IBM Cognos Analytics
11.1 版

管理與安全手冊

©

Produktinformationen

Dieses Dokument gilt für IBM Cognos Analytics Version 11.1.0 und kann auch für nachfolgende Releases gelten.

Copyright

目錄

Einleitung

Diese Informationen sind für die Verwendung mit IBM® Cognos Administration, der Verwaltungskomponente der IBM Cognos -Software, bestimmt.

Diese Informationen enthalten schrittweise Prozeduren und Hintergrundinformationen, die Sie bei der Verwaltung von IBM Cognos -Software unterstützen.

Informationen suchen

Um die Produktdokumentation im Web, einschließlich aller übersetzten Dokumentation, zu finden, greifen Sie auf IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter) zu.

Funktionen zur behinderten

IBM Cognos Administration verfügt über Funktionen zur behindertengerechten Bedienung, die Benutzern mit einer körperlichen Behinderung, wie z. B. eingeschränkter Mobilität oder eingeschränktem Sehvermögen, bei der Verwendung von Informationstechnologieprodukten helfen. Die Verfügbarkeit von Funktionen zur behindertengerechten Bedienung kann jedoch unterschiedlich sein, wenn andere Seiten und Komponenten, die keine behindertengerechte Bedienung unterstützen, der Cognos Administration-Benutzerschnittstelle hinzugefügt werden.

Informationen zu den Funktionen zur behindertengerechten Bedienung, die in der IBM Cognos Administration verfügbar sind, finden Sie unter Anhang A, „Funktionen zur behinderten”, auf Seite 429.

Die HTML-Dokumentation von IBM Cognos enthält Funktionen zur behindertengerechten Bedienung PDF-Dokumente sind ergänzend und enthalten als solche keine zusätzlichen Funktionen zur behindertengerechten Bedienung.

Vorausschauende Anweisungen

In dieser Dokumentation wird die aktuelle Funktionalität des Produkts beschrieben. Verweise auf Artikel, die derzeit nicht verfügbar sind, können eingeschlossen werden. Keine Implikation einer zukünftigen Verfügbarkeit sollte abgeleitet werden. Solche Verweise sind keine Verpflichtung, kein Versprechen oder keine rechtliche Verpflichtung, Material, Code oder Funktionalität zu liefern. Die Entwicklung, das Release und das Timing von Features oder Funktionen bleiben im alleinigen Ermessen von IBM.

Muster-Disclaimer

Die Beispielfirma "Outdoor", "Go Sales", "Go Sales", jede Variation der Namen "Sample Outdoors" oder "Great Outdoors" und "Planning Sample" stellen fiktive Geschäftsoperationen mit Beispieldaten dar, die für die Entwicklung von Beispielanwendungen für IBM -und IBM -Kunden verwendet werden. Zu diesen fiktiven Datensätzen gehören Beispieldaten für Verkaufstransaktionen, Produktverteilung, Finanzen und Personalressourcen. Jede Ähnlichkeit mit tatsächlichen Namen, Adressen, Kontaktnummern oder Transaktionswerten ist zufälligerweise. Andere Musterdateien können fiktive Daten manuell oder maschinell erzeugt enthalten, Faktendaten aus akademischen oder öffentlichen Quellen oder Daten, die mit Genehmigung des Rechteinhabers verwendet werden, zur Verwendung als Beispieldaten für die Entwicklung von Musteranwendungen. Auf Produktnamen, auf die verwiesen wird, können die Marken ihrer jeweiligen Eigentümer sein. Unerlaubte Vervielfältigung ist untersagt.

Kapitel 1. IBM Cognos Software Administration

Nachdem IBM Cognos -Software installiert und konfiguriert ist, können Sie Serververwaltung, Datenverwaltung, Sicherheits-und Inhaltsverwaltung, Aktivitäten-Management und Services-Verwaltung ausführen.

Sie können auch die folgenden Verwaltungstasks ausführen:

- Aufgaben automatisieren
- Einrichten Ihrer Umgebung und Konfiguration Ihrer Datenbank für mehrsprachige Berichterstellung
- Schriftarten installieren
- Drucker einrichten
- Web-Browser konfigurieren
- Zugriff von Benutzerzugriff auf Berichte der Serie 7
- Zugriff auf IBM Cognos -Software beschränken

Abgesehen von den typischen Verwaltungstasks können Sie auch die Darstellung und Funktionalität verschiedener IBM Cognos -Komponenten anpassen.

Informationen zu potenziellen Problemen finden Sie im *Handbuch zur Fehlerbehebung für IBM Cognos Analytics*.

IBM Cognos Administration

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf **IBM Cognos Administration**verfügen.

Weitere Informationen finden Sie unter Kapitel 13, „Funktionen” , auf Seite 207.

Tabelle 1. Arten von Verwaltungstools

Verwaltungsbereich	**Registerkarte**	**Verwendung**
Aktivitäten	**Status**	Auf Aktuelle, frühere, anstehende und geplante IBM Cognos -Einträge verwalten.
Content Manager-Computer	**Status**	Zum Verwalten von Content Manager-Computer.
Content-Store	**Konfiguration**	So führen Sie Wartungstasks für Content Storeaus.
Datenquellen	**Konfiguration**	So erstellen und verwalten Sie Datenquellen-Verbindungen.
Implementierung	**Konfiguration**	In implementieren IBM Cognos , um aus einer Quellenumgebung zu exportieren und anschließend in einer Zielumgebung zu importieren.
Dispatcher und Services	**Status**	Zum Verwalten von Dispatcher und Services.

