.

Dieses Handbuch enthält Anweisungen zur Installation, zur Aktualisierung, zur Konfiguration und zum Testen von IBM Cognos Analytics.

Zielgruppe

Um dieses Handbuch nutzen zu können, müssen Sie mit folgenden Themen vertraut sein:

- Berichterstellungskonzepte
- Datenbank- und Data-Warehouse-Konzepte
- Sicherheitsfragen
- Grundlegende Kenntnisse der Verwaltung von Windows oder UNIX
- Vorhandene Serverumgebung und Sicherheitsinfrastruktur in Ihrer Organisation

Suchen von Informationen

Zugriff auf die Produktdokumentation im Web, einschließlich der gesamten übersetzten Dokumentation, besteht über das IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter). Releaseinformationen werden direkt in IBM Knowledge Center veröffentlicht und umfassen Links zu den letzten Technotes und APARs.

Zugriff auf die PDF-Versionen der Onlinehilfedateien des Produkts besteht über die PDF-Links am Anfang jeder HTML-Seite oder über die Webseite mit der IBM Cognos-Produktdokumentation (www.ibm.com/support/docview.wss?uid=swg27047187).

Zukunftsgerichtete Aussagen

In dieser Dokumentation wird die Funktionalität des Produkts zum gegenwärtigen Zeitpunkt beschrieben. Möglicherweise finden sich Verweise auf Funktionen, die derzeit nicht verfügbar sind. Dies bedeutet jedoch nicht, dass die betreffenden Funktionen in Zukunft zwangsläufig zur Verfügung stehen werden. Solche Verweise stellen keinerlei Verpflichtung, Zusage oder rechtliche Verbindlichkeit dar, Material, Code oder Funktionen bereitzustellen. Die Entwicklung und Bereitstellung von Features und Funktionen sowie der Zeitpunkt hierfür liegen ausschließlich im Ermessen von IBM.

Haftungsausschluss für Beispiele

Die Beispielfirma für Outdoor-Ausrüstung, das Unternehmen 'Abenteuer und Freizeit (AUF)', dessen Vertriebsabteilung, alle Variationen der Namen 'Beispielfirma für Outdoor-Ausrüstung' und 'Abenteuer und Freizeit' sowie das Planungsbeispiel stellen fiktive Geschäftsvorgänge mit Beispieldaten dar, mit denen die Beispielanwendungen für IBM und IBM Kunden erstellt wurden. Zu diesen fiktiven Datensätzen gehören Beispieldaten für Verkaufstransaktionen, Produktvertrieb, Finanzwesen und Personalwesen. Ähnlichkeiten mit tatsächlichen Namen, Adressen, Kontaktdaten oder Transaktionswerten sind rein zufällig. Andere Beispieldateien können Daten folgender Art enthalten: manuell oder vom System generierte fiktive Daten, aus wissenschaftlichen oder öffentlichen Quellen zusammengestellte Fakten sowie Daten, die mit Zustimmung der Copyrightinhaber als Beispieldaten zur Entwicklung von Beispielanwendungen genutzt werden dürfen. Referenzierte Produktnamen können Marken der jeweiligen Rechtsinhaber sein. Nicht autorisiertes Kopieren dieser Daten ist unzulässig.