Tabelle 1. Arten von Verwaltungstools (Forts.)		
Verwaltungsbereich	**Registerkarte**	**Verwendung**
Drucker	**Konfiguration**	So erstellen und verwalten Sie Drucker.
Sicherheit	**Sicherheit**	Zu Kontrollzugriff für bestimmte Produktfunktionen, wie z. B. Verwaltung und Berichterstellung, und Funktionen in den Funktionen, wie z. B. das Bersten und das benutzerdefinierte SQL.
System-, Dispatcher-, Server-und Serviceadministration	**Status**	Auf Überwachen der Systemleistung mit Systemmetriken und Server verwalten.
Serveroptimierung	**Status**	Auf Optimierung der Geschwindigkeit und Effizienz von IBM Cognos -Software.
Benutzer, Gruppen und Rollen	**Sicherheit**	So erstellen und verwalten Sie Benutzer, Gruppen und Rollen.

Systemweite zugängliche Berichtsausgabe aktivieren

Sie können systemweite Einstellungen für die zugängliche Berichtsausgabe angeben, die für alle Einträge gelten, einschließlich Berichte, Jobs und geplante Einträge.

Zugängliche Berichte enthalten Features, wie z. B. Alternativtext, die Benutzern mit Behinderungen den Zugriff auf Berichtsinhalte mit Hilfe von unterstützenden Technologien ermöglichen, wie z. B. Sprachausgabeprogrammen.

Die Einstellungen für die behindertengerechte Bedienung in den Benutzervorgaben und Berichtseigenschaften können die systemweiten Einstellungen in der IBM Cognos Administration überschreiben.

Für barrierefreie Berichte ist mehr Berichtsverarbeitung erforderlich und eine größere Dateigröße als nicht zugängliche Berichte. Infolgedessen wirken sich zugängliche Berichte auf die Leistung aus. Standardmäßig ist die Unterstützung für die zugängliche Berichtsausgabe inaktiviert.

Die verfügbare Berichtsausgabe ist für die folgenden Formate verfügbar: PDF, HTML und Microsoft Excel.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Dispatcher und Services**.
2. Klicken Sie in der Symbolleiste der Seite ' **Konfiguration** ' auf die Schaltfläche 'Eigenschaften festlegen'  .
3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Klicken Sie in der Dropdown-Liste **Kategorie** auf **Administratorüberschreibung**.
5. Klicken Sie für die Kategorie **Administratorüberschreibung** neben **Unterstützung der behindertengerechten Bedienung für**in der Spalte **Wert** auf **Bearbeiten**.

6. Wählen Sie auf der Seite **Unterstützung der behindertengerechten Bedienung für** eine der folgenden Optionen aus:

Option	Beschreibung
Inaktivieren	Die zugängliche Berichtsausgabe ist für Benutzer nicht verfügbar.
Obligatorisch machen	Die zugängliche Berichtsausgabe wird immer erstellt.
Dem Benutzer die Möglichkeit geben,	Die zugängliche Berichtsausgabe wird vom Benutzer angegeben. Wenn Sie diese Option auf **Nicht ausgewählt**setzen, wird die zugängliche Berichtsausgabe nicht automatisch erstellt. Dies ist der Standardwert. Wenn Sie diese Option auf **Ausgewählt**setzen, wird die zugängliche Berichtsausgabe standardmäßig erstellt.

Aufgaben automatisieren

Praktisch alles, was Sie mit dem Produkt tun können, können Sie mit Hilfe der entsprechenden API, URL-Schnittstelle oder Befehlszeilentool erreichen, wie in der folgenden Tabelle dargestellt.

Tabelle 2. Aufgaben automatisieren

Ziel	Automationsschnittstelle	Informationen
Ändern Sie ein Modell oder veröffentlichen Sie es erneut in UNIX -oder Microsoft Windows -Betriebssystemen.	Script-Player-Tool	*IBM Cognos Framework Manager-Entwicklerhandbuch* und *IBM Cognos Framework Manager-Benutzerhandbuch*
Ändern Sie ein nicht publizierter Modell mit den Methoden "updateMetadata" und "queryMetadata".	BI-Bus-API	*IBM Cognos Software Development Kit Developer Guide*
Rufen Sie die in dem veröffentlichten Paket verfügbaren Abfrageelemente mit der Methode "getMetadata" ab.	BI-Bus-API	*IBM Cognos Software Development Kit Developer Guide*
Funktionalität für Benutzer erteilen.	BI-Bus-API	*IBM Cognos Software Development Kit Developer Guide*
Verwalten und implementieren Sie die Sicherheit.	BI-Bus-API	*IBM Cognos Software Development Kit Developer Guide*

Tabelle 2. Aufgaben automatisieren (Forts.)		
Ziel	**Automationsschnittstelle**	**Informationen**
Sie können Berichte über einen Hyperlink auf einer HTML-Seite ausführen, anzeigen und bearbeiten. Verwenden Sie URLs, um Berichte anzuzeigen, zu bearbeiten und auszuführen.	URL-Schnittstelle	*IBM Cognos Software Development Kit Developer Guide*
Bearbeiten von Objekten im Content-Store. Content Manager verwalten.	BI-Bus-API	*IBM Cognos Software Development Kit Developer Guide*
Berichte verwalten.	BI-Bus-API	*IBM Cognos Software Development Kit Developer Guide*
Verwalten von Servern und Verwalten von Dispatchern.	BI-Bus-API	*IBM Cognos Software Development Kit Developer Guide*
Ändern oder Autorenberichte.	BI-Bus-API und Berichtsspezifikation	*IBM Cognos Software Development Kit Developer Guide*

Einrichten einer mehrsprachigen Berichtsumgebung

Sie können eine mehrsprachige Berichtsumgebung einrichten.