Index

Numerische Stichwörter

32-Bit-Gateways 123
64-Bit
    Berichtsserver 118

A

Abfragedatenbanken 59
Abfrageservice 303
Ablaufdatum für Inhalte
    Bildverzeichnis 122
Active Directory
    LTPA 262
Active Directory Server
    Aktivierung von SSL 265
    Authentifizierung in mehreren Domänen 266
    erweiterte Eigenschaften 266
    für die Authentifizierung 263
    mit einem LDAP-Namespace 283
    Single Sign-on aktivieren 267
Agentenservice 300
AIX
    Umgebungsvariablen 91, 94, 112, 121
Aktiver Content Manager 93
Aktives Scripting
    in Web-Browsern aktivieren 13
Aktivierung
    IBM Cognos Application Firewall 181
    Services 183
Aktualisierung
    Java-Umgebung 4
Aliasse
    Konfiguration auf Web-Servern 122
Analysestile
    in Arbeitsbereichen 253
Andere Komponenten 59
Änderung
    E-Mail-Codierung 241
    Java-Versionen 170
    Konfigurationsvorlage 304
    Standardkonfigurationseinstellungen 171
    URIs 172
Anfragestile
    in Arbeitsbereichen 253
Angepasste Benutzereigenschaften
    LDAP 288
Anmeldung
    ausblenden während Anmeldung 275
    Konfiguration der Sicherheit 110
Annotation- 300
Anonyme Anmeldung
    Inaktivierung 258
Anwendungsebene
    Komponenten 56
Anwendungspools 122
Apache HTTP Server
    Konfiguration 134
    Konfiguration für Cognos Analytics 133
    Namespace 148
apache_mod, Datei
    Konfiguration für Gateways 154, 155
Apache-Web-Server
    Aliasse konfigurieren 122
Application Tier Components
    auf separatem Computer installieren 60
    Konfigurationsanforderungen 61
Arbeitsbereiche
    Berichtsstile 253
ARBORPATH, Umgebungsvariable 116
Archivierung
    Berichtsausgabe 193
    IBM Cognos-Inhalt 317
Archivierungszeiten
    Angeben 321
Asynchrones Zeitlimit 305
Audit
    Protokolle 224
Auditprotokolle
    Protokollziele 224
    Siehe auch Fehlerbehebung
Ausfallschutz 60
Ausfallzeiten
    Angeben 321
Ausgabeformate
    Einschränkung 322
Authentifizierung
    Active Directory Server 263
    Anforderungen für das Single Sign-on mit Microsoft Analysis Server oder Microsoft SQL Server 264
    angepasste Benutzereigenschaften für LDAP 288
    benutzerdefinierte Authentifizierungsprovider 274, 275
    benutzerdefinierte Eigenschaften für Active Directory Server 265
    Domänenstrukturen für Active Directory Server 266
    Einzelanmeldung mit IBM Cognos Series 7-Namespace 278
    Einzelanmeldung über Active Directory Server 267
    Inaktivierung der anonymen Anmeldung 258
    Konfiguration des IBM Cognos Series 7-Namespace 277
    LDAP 280, 282
    LDAP mit Active Directory Server 283
    LDAP mit IBM Directory Server 284
    LDAP mit Novell Directory Server 285
    LDAP mit Oracle Directory Server 287
    Löschen von Namespaces 296
    Namespaces verwenden 257
    SaferAPIGetTrustedSignon (Funktion) 279
    SAP 291
    Single Sign-on mit LDAP 290
    Single Sign-on mit SAP 293
    SiteMinder 294, 295

Authentifizierung *(Forts.)*
SSL mit LDAP 288
Trusted Sign-on-Plug-ins für IBM Cognos Series 7 278
Authentifizierungsprovider
Konfiguration von IBM Cognos BI für die Sicherheit 110

B

Basisinstallationen
mehrere Positionen 90
Befehlszeilenoptionen 325
Beispiele
IBM Cognos Workspace 253
Benachrichtigungsdatenbank
Einstellungen für Db2 unter z/OS 200
Erstellung 199
Konfiguration 201
Tabellenbereiche erstellen 97
Tabellenbereiche für Db2 for z/OS 200
Verwendung von SSL 213
Benutzer-DN und Kennwort für Bindung (Eigenschaft)
Sonderzeichen für LDAP-Namespace 280
Benutzerberechtigungen
in unbeaufsichtigter Konfiguration ändern 309
benutzerdefinierte Authentifizierungsprovider 274
Benutzerdefinierte Eigenschaften
Active Directory Server 265
Benutzerkonto
Anforderungen zum Ausführen des IBM Cognos-Service 103, 116, 169
Benutzerländereinstellung
zu Inhaltsländereinstellung zuordnen 238
Benutzeroberfläche
Sprachunterstützung anpassen 236
zuordnen für Produktländereinstellung 240
Benutzerprotokolle 234
Benutzersuche (Eigenschaft)
Sonderzeichen für LDAP-Namespace 280
Benutzertaskservice 301
Berechtigungen
ausführen 246
des Benutzerkontos, das für den IBM Cognos-Service verwendet wird 103, 116, 169
für Transformer-Modellierer 165
Richtlinie festlegen 246
Transitberechtigung 246
Bereitstellung
Konfigurationsobjekte 84
Transformer für Modellierer 166
Bereitstellungsarchive
Import 84
verschieben 83
Berichte
Sprachunterstützung anpassen 237
Standardschriftart ändern 191
Zustellzeit reduzieren 304
Berichte drucken
für UNIX- und Linux-Druckserver anpassen 198
Berichtsausgabe
gemeinsame Nutzung mit anderen Benutzer außerhalb von IBM Cognos Analytics 192
in einem Dateisystem speichern 192
wiederverwenden 193
Berichtsdatenservice 303
Berichtsserver
64-Bit aktivieren 118
Berichtsservice
Anforderungen 300
Liste eingebetteter Schriftarten für PDF-Berichte 191
Berichtsservices 303
Berichtsspezifikationen
Archivierung ausschalten 323
Upgrade 85
Berichtsstile
in Arbeitsbereichen 253
Berichtsverteilung
in einem Netz 304
Betriebssystem
Speichereinstellungen 3
unterstützte Versionen 1
Bibliotheksdateien 7
Bilder
Ablaufdatum für Inhalte 122
laden 122

C

CA SiteMinder
Scriptübergreifende Prüfung in IBM Cognos Application Firewall 181
CA,, *Siehe* Zertifizierungsstelle
chase_referral (Dateien) 266
Chinesisch (VR China)
Konfiguration von Schriftarten 188, 191
Cipher Suites
Priorität für SSL-Verbindungen 212
Clientkonfiguration
Db2-Datenbanken 96
Codepages für Datenquellen 155
cogconfig.sh
Befehlszeilenoptionen 325
Cognos Analytics-Portal 56
Cognos Workspace, `genehmigte Domänen` 181
Cognos-Service
über die Befehlszeile starten 312
cogstartup.lock (Datei) 334
cogstartup.xml (Datei)
manuelle Änderung der Eigenschaften 309
Common Symmetric Key 178
Content Manager
aktiv und standby 93, 196
Ändern von Zeitzonen 240
Anforderungen beim Verwenden von IBM Cognos Transformer mit dem Series 7-Namespace 157, 276
auf mehreren Computern konfigurieren 107
Ausfallschutz 60
Berichtsausgabe extern speichern 197
Installationsoptionen 60
Komponente 60
Komponentenbeschreibung 56
Konfiguration 60
Protokollserver 224
Replikation 196
Standby 60
Content Manager 8
Berichtsspezifikationsarchivierung inaktivieren 323

Content Manager-Service 301
Content Manager-URIs 107, 117
Content Store
  Komponentenbeschreibung 59
  mehrere Versionen von IBM Cognos BI 78
  Tabellenbereiche erstellen 97
  und weitere Positionen, an denen die Berichtsausgabe gespeichert werden kann 192
  unter Oracle erstellen 10
  Verbindungsmanagement 103
  Verwendung von SSL 213
Cookies
  anpassen 242
  Einstellungen 242
  in Web-Browsern aktivieren 13

D

Dateisystem
  um Kopien der Berichtsausgabe zu speichern 192
Datenbank für benutzergeführte Aufgaben und Anmerkungen
  Tabellenbereiche für Db2 unter z/OS 247
Datenbankclient
  Anforderungen für Transformer 65
  Anforderungen für Transformer-Modellierer 165
  für eine Protokolldatenbank einrichten 227
Datenbanken
  Benachrichtigung 108
  Datenbankclient protokollieren 227
  Protokollierung 229
Datenbankkonnektivität
  Berichtsdatenbank 113
Datenbanktreiber
  Db2 96
  Informix 102, 228
  Oracle 101
Datenbankverbindungen
  MS SQL Server und SSL 215
  SSL 215
Datenbankverbindungszeichenfolgen
  IBM Db2 103
  Microsoft SQL Server 103
  Oracle 103
Datenebene
  Content Manager 56
Datenquellen
  für Framework Manager 155
  Komponentenbeschreibung 59
  ODBC-Verbindungen 114
Datenquellenverbindungen
  einrichten 103
Datenschutzalgorithmus 179
Db2
  als Repository für Protokollnachrichten festlegen 229
  Clientkonfiguration 96
  Codepages 155
  Datenbankkonnektivität 113
  Datenbanktreiber 96
Db2-Content Store
  Script 97
Deinstallation
  Cognos Analytics 314
  Framework Manager 314
Deinstallation *(Forts.)*
  IBM Cognos Analytics 313
  nicht erfolgreich 314
  Transformer 314
Deinstallation im Hintergrundmodus 36
Diagnose, *Siehe* Fehlerbehebung
Dispatcher
  Import 84
  löschen 82
  Systemmetriken 299
Domänen
  Domänenstrukturen des Active Directory Server 266
  Einstellung für Cookies 242
  genehmigt für Cognos Workspace 181
Dynamischer Abfragemodus
  Datenbankkonnektivität 113
  Speichereinstellungen 3

E

E-Mail-Nachrichten
  Codierung ändern 241
E-Mail-Server
  Konfiguration 108
Eigenschaften
  in unbeaufsichtigter Konfiguration ändern 309
  Pfad temporärer Dateien 183
Eingebettete Schriftarten 191
Ereignismanagementservice 301
Ereignisprotokolle 228
ESSBASEPATH, Umgebungsvariable 116
Event Studio
  Komponentenbeschreibung 57
Export
  Konfigurationsdateien 35
Externer Identitätsabgleich, Eigenschaft
  für einen LDAP-Namespace bearbeiten 290
Externer Identitätsabgleich, Zuordnungseigenschaft
  Sonderzeichen für LDAP-Namespace 280
Externer Objektspeicher
  für Berichtsausgaben 197
  Verbindung testen 198
Externes Repository
  Inhalt archivieren 317