Sie können Berichte erstellen, die Daten in mehr als einer Sprache anzeigen, und verschiedene regionale Einstellungen verwenden. Dies bedeutet, dass Sie einen Bericht erstellen können, der von den Berichtskonsumenten überall auf der Welt verwendet werden kann.

Die Beispieldatenbanken, die mit IBM Cognos -Software bereitgestellt werden, speichern eine Auswahl von Textfeldern, wie z. B. Namen und Beschreibungen, in mehr als 25 Sprachen, um eine mehrsprachige Berichtsumgebung zu demonstrieren.

Hier ist der Prozess für die Erstellung einer mehrsprachigen Berichtsumgebung:

- Verwenden Sie mehrsprachige Metadaten.

  Der Datenquellenadministrator kann mehrsprachige Daten in einzelnen Tabellen, Zeilen oder Spalten speichern.

- Erstellen Sie ein mehrsprachiges Modell.

  Modellierungsprogramme verwenden Framework Manager, um dem Modell mehrsprachige Metadaten aus einem beliebigen Datenquellentyp mit Ausnahme von OLAP hinzuzufügen. Sie fügen mehrsprachige Metadaten hinzu, indem sie definieren, welche Sprachen das Modell unterstützt, Textzeichenfolgen im Modell für Dinge wie Objektnamen und -beschreibungen zu übersetzen und zu definieren, welche Sprachen in jedem Paket exportiert werden. Wenn die Datenquelle mehrsprachige Daten enthält, können Modellierer Abfragen definieren, die Daten in der Standardsprache für den Berichtsbenutzer abrufen.

  Weitere Informationen finden Sie im *IBM Cognos Framework Manager-Benutzerhandbuch*.

- Erstellen Sie mehrsprachige Karten.

  Administratoren und Modellierer verwenden ein Microsoft Fenster -Betriebssystemdienstprogramm namens Map Manager, um Karten zu importieren und Beschriftungen für Maps in Reportingzu aktualisieren. Für Karten-Features wie Land-oder Region-und Stadtnamen können Administratoren und

Modellierer alternative Namen definieren, um mehrsprachige Versionen von Text bereitzustellen, die auf der Karte angezeigt werden.

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

- Erstellen Sie einen mehrsprachigen Bericht.

  Der Berichtsersteller verwendet Reporting , um einen Bericht zu erstellen, der in verschiedenen Sprachen angezeigt werden kann. Sie können beispielsweise angeben, dass Text, wie z. B. der Titel, auf Deutsch erscheint, wenn der Bericht von einem deutschen Benutzer geöffnet wird. Sie können auch Übersetzungen für Textobjekte hinzufügen und andere sprachabhängige Objekte erstellen.

  Weitere Informationen finden Sie im *IBM Cognos Analytics - Reporting Benutzerhandbuch*.

- Geben Sie die Sprache an, in der ein Bericht angezeigt wird.
  - Definieren Sie für jeden Eintrag im Portal mehrsprachige Eigenschaften, wie z. B. einen Namen, einen Anzeigentipp und eine Beschreibung.
  - Geben Sie die Standardsprache an, die verwendet werden soll, wenn ein Bericht ausgeführt wird.

    Tipp: Sie können die Standardsprache auf der Seite mit den Ausführungsoptionen, in den Berichtseigenschaften oder in Ihren Vorgaben angeben.
  - Geben Sie eine andere Sprache als die Standardsprache an, die verwendet werden soll, wenn ein Bericht ausgeführt wird.

Die Daten werden dann in der Sprache und mit den in der Sprache angegebenen regionalen Einstellungen angezeigt.

- Web-Browser-Optionen des Benutzers
- Die Ausführungsoptionen
- Benutzervorgaben für IBM Cognos Analytics

Jeder Text, den Benutzer oder Autoren hinzufügen, wird in der Sprache angezeigt, in der sie eingegeben wurden.

Konfigurieren Ihrer Datenbank für die mehrsprachige Berichterstellung

IBM Cognos Analytics ist ein Unicode-Produkt, das in der Lage ist, Daten in vielen Sprachen und Codierung abzufragen.

IBM Cognos Analytics fragt in der Regel die Datenbank mit der nativen Datencodierung der Datenbank ab (Latin-1, Shift-JIS, Unicode usw.). IBM Cognos Analytics übersetzt diese Daten nach Bedarf in Unicode.

Wenn Sie Datenbanken mit zwei oder mehr Datencodierungen abfragen, fordert Reporting die Daten in Unicode an. Für bestimmte Datenbanken ist eine bestimmte Konfiguration der Client-oder Serversoftware erforderlich, um diese Funktionalität zu aktivieren. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Datenbankanbieter.

Hinweis: Informationen zu Sicherheitsfragen für Rundfahrten, wenn Zeichen von Unicode in Shift-JIS und zurück konvertiert werden, finden Sie in den Informationen zum Dienstprogramm 'Round Trip Safety Configuration' in Anhang B, „Round Trip Safety Configuration of Shift-JIS Charaktere”, auf Seite 435.

Schriftarten installieren

IBM Cognos -Software verwendet Schriftarten, um HTML-Berichte und -Seiten in Browsern anzuzeigen, PDF-Berichte auf dem IBM Cognos -Server darzustellen und in PDF-und HTML-Berichten verwendete Diagramme wiederzugeben.

Damit die Ausgabe korrekt angezeigt werden kann, müssen Schriftarten verfügbar sein, in denen der Bericht oder das Diagramm wiedergegeben wird. Im Fall von Diagrammen und PDF-Berichten müssen die Schriftarten auf dem IBM Cognos -Server installiert werden. Wenn ein Reporting -Benutzer beispielsweise die Schriftart Arial für einen Bericht auswählt, muss Arial auf dem IBM Cognos -Server installiert werden,

damit Diagramme und PDF-Dateien ordnungsgemäß wiedergegeben werden können. Wenn eine angeforderte Schriftart nicht verfügbar ist, ersetzt die IBM Cognos -Software eine andere Schriftart.