F

Fehlerbehebung
  für einen bestimmten Benutzer 234
  Probleme identifizieren 327
  Protokollierung 224
ferne Protokollserver
  Konfiguration 229
FileNet
  Angepasste Klassen importieren 319
  Berichtsspezifikationsarchivierung inaktivieren 323
Firefox
  Einstellungen 13
Firewalls
  Hinweise zur Installation 62
Framework Manager
  außerhalb einer Firewall 155
  Datenquellen einrichten 155

Framework Manager *(Forts.)*
Deinstallation 314
innerhalb der Netzfirewall 154
Installation 151, 152
Installationsoptionen 64
Komponentenbeschreibung 58
Konfiguration 64
Systemanforderungen 151
Testen von Installation und Konfiguration 157

G

Gateway
32-Bit-Gateways verwenden 123
Installation 121
Namespace 147, 148
Gateways
in einem Netz hinzufügen, um Zustellzeiten zu reduzieren 304
Komponentenbeschreibung 57
Konfiguration 124
Konfiguration von apache_mod 154, 155
Konfiguration von ISAPI 154, 155
Protokolldatei 334
GB18030 188, 191
Gemeinsame Vertrauenswürdigkeit
für IBM Cognos Analytics und andere Server einrichten 211
Google Chrome
Einstellungen 13
Grafikservice 301

H

Hintergrundmodus 31
HTML-Cookies„ *Siehe* Cookies
httpEndpoint
Konfigurationsgruppe 175

I

IBM Cognos Administration
Komponentenbeschreibung 56
IBM Cognos Analytics
Anmeldung 110
Deinstallation 313
Dispatcher 303
Fehlerbehebung bei Installationen 327
Konfiguration 12
Services 303
IBM Cognos Analytics for Microsoft Office 57
IBM Cognos Application Firewall
Konfiguration 181
IBM Cognos Configuration
Befehlszeilenoptionen 325
Komponentenbeschreibung 56
nicht überwachter Modus 35
Probleme beim Öffnen 334
Verwenden von Systemschriftarten 191
IBM Cognos Configuration kann nicht geöffnet werden 334
IBM Cognos Controller
Datenzugriff in IBM Cognos Analytics 67
IBM Cognos Planning - Analyst
Datenzugriff in IBM Cognos Analytics 67
IBM Cognos Planning - Analyst *(Forts.)*
Datenzugriff in IBM Cognos Analytics 67
IBM Cognos Planning - Contributor
Aktivierung von geplanten Berichten und Agenten 254
Datenzugriff in IBM Cognos BI 67
IBM Cognos Series 7
Aktivierung von SSL 278
für die Authentifizierung 276
Single Sign-on aktivieren 278
Trusted-Sign-on-Plug-ins 278
IBM Cognos Series 7-PowerCubes
Anforderungen zum erfolgreichen Konvertieren der Sprache 67
IBM Cognos Workspace
Anforderungen zum Laden für Microsoft IIS 247
Beispiele 253
Berichtsstile 253
Konfiguration 245
IBM Cognos-Inhaltsarchivierung
Externes Repository 317
IBM Cognos-Service
Konfiguration 304
über die Befehlszeile beenden 312
Voraussetzungen für das Benutzerkonto, das für den Service verwendet wird 103, 116, 169
IBM Connections
Zusammenarbeit einrichten 244
IBM Content Manager 8
Angepasste Klassen importieren 320
Import
Angepasste Klassen für IBM Content Manager 8 320
IBM Db2
Verbindungszeichenfolgen erstellen 103
IBM Directory Server
mit einem LDAP-Namespace 284
IBM FileNet Content Manager 317
IBM HTTP server
Namespace 148
IBM HTTP Server
Konfiguration 134
Konfiguration für Cognos Analytics 133
IBM Java Software Development Kit 234
IBMid 271
Identitätsprovider für OpenID Connect 270, 271
IIS
Namespace 147
SSO konfigurieren 138
IIS-Web-Server
Einzelanmeldung über Active Directory 267
Import
Angepasste Klassen für FileNet 319
Bereitstellungsarchive 84
Konfigurationen 84
Informix
als Repository für Protokollnachrichten festlegen 229
Content Store erstellen 12
Datenbanktreiber 102, 228
Protokolldatenbank erstellen 12
Installation
Basisinstallation bei mehreren Positionen 90
Framework Manager 151

Installation *(Forts.)*
IBM Cognos Analytics 31
Modi 90
Optionen für Content Manager 60
Optionen für die Serverkomponenten 62
Optionen für Framework Manager 64
Optionen für Transformer 64
Reihenfolge für Serverkomponenten 89
Test 111, 119, 149
Testen von Framework Manager 157
Testen von Transformer 164
Transformer 157
unbeaufsichtigt 31
unbeaufsichtigte Installation 31
UNIX, Linux 91
Installationsdatei
Herunterladen für Transformer-Modellierer 165
Installationsoptionen
Modellierungskomponenten 62
Integrated Facility for Linux (IFL) 62
Interaktiven Erkennungsvisualisierungsservice 301
Internet Explorer
Einstellungen 13
IP-Adressversion 243
IPv4 243
IPv6 243
ISAPI
Konfiguration für Gateway 154, 155

J

Java
Laufzeitumgebungen aktualisieren 4
Versionen ändern 170
Java Management Extensions
Konfiguration von JMX-Eigenschaften für die Fernüberwachung von Systemmetriken 299
mit Benutzerprotokollen 234
Java Software Development Kit von IBM 299
Java-Scripts
in Web-Browsern aktivieren 13
JDBC
Kerberos, Single Sign-on 218, 220–222
JDBC-Treiber
Einrichten von Oracle-Datenbanken 227
Jobservice 301
JRE-Dateien
Aktualisierung 4
JVM
Änderung 170

K

Kennwörter
in unbeaufsichtigter Konfiguration ändern 309
Kerberos-Authentifizierung
eingeschränkte Delegierung 268
Kerberos, Single Sign-on
JDBC 218, 220–222
Koexistenz 78
Kompatibler Abfragemodus
64-Bit-Datenquellen 113
Speichereinstellungen 3
Komponenten
Application Tier Components 61
Cognos Analytics-Portal 56
Content Manager 56, 60
Content Store 59
Datenquellen 59
Event Studio 57
Framework Manager 58
Gateways 57
IBM Cognos Administration 56
IBM Cognos Configuration 56
IBM Cognos Workspace 57
Komponenten der Anwendungsebene (Application Tier Components) 60
Map Manager 58
Query Studio 57
Reporting 56
Transformer 58
Komponenten der Anwendungsebene
Protokollserver 224
Konfiguration
Active Directory-Namespace 264
Ändern der Vorlage 304
Anforderungen für das Single Sign-on mit Microsoft Analysis Server oder Microsoft SQL Server 264
apache_mod für Gateway 154, 155
automatisieren 31
Benachrichtigungsdatenbanken 201
benutzerdefinierte Authentifizierungsprovider 275
Content Manager 60
Eigenschaften in unbeaufsichtigter Konfiguration 309
Einstellungen für Cognos Analytics 5
Framework Manager 64
Gateways 124
gemeinsame Vertrauenswürdigkeit für andere Server 211
globale Einstellungen 235
Hinzufügen von Ressourcen 307
IBM Cognos Analytics 12
IBM Cognos Configuration kann nicht geöffnet werden 334
IBM Cognos Workspace 245
IBM Cognos-Service 304
ISAPI für das Gateway 154, 155
Konfigurationsgruppe 175
Landkartendiagramme für Reporting 195
LDAP-Namespace 282
LDAP-Namespace für Active Directory Server 283
LDAP-Namespace für IBM Directory Server 284
mehrere Versionen von IBM Cognos Analytics 78
nicht überwacht 35
Pfad temporärer Dateien 183
Router 253
SAP-Namespace 292
Schriftarten 188
SiteMinder-Namespace 295
Sperrdatei 334
SSL-Protokoll 208
Standardeinstellungen ändern 171
Standardverschlüsselungsprovider 179
Standardzeitzone 240
Standby-Content Manager 107
Transformer 64
über die Befehlszeile ausführen 312

Konfiguration *(Forts.)*
Übertragungsspezifikationsdateien (.ats) 31
Umgebungseigenschaften für Anwendungsservicekomponenten 117
unbeaufsichtigt 31
von IBM Cognos Analytics zur Zusammenarbeit mit anderen IBM Cognos-Produkten 253
Web-Server 122
Zertifizierungsstellenservice 204
Ziel für Protokollnachrichten 224
Konfigurationsdateien
coglocale.xml 310
cogstartup.xml 307
Export 35
Konfigurationsgruppe 175
Konfigurieren
Web-Browser 13
Konfigurieren des Software Development Kit 254