Da HTML-Berichte in einem Browser wiedergegeben werden, müssen die erforderlichen Schriftarten auf dem Personal Computer jedes IBM Cognos -Software-Benutzers installiert werden, der den HTML-Bericht liest. Wenn eine angeforderte Schriftart nicht verfügbar ist, ersetzt der Browser eine andere Schriftart.

Wenn Sie Berichte erstellen, müssen Sie Schriftarten auswählen, die Ihr IBM Cognos -Server oder -Benutzer installiert haben. Microsoft stellt eine breite Auswahl an Schriftarten mit verschiedenen Sprachenpaketen bereit, sodass dies wahrscheinlich kein Problem im Microsoft Fenster -Betriebssystem sein wird. Auf UNIX -Servern sind jedoch selten Schriftarten installiert. Sie sollten bereit sein, die Schriftarten zu erwerben und zu installieren, die Sie sowohl auf dem Server als auch auf den Browser-Clients benötigen.

Informationen zu den Einstellungen für PDF-Dateien finden Sie unter „PDF-Dateieinstellungen" auf Seite 70 .. Informationen zur Verwendung von PDF-Format in Berichten finden Sie unter „Berichtsformate" auf Seite 367. Informationen zum Konfigurieren von Schriftarten und zum Zuordnen von Ersatzschriftarten finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

IBM Cognos -Standardschriftart

Wenn eine angeforderte Schriftart nicht gefunden wird, gibt der IBM Cognos -Server PDF-Dateien und Diagramme mit einer Standardschriftart wieder.

Andale WT, ein Teil der sans-serif-Font-Familie, ist wegen seiner breiten Unterstützung von Unicode-Zeichen die Standardschriftart. Sie ist jedoch nicht unbedingt für alle Sprachen vollständig und kann nicht als attraktiv als gekaufte Schriften angesehen werden. Diese Schrift hat auch keine Glyph-Substitution (GSUB) und Ligaturunterstützung in den meisten Sprachen.

Reporting -Schriftarten

Reporting ist eine HTML-und JavaScript -Anwendung, die in einem Browser ausgeführt wird.

Aufgrund des Browserdesigns wird Reporting in der Sicherheitssandbox des Browsers ausgeführt und hat keinen Zugriff auf die Liste der auf dem lokalen Computer installierten Schriftarten. Stattdessen werden in Reporting Schriftarten verwendet, die in der globalen Konfiguration von IBM Cognos konfiguriert sind.

Weitere Informationen finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Drucker einrichten

Um Drucker für Benutzer verfügbar zu machen, wenn sie Berichte verteilen, können Sie Einträge für Drucker erstellen und diese im Content-Store von IBM Cognos speichern.

Wenn Benutzer einen Bericht drucken möchten, können sie einen Drucker auswählen, den Sie eingerichtet haben, ohne die Details zu den Netzadressen kennen zu müssen.

Wenn Sie einen Druckereintrag erstellen, müssen Sie sicherstellen, dass der von Ihnen definierte Drucker auf dem Computer eingerichtet ist, auf dem IBM Cognos installiert ist.

Um Drucker einzurichten, müssen Sie über die erforderlichen Funktionen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Sie müssen über Schreibberechtigungen für den Cognos -Namespace verfügen, siehe Kapitel 13, „Funktionen", auf Seite 207.

Um mögliche Fehler zu vermeiden, müssen Sie sicherstellen, dass die folgenden Bedingungen erfüllt sind, bevor Sie versuchen, den Druck zu drucken:

- Stellen Sie sicher, dass Adobe Reader auf jedem Computer installiert ist, auf dem IBM Cognos -Server installiert sind.
- Stellen Sie sicher, dass der IBM Cognos -Server mit einem Account gestartet wird, der über Zugriff auf den Netzwerkdrucker verfügt.

  Manchmal haben Systemkonten möglicherweise keinen Zugriff auf Netzwerkdrucker.

- Wenn IBM Cognos auf einem UNIX -Betriebssystem installiert ist, stellen Sie sicher, dass der Befehl **lpstat -v**einen konfigurierten Drucker zurückgibt und dass eine Druckervariable definiert ist.
- Wenn Sie die Netzadresse für den Drucker definieren, verwenden Sie die folgende Syntax:

  Verwenden Sie für Microsoft Fenster das Betriebssystem *Servername**Druckername*.

  Verwenden Sie für ein UNIX -Betriebssystem *Druckername*. Dies ist der Name der Druckwarteschlange, der vom Befehl `lpstat -v` angezeigt wird.
- Der Netzname muss mit dem Namen der Druckwarteschlange in lp übereinstimmen.
- Stellen Sie sicher, dass IBM Cognos -Benutzer über die korrekten Zugriffsberechtigungen für den Drucker verfügen.

Für die Rollenverzeichnisadministratoren müssen alle Zugriffsberechtigungen erteilt werden, und die Gruppe "Jeder" muss über die Berechtigungen "Lesen", "Ausführen" und "traverse" verfügen.

Tipp: Um Zugriffsberechtigungen für einen Drucker zu überprüfen oder zuzuordnen, klicken Sie in der Spalte **Aktionen** auf die Schaltfläche mit den Eigenschaften  für den Drucker und klicken Sie dann auf die Registerkarte **Berechtigungen** .

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Drucker**.

   Eine Liste der Drucker wird angezeigt.