L

Ländereinstellungen
unterstützte Ländereinstellungen für Inhalte anzeigen 237
unterstützte Produktländereinstellungen anzeigen 236
Ländereinstellungen für Inhalte
anpassen 237
unterstützte Ländereinstellungen anzeigen 237
zu Benutzerländereinstellung zuordnen 238
Landkartendiagramme 195
Lastausgleich
Aktivieren und Inaktivieren von Services 183
E-Mail-Server-Einstellungen 108
einrichten 60
Latenzzeit
verbessern 304
LDAP
Active Directory Server 283
Aktivierung von SSL 288
angepasste Eigenschaften 288
Eigenschaft 'Externer Identitätsabgleich' bearbeiten 290
für die Authentifizierung 280
IBM Directory Server 284
Konfiguration eines Namespace 282
LTPA 260
Novell Directory Server 285
Oracle Directory Server 287
Single Sign-on aktivieren 290
Lifecycle Manager 68, 85
Lightweight Third-Party Authentication (LTPA)
Active Directory 262
LDAP-Namespace 260
Linux
ODBC-Verbindungen zu Datenquellen 114
Protokollnachrichten 228
Starten und Stoppen des Cognos-Service 312
ulimit-Einstellungen 3
Umgebungsvariablen 91, 94, 112, 121
löschen
Dispatcher 82
LTPA 259

M

Map Manager
Komponentenbeschreibung 58
Metadatenservice 302
Metriken
für Server, Dispatcher und Services 299
Microsoft Analysis Server
Anforderung für Namespace 264
Microsoft Analysis Services
Datenquellenumgebung einrichten 155
Einzelanmeldung bei MSAS-Datenquellen 267
Microsoft IIS
Anforderungen zum Laden von IBM Cognos Workspace 247
konfigurieren von SSL auf 138
Microsoft Office
Berichtsdatenservice 303
Microsoft SQL Server
als Repository für Protokollnachrichten festlegen 229
Anforderung für Namespace 264
Datenbankkonnektivität 113
SSL 215
Verbindungszeichenfolgen erstellen 103
Migrationsservice 302
MIME-Typen
müssen zum Laden von IBM Cognos Workspace in Microsoft IIS angegeben sein 247
Mobiler Service 302
Modellierer
Transformer bereitstellen 166
Modellierung 57
Modellierungskomponenten
Installationsdatei für Transformer-Modellierer 165
Installationsoptionen 62
MSAS„ *Siehe* Microsoft Analysis Services
multi_domain_tree 266

N

Namespaces
Anforderungen für Content Manager beim Verwenden von Transformer mit dem Series 7-Namespace 276
Authentifizierung 257
Konfiguration von benutzerdefinierten Authentifizierungsprovidern 275
löschen 296
OpenID Connect 270
während Anmeldung ausblenden 275
Netezza
Datenquellenverbindungen 113
Einrichten von ODBC-Verbindungen 114
Novell Directory Server
mit einem LDAP-Namespace 285

O

ODBC-Verbindungen für Datenquellen 114
OpenID Connect
Benutzer hinzufügen 272, 274, 276
Generic 273
Identitätsprovider 271

OpenID Connect *(Forts.)*
Konfiguration eines Namespace 271
Protokollierung zu Diagnosezwecken 271
unterstützte Identitätsprovider 270
Optimieren
Db2-Content Store 303
Oracle
als Repository für Protokollnachrichten festlegen 229
Datenbank-JDBC-Treiber 227
Datenbankkonnektivität 113
Datenbanktreiber 101
mehrsprachige Unterstützung 155
Verbindungszeichenfolgen erstellen 103
Oracle Directory Server
mit einem LDAP-Namespace 287
Oracle Essbase
Konfiguration 115
Microsoft Windows (64-Bit) 116
UNIX 116
Oracle ESSBASE
Datenquellenverbindungen 113
Oracle Java SE Development Kit 234, 299

P

PDF-Schriftarten
Zuordnung zu integrierten PDF-Schriftarten für schnelleres Drucken von Berichten 190
Pfad temporärer Dateien
Konfiguration 183
Pfade
Einstellung für Cookies 242
Planning Analytics 68
Ports
Änderung 172, 174
mehrere Versionen von IBM Cognos Analytics 78
Standardkonfigurationseinstellungen 5
PowerCubes
Anforderungen zum erfolgreichen Konvertieren der Sprache 67
Zugriff in IBM Cognos Analytics 67
Präsentationsservice
Anforderungen 300
Produkte
unterstützte Versionen 1
Produktländereinstellungen
unterstützte Ländereinstellungen anzeigen 236
zuordnen für Benutzeroberfläche 240
Protokoll
IP-Adresse 243
Protokolldateien
Deinstallation 335
Gatewayfehler 334
Hintergrundmodus 335
Installationskonfiguration 333
Ländereinstellungskonfiguration 334
Laufzeit 334
Startkonfiguration 333
Übertragung 333
Protokolldatenbank
Db2 7
Mithilfe des Informix-Datenbankservers erstellen 12
mithilfe von Microsoft SQL Server erstellen 11
mithilfe von Oracle erstellen 10
Protokolldatenbank *(Forts.)*
Richtlinien für Erstellung 225
Tabellenbereiche für Db2 unter z/OS 225
Verwendung von SSL 213
Protokolle
Service 302
Verarbeitung von Nachrichten 224
Protokollierung
Dateien verwenden 228
Datenbank 229
Datenbankclient 227
ferne Protokollserver 228
Konfiguration 229
Protokollierung zu Diagnosezwecken
Fehlerbehebung für OpenID Connect-Namespaces 271
Protokollnachrichten
ferner Protokollserver 224
für IBM Cognos Application Firewall aktivieren 181
Protokollziele 224
Siehe auch Auditprotokolle
Protokollziele
Typen 224