   Tipp: Um einen Drucker zu entfernen, wählen Sie das Kontrollkästchen für den Drucker aus, und klicken Sie auf die Schaltfläche zum Löschen.
2. Klicken Sie in der Symbolleiste auf die neue Druckerschaltfläche  .
3. Geben Sie einen Namen und, wenn Sie möchten, eine Beschreibung für den Drucker ein.

   Tipp: Verwenden Sie einen Namen, der Details zum Drucker bereitstellt, z. B. Color Printer-4th Floor (Farbdrucker-4. Stock).
4. Geben Sie die Netzadresse des Druckers ein, indem Sie das Format *Servername**Druckername* für einen Netzwerkdrucker in einer Fenster -Installation und *Druckername* für eine UNIX -Betriebssysteminstallation oder für einen lokalen Drucker unter Fensterverwenden.
5. Klicken Sie auf **Fertigstellen**.

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 3. Aktivierte Browsereinstellungen

Browser	**Einstellung**
Alle Browser	Pop-ups für alle Cognos Analytics -Seiten zulassen

Tabelle 3. Aktivierte Browsereinstellungen (Forts.)	
Browser	**Einstellung**
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> / ibmcognos`. Dies ermöglicht die automatische Bedienerführung für Dateidownloads.

Von Cognos Analytics -Komponenten verwendete Cookies

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

Tabelle 4. 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.
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.
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.
pp_session	Sitzung temporär	Speichert Sitzungsinformationen, die für PowerPlay Studio spezifisch sind.
Qs	Persistent	Speichert die Einstellungen, die der Benutzer für Benutzerschnittstellenelemente wie Menüs und Symbolleisten herstellt.

Tabelle 4. Von Cognos Analytics -Komponenten verwendete Cookies (Forts.)		
Cookie	**Typ**	**Zweck**
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.
FrameBorder Seitenausrichtung Seitengröße PDFLayerDimension PDFOPTS	Sitzung temporär	Diese Cookies speichern die Einstellungen für den Export in PDF.
DimTreeToolbarVisible	Persistent	Speichert die Einstellung, die bestimmt, ob die Symbolleiste der Dimensionsanzeigefunktion angezeigt oder ausgeblendet werden soll.
cea-ssa	Sitzung temporär	Speichert die Einstellung, die bestimmt, ob die Benutzersitzungsinformationen mit anderen Cognos Analytics -Komponenten gemeinsam genutzt werden.
BRES	Sitzung temporär	Speichert Informationen, die verwendet werden, um die Bildschirmauflösung zu bestimmen, mit der Diagramme wiedergegeben werden.

Tabelle 4. Von Cognos Analytics -Komponenten verwendete Cookies (Forts.)		
Cookie	**Typ**	**Zweck**
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.

Benutzerzugriff auf Series 7-Berichte zulassen

Wenn die IBM Cognos -Software ordnungsgemäß für die Verwendung des IBM Cognos Series 7-Namespace konfiguriert ist, können Sie Benutzern den Zugriff auf NewsIndexes und NewsBoxes der Series 7-Version von IBM Cognos Upfront ermöglichen.

We recommend that IBM Cognos Analytics and IBM Cognos Series 7 use the same Web server if Upfront is set up to use relative URLs. If IBM Cognos Analytics and IBM Cognos Series 7 use different Web servers, configure Series 7 to use fully qualified URL. Auf diese Weise können Benutzer die Schaltfläche "Zurück" des Web-Browsers verwenden, um von Upfront zurück zu IBM Cognos Analyticszu navigieren.

Informationen zur Konfiguration von Series 7 finden Sie unter *IBM Cognos Series 7 Configuration Manager Benutzerhandbuch*.

Vorgehensweise

1. In IBM Cognos Configuration, configure IBM Cognos to use your IBM Cognos Series 7 namespace. Weitere Informationen finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.
2. Stellen Sie im **Eigenschaften** -Fenster unter **Cookieeinstellungen**sicher, dass die Eigenschaft **Sichere Markierung aktiviert** auf **Falsch**gesetzt ist.
3. Klicken Sie im Menü **Datei** auf **Speichern** und schließen Sie IBM Cognos Konfiguration.
4. Stellen Sie sicher, dass der Ticketserver für den IBM Cognos Series 7-Namespace aktiv ist.
5. Ensure that the timeout value of the Series 7 ticket server is set to the same value or to a higher value than the IBM Cognos passport timeout value.
6. Öffnen Sie auf dem Computer, auf dem IBM Cognos -Software installiert ist, die *Installationsposition*`/templates/ps/system.xml` -Datei in einem Editor.

Stellen Sie sicher, dass Ihr Editor das Speichern von Dateien im UTF-8-Format unterstützt.

7. Suchen und bearbeiten Sie (mit einem XML-Editor) den Parameter `Series7` wie folgt:

```
<!-- Series 7 Integration parameters -->
<param name="series7">
  <enabled>true</enabled>
  <!-- character encoding used by series7 -->
  <encoding>series7_character_encoding</encoding>
  <!-- host and port to connect to Upfront server -->
  <host>Upfront_host_name</host>
  <port>Upfront_dispatcher_port_number</port>
  <!-- Upfront gateway location -->
  <gateway>Upfront_gateway_location</gateway>
  <!-- If required, specify the prefix for IBM Cognos
back URLs when linking to Series 7 content. (eg. http://ibmcognos_computer)
otherwise relative URL's will be used -->
  <back-prefix>http://Series 7_server</back-prefix>
</param>
```

   Um die Zeichencodierung anzuzeigen, die von Series 7 verwendet wird, klicken Sie in Series 7 Configuration Manager auf der Registerkarte **Eigenschaften** auf **IBM Cognos-Gemeinsam genutzt**, klicken Sie auf **Ländereinstellung**und anschließend auf die Eigenschaft **Codierung** .