Q

Query Studio
Komponentenbeschreibung 57

R

Registrierung entfernen
Dispatcher 82
relationaler Metadatenservice 303
Reporting
Ändern der Position von Landkartendiagrammen 195
Komponentenbeschreibung 56
Reporting-Anforderungen
für Transformer-Benutzer 65
Repositoryservices 303
Ressourcen
hinzufügen 307
Rollenbasierte Server
Hinweise zu Transformer 65
Router
Konfiguration 253

S

Safari 5
Einstellungen 13
SaferAPIGetTrustedSignon (Funktion)
für die Authentifizierung 279
sAMAccountName
Kerberos-Authentifizierung verwenden 268
SAP
für die Authentifizierung 291
Single Sign-on aktivieren 293
SAP BW
Autorisierungseinstellungen für IBM Cognos BI-Administratoren 292
Autorisierungseinstellungen für IBM Cognos BI-Benutzer 291
Datenquellenverbindungen 113

SAP BW *(Forts.)*
Konnektivität 292
Schriftarten
Ändern der Standardeinstellung 191
für PDF-Berichte ändern 191
Konfiguration 188
Liste eingebetteter Schriftarten für PDF-Berichte 191
Verwenden von Systemschriftarten in Cognos Configuration 191
Schriftarteneinbettungslisten 191
Schutzqualität bei SSL-Verbindungen 212
Scriptgesteuerte Deinstallation 36
Scripts
Content Store in Db2 erstellen 97
Scriptübergreifende Prüfung
in IBM Cognos Application Firewall konfigurieren 181
Secure Sockets Layer„ *Siehe* SSL
Series 7 IQD Bridge
Installation 157
Series 7-PowerCubes
Anforderungen zum erfolgreichen Konvertieren der Sprache 67
Server
Systemmetriken 299
Serverkomponenten
Installationsoptionen 62
Installationsreihenfolge 89
Serverzeitzonen
Änderung 240
Service
Benutzertask 301
Grafiken 301
Services
Abfrage 303
Agent 300
aktivieren und inaktivieren 183
Anmerkung 300
Bericht 300, 303
Berichtsdaten 303
Content Manager 301
Darstellung 303
Deinstallation 313
Ereignismanagement 301
IBM Cognos Analytics 303
Interaktive Erkennungsdarstellung 301
Job 301
Metadaten 302
Migration 302
Mobil 302
Monitor 303
Präsentation 300
Protokoll 302
Relationale Metadaten 303
Repository 303
Stapelbericht 300
Systemmetriken 299
über die Befehlszeile starten 312
über die Befehlszeile stoppen 312
zur Verbesserung der Leistung anpassen 300
Zustellung 301
Sichere LDAP-Kommunikation 288
Sicherheit
Aktivierung 110
Einstellungen für Web-Browser 1
Sicherheitsflag
Einstellung für Cookies 242
Single Sign-on
Active Directory-Namespace 267
LDAP-Namespace 290
mit IBM Cognos Series 7-Namespace 278
SAP-Namespace 293
SiteMinder
Konfiguration von Namespaces 295
Software Development Kit
Konfiguration 254
Softwarevoraussetzungen
unterstützte Produktversionen 1
Solaris
Umgebungsvariablen 91, 94, 121
Sonderzeichen
in LDAP-Namespace-Eigenschaften 280
Speichereinstellungen 3
Speicherpositionen
Landkartendiagramme 195
Sprache
an Benutzeroberfläche anpassen 236
für die Transformer-Benutzeroberfläche festlegen 158
Unterstützung von Ländereinstellungen für Inhalte anpassen 237
SSL
Active Directory Server 265
Aktivierung auf Web-Servern 130
Benachrichtigungsdatenbank 213
Content Store-Datenbank 213
gemeinsame Vertrauenswürdigkeit für andere Server einrichten 211
IBM Cognos Series 7-Namespace verwenden 278
Konfiguration 138, 208
LDAP-Namespace 288
Microsoft SQL Server 215
Protokolldatenbank 213
Schutzqualität 212
SSO 133
Stammverzeichnis
zum Speichern einer Berichtsausgabe außerhalb von IBM Cognos Analytics 192
Standby-Content Manager
Konfiguration 107
Stapelberichtsservice
Liste eingebetteter Schriftarten für PDF-Berichte 191
Stapelverarbeitungsservice 300
Start
Konfigurationssperrdatei 334
Starten des Cognos-Service
über die Befehlszeile 312
Starten von Cognos Analytics 149
Startoptionen 325
Stoppen des Cognos-Service
über die Befehlszeile 312
Systemanforderungen
Framework Manager 151
Transformer 158
Systemmetriken
Fernüberwachung 299
Systemprotokoll
Ziel für Protokollnachrichten 228