8. Speichern Sie die Datei system.xml im UTF-8-Format.
9. Using IBM Cognos Configuration, stop and then restart IBM Cognos Analytics.

   Weitere Informationen zum Stoppen von IBM Cognos Analyticsfinden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Zugriff auf IBM Cognos -Software beschränken

Möglicherweise möchten Sie nicht, dass alle Benutzer, die in einer Authentifizierungsquelle vorhanden sind, Zugriff auf die IBM Cognos -Software haben.

Um die IBM Cognos -Software zu schützen, müssen Sie das Produkt so konfigurieren, dass nur Benutzer, die zu einer bestimmten Gruppe oder Rolle in Ihrer Authentifizierungsquelle oder im Namespace von Cognos gehören, Zugriff auf das Produkt haben.

Es wird empfohlen, den Namespace von Cognos zu verwenden, da er vorkonfigurierte Gruppen und Rollen enthält, die Ihnen helfen, die IBM Cognos -Software schnell zu sichern. Eine der vorkonfigurierten Gruppen ist "Jeder". Standardmäßig gehört die Gruppe "Jeder" zu mehreren integrierten Gruppen und Rollen im Namespace " Cognos ". Wenn Sie sich für die Verwendung des Namespace von Cognos entscheiden, müssen Sie die Gruppe "Jeder" aus allen integrierten Gruppen und Rollen entfernen und sie durch Gruppen, Rollen oder Benutzer ersetzen, die für den Zugriff auf die IBM Cognos -Software berechtigt sind.

Gehen Sie wie folgt vor, um den Zugriff auf die IBM Cognos -Software zu beschränken:

- Aktivieren Sie in IBM Cognos Konfiguration die erforderlichen Eigenschaften, um den Zugriff zu beschränken.

  Weitere Informationen finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.
- Entfernen Sie in **IBM Cognos Administration**die Gruppe "Jeder" aus allen integrierten Gruppen und Rollen.

  Ersetzen Sie sie durch Gruppen, Rollen oder Benutzer, die berechtigt sind, auf die verschiedenen Funktionsbereiche der IBM Cognos -Software zuzugreifen. Weitere Informationen finden Sie unter Kapitel 15, „Anfangssicherheit”, auf Seite 223.
- Konfigurieren Sie Zugriffsberechtigungen für einzelne Einträge, wie z. B. Ordner, Pakete, Berichte, Seiten usw. Weitere Informationen finden Sie unter Kapitel 12, „Zugriffsberechtigungen und Berechtigungsnachweise”, auf Seite 193.

Weitere Informationen zu den Sicherheitskonzepten, die in der IBM Cognos -Software implementiert sind, finden Sie unter Kapitel 10, „Sicherheitsmodell”, auf Seite 181.

Kapitel 2. IBM Cognos Analytics -Anwendungen erstellen

Sie verwenden die IBM Cognos Analytics -Komponenten, um Berichterstellungs-und Analyseanwendungen zu erstellen.

Die Lebensdauer einer IBM Cognos Analytics -Anwendung kann Monate oder sogar Jahre sein. Während dieser Zeit können Daten geändert und neue Anforderungen angezeigt werden. Da sich die zugrunde liegenden Daten ändern, müssen die Autoren vorhandene Inhalte ändern und neue Inhalte entwickeln. Administratoren müssen außerdem Modelle und Datenquellen im Laufe der Zeit aktualisieren. Weitere Informationen zur Verwendung von Datenquellen finden Sie in der *IBM Cognos Analytics Administration and Security Guide* und in der *IBM Cognos Framework Manager-Benutzerhandbuch*.

Vorbereitende Schritte

In einer Arbeitsanwendung finden die technische und sicherheitstechnische Infrastruktur und das Portal statt, ebenso wie Prozesse zum Änderungsmanagement, zur Datenkontrolle und so weiter. Weitere Informationen finden Sie im Handbuch IBM Cognos Solutions Implementation Methodology, das die Implementierung von Roadmaps und unterstützenden Dokumenten umfasst. Informationen zu dem Toolkit finden Sie auf der IBM Portal für Unterstützung (www.ibm.com/support/entry/portal/support).

Wenn Sie IBM Cognos Analytics zum Erstellen von Anwendungen in allen Ihren IBM Cognos Analytics -Komponenten verwenden, suchen und bereiten Sie Datenquellen und -modelle, erstellen und veröffentlichen Sie den Inhalt und geben Sie dann die Informationen an. Die folgende Grafik gibt einen Überblick über den Workflow.

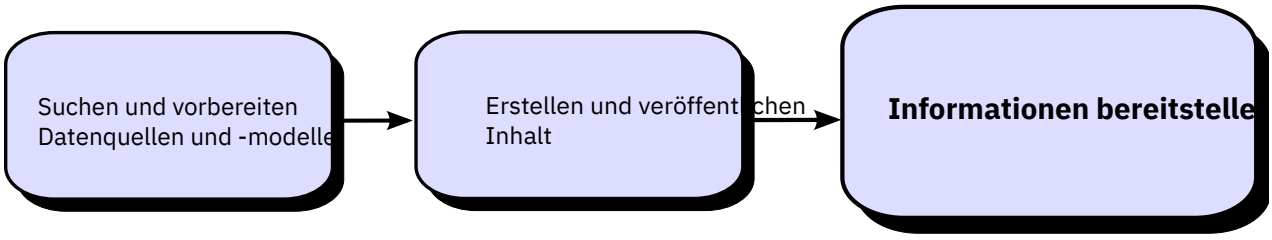


Abbildung 1. Anwendungen von Cognos Analytics zum Erstellen von Anwendungen verwenden

Vorgehensweise

1. Suchen und bereiten Sie Datenquellen und -modelle vor.

   IBM Cognos Analytics kann aus einer Vielzahl von Datenquellen berichten, sowohl relationalen als auch dimensionalen Datenquellen. Datenbankverbindungen werden in der Webverwaltungs-Schnittstelle erstellt und für die Modellierung, für das Authoring und für die Ausführung der Anwendung verwendet.