T

Tabellenbereiche
  Content Store-Scripts 97
  Db2 for z/OS 200
  Db2 unter z/OS 225, 247
Teradata
  Datenquellenverbindungen 113
Test
  Framework Manager 157
  Transformer-Installation 164
Testen der Installation 111, 119, 149
Thailändische E-Mail-Codierung
  JRE-Anforderungen 241
ThirdPartyCertificateTool
  Befehle und Beispiele 202
Threadausführungszeiten
  Angeben 321
TM1
  Datenquellenverbindungen 113
Transformer
  Anforderungen für Content Manager beim Verwenden des Series 7-Namespaces 157, 276
  Datenzugriff in IBM Cognos Analytics 67
  Deinstallation 314
  für Modellierer bereitstellen 166
  Installation 151, 157, 158
  Installation unter Linux und UNIX 159
  Installation unter Windows 160
  Installationsoptionen 64
  Komponentenbeschreibung 58
  Konfiguration 64
  Schritte zum Testen der Installation 164
  Systemanforderungen 158
Transformer Installationsdatei 165

U

überprüfen 174
Übertragungsspezifikationsdateien (.ats)
  Konfiguration 31
Überwachungsservice 303
ulimit-Einstellungen 3
Umgebungsvariablen
  Konfiguration für Anwendungsservicekomponenten 117
  unter UNIX oder Linux installieren 91, 94, 112, 121
Unbeaufsichtigte Installation
  Antwortdateivorlagen 33
  einrichten 31
Unbeaufsichtigte Installationen 31
Unbeaufsichtigte Konfiguration
  Eigenschaften ändern 309
  einrichten 31
Unbeaufsichtigte Konfigurationen 31
UNIX
  ODBC-Verbindungen zu Datenquellen 114
  Protokollnachrichten 228
  Starten und Stoppen des Cognos-Service 312
  ulimit-Einstellungen 3
  Umgebungsvariablen 91, 94, 112, 121
Unterstützte Umgebungen 1
Upgrade
  Berichte aus unterschiedlichen Versionen vergleichen 85
  Berichtsspezifikationen 85
  Content Store 81
  Inhalte verschieben 80
  Prozess 74
  Ressourcen 76
  Tools, die die Aktualisierung von IBM Cognos ReportNet unterstützen 68
  von anderen IBM Cognos-Produkten auf IBM Cognos Analytics 66
URI
  Standardkonfigurationseinstellungen 5
URI der Collaboration-Erkennung
  Konfigurieren 244
URIs
  Änderung 172, 174
UTF-8
  Codierung für E-Mail-Nachrichten 241

V

Verarbeiten von Protokollnachrichten 224
Verschlüsseln temporärer Dateien (Eigenschaft) 183
Verschlüsselung
  Einstellungen in unbeaufsichtigter Konfiguration ändern 309
Verschlüsselungsprovider
  Einstellungen 179
  Zertifikatssignieranforderung 205
Verteilte Installationen
  Szenarios 59
Verwaltung
  Systemleistung verbessern 299
Virtualisierung
  Unterstützte Umgebungen 1
Virtuelle Verzeichnisse 122
Vorlage
  Ändern der Vorlagengröße 304
Vorlagen
  Antwortdatei 33

W

Währung
  Unterstützung anpassen 236
Web-Browser
  Konfigurieren 13
  Sicherheitseinstellungen 1
Web-Server
  Aktivierung von SSL 130
  Einzelanmeldung über Active Directory und IIS Web-Server 267
  Konfiguration 122
  Ladezeit einrichten 122
  Namespace 147, 148
Wiederherstellung nach einer nicht erfolgreichen Deinstallation 314
Windows 91
Windows-Authentifizierung 267
Windows-Ereignisprotokoll
  Ziel für Protokollnachrichten 228

Windows-Installation 91

Z

Zeitzonen
    Änderung 240
Zertifikatssignieranforderung 205
Zertifizierungsstelle
    Konfiguration 204
    Service konfigurieren 204
Zielgruppe des Dokuments 337
Zusammenarbeit
    mit IBM Connections 181
Zustellservice 301
Zustellung
    Berichte schneller öffnen 304