   Um Daten für das Authoring und die Anzeige zu verwenden, benötigen die Studios eine Untergruppe eines Modells der Metadaten (das als Paket bezeichnet wird). Die Metadaten benötigen möglicherweise eine umfangreiche Modellierung in Framework Manager.
2. Erstellen und veröffentlichen Sie den Inhalt.

   Berichte, Scorecards, Analysen, Arbeitsbereiche und vieles mehr werden in den Studios von IBM Cognos Analyticserstellt. Welches Studio Sie verwenden, hängt von dem Inhalt, der Lebensdauer und dem Publikum des Berichts ab, und ob die Daten dimensional oder relationell modelliert werden. Beispielsweise werden Self-Service-Berichte und Analysen über IBM Cognos Query Studio und IBM Cognos Analysis Studio durchgeführt und geplante Berichte werden in IBM Cognos Analytics -Reportingerstellt. Reporting -Berichte und Scorecards werden in der Regel für ein breiteres Publikum

vorbereitet, veröffentlicht und für das Bersten, die Verteilung und so weiter geplant. Sie können Reporting auch verwenden, um Vorlagen für die Self-Service-Berichterstellung vorzubereiten.

3. Die Informationen übergeben und anzeigen.

   Sie liefern Inhalt aus dem IBM Cognos -Portal und zeigen Informationen an, die von anderen Mechanismen gespeichert oder bereitgestellt wurden. Darüber hinaus können Sie Berichte, Analysen, Scorecards und mehr aus dem Studio ausführen, in dem sie erstellt wurden.

   Informationen zur Optimierung und Leistung finden Sie in der *IBM Cognos Analytics Administration and Security Guide* und in der IBM Portal für Unterstützung (www.ibm.com/support/entry/portal/support).

Kapitel 3. Protokollierung konfigurieren

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.

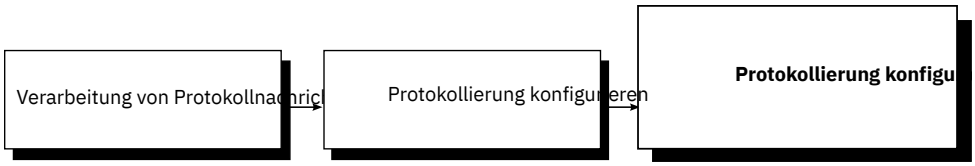


Abbildung 2. Der Workflow für die Implementierung der Protokollierung

- 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*.

Protokollnachrichten

Sie können die Speicherposition der Protokollnachrichten sowie die Größe und die Anzahl der Protokolldateien angeben. Sie können auch die Eigenschaften des Protokollservers konfigurieren.

Standardmäßig werden Protokollnachrichten in der `cogaudit.log` -Datei gespeichert, die sich im Verzeichnis `installationsposition/Protokolle` befindet. Die Protokollnachrichten können auch in einer Datenbank gespeichert werden. Weitere Informationen finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Verwenden Sie Protokollnachrichten nur für die Fehlerbehebung. Wenn Sie Bericht, Dashboard oder Story-Nutzung verfolgen möchten, verwenden Sie Prüfberichte. Weitere Informationen finden Sie unter „Prüfberichte" auf Seite 19.

Weitere Informationen zum Protokollservice finden Sie unter „Dispatcher und Services" auf Seite 41.

Protokollierungsstufen

Sie legen Protokollierungsstufen fest, um die Ereignisse und Nachrichten anzugeben, die in der Protokolldatei oder in der Protokolldatenbank aufgezeichnet werden sollen.

Bei einem Ereignis handelt es sich um ein Vorkommen in Ihrer IBM Cognos -Umgebung, das erheblich genug ist, um verfolgt zu werden, z. B. das Starten oder Stoppen eines Service.

Sie können für jeden Dispatcher-Service eine andere Protokollierungsstufe festlegen. Sie können dies für jeden Dispatcher oder für alle Dispatcher im selben Ordner tun. Durch die Festlegung unterschiedlicher Protokollierungsstufen für verschiedene Services können Sie die Menge der irrelevanten Protokollinformationen reduzieren. Wenn Sie beispielsweise den Stapelberichtsservice beheben müssen, können Sie eine detaillierte Protokollebene für diesen Service auswählen, indem Sie Protokollnachrichten auf ein Minimum beschränken. Die Protokollierungsstufe für einen Service gilt für alle zugehörigen Komponenten.

Tipp: Der Protokollservice verfügt nicht über Protokollierungsstufen, die diesem Service zugeordnet sind.

In der folgenden Tabelle sind die Details zu den Protokollen der einzelnen Protokollebene aufgeführt.

Tabelle 5. Protokollierungsstufen

Details	Minimal	Basis	Anforderung	Trace	Voll
System-und Servicestart und -abschaltung, Laufzeitfehler	X	X	X	X	X
Benutzeraccountverwaltung und Laufzeitverwendung		X	X	X	X
Anforderungen verwenden		X	X	X	X
Serviceanforderungen und -antworten			X		X

Tabelle 5. Protokollierungsstufen (Forts.)					
Details	**Minimal**	**Basis**	**Anforderung**	**Trace**	**Voll**
Alle Anforderungen an alle Komponenten mit ihren Parameterwerten				X	X
Weitere Abfragen zu IBM Cognos -Komponenten (native Abfrage)				X	X

Sie können die Systemleistung verwalten, indem Sie die Menge der vom Server ausgeführten Protokollierung verwalten. Da umfangreiche Protokollierung Auswirkungen auf die Serverleistung hat, kann die Erhöhung der Protokollierungsstufe die Leistung der IBM Cognos -Software negativ beeinflussen.

Die Standardprotokollierungsstufe ist "Minimal". Verwenden Sie unter der Anleitung für die Kundenunterstützung die vollständigen Protokollierungs-und Traceebenen nur für detaillierte Fehlerbehebungszwecke. Sie können die Serverleistung erheblich beeinträchtigen.

Wenn Sie Prüfberichte verwenden, finden Sie in „Prüfberichterstellung einrichten“ auf Seite 19 Richtlinien zum Festlegen der Protokollierungsstufe. Informationen zum Festlegen der Protokollierungsstufen für Prüfberichte finden Sie unter „Prüfberichte“ auf Seite 19.

Berichtsvalidierungsebenen und Protokollebenen

Sie können Informationen zur Berichtsvalidierungsstufe erfassen, indem Sie die entsprechende Protokollierungsstufe festlegen. Berichtsvalidierungsnachrichten können in Systemprotokollnachrichten eingeschlossen werden.

Sie können die Validierungsinformationen auf unterschiedliche Weise verwenden. Wenn das System eine allgemein schlechte Antwort liefert, können Sie die Protokollierung auf ein höheres Niveau festlegen. Die zusätzlichen Informationen können Ihnen helfen festzustellen, welche Berichte zu Fehlern sind und warum. Wenn Sie Warnungen in den Protokollen sehen, kann dies bedeuten, dass Benutzer fragwürdige Ergebnisse erhalten. Sie können die Eigner der auslaufenden Berichte benachrichtigen.

Es gibt vier Berichtsvalidierungsstufen und fünf Protokollierungsstufen. Die folgende Tabelle zeigt die Übereinstimmung zwischen ihnen.

Tabelle 6. Berichtsvalidierungsebenen und Protokollebenen	
Berichtsvalidierungsstufe	**Protokollierungsstufe**
Fehler	Minimal, Basis
Warnung	Anforderung
Schlüsseltransformation	Trace
Informationen	Voll

Je höher Sie die Protokollebene festlegen, desto mehr beeinträchtigt sie die Systemleistung. Normalerweise legen Sie die Ebene auf 'Minimal' oder 'Basic' fest, um Fehler zu erfassen, oder auf 'Anforderung', um Fehler und Warnungen zu erfassen.

Informationen zu Berichten und Berichtsvalidierungen finden Sie im *IBM Cognos Analytics - Reporting Benutzerhandbuch*.

Native Abfrageprotokollierung

Wenn Sie Prüfberichte erstellen möchten, die die Abfragen enthalten, die für Ihre Berichtsdatenquelle ausgeführt werden, müssen Sie die native Abfrageprotokollierung aktivieren. Sie können die native Abfrageprotokollierung verwenden, um zu erfahren, welche Arten von Informationsbenutzern erforderlich sind oder ob ein Bericht effizient ausgeführt wird. Informationen zum Erstellen von Prüfberichten finden Sie im Artikel „Prüfberichte“ auf Seite 19.

Wenn Sie die native Abfrageprotokollierung im dynamischen Abfragemodus (DQM) aktivieren möchten, setzen Sie **Prüfprotokollebene für Abfrageservice** auf **Anforderung** oder höher, wenn Sie Prüfberichterstellung einrichten verwenden. Wenn Sie jedoch Prüfberichte verwenden, können Sie die native Abfrageprotokollierung unabhängig von der Request-Level-Protokollierung aktivieren, wie in „Protokollierungsstufen festlegen“ auf Seite 18beschrieben.

Protokollierung der Berichtsausführungsoptionen

Sie können Berichtsausführungsoptionen an Ihrem Protokollierungssystem protokollieren. Zu den Berichtsausführungsoptionen gehören: Eingabeaufforderungsparameter, Ausführungsoptionen und Berichtsspezifikationen.

Diese Funktionalität ist standardmäßig inaktiviert. Sie können diese Funktion mit den folgenden erweiterten Parametern für den Berichtsservice und den Stapelberichtsservice aktivieren:

RSVP.PARAMETERS.LOG
Wenn dieser Parameter auf 'true' gesetzt ist, werden die Ausführungsoptionen und Eingabeaufforderungsparameter protokolliert.

Standardwert: false

RSVP.REPORTSPEC.LOG
Wenn dieser Parameter auf 'true' gesetzt ist, werden die Berichtsspezifikationen protokolliert.

Standardwert: false

Informationen zum Festlegen dieser Parameter für den Berichtsservice und den Stapelberichtsservice finden Sie unter „Erweiterte Einstellungen für bestimmte Services konfigurieren“ auf Seite 519.

Protokollierungsstufen festlegen

Sie legen Protokollierungsstufen fest, um die Ereignisse und Nachrichten anzugeben, die in der Protokolldatei oder in der Protokolldatenbank aufgezeichnet werden sollen.

Bei einem Ereignis handelt es sich um ein Vorkommen in Ihrer IBM Cognos -Umgebung, das erheblich genug ist, um verfolgt zu werden, z. B. das Starten oder Stoppen eines Service.

Die Protokollierungsstufen, die Sie für das System festgelegt haben, gelten für alle Dispatcher und Services. Die Protokollierungsstufen, die Sie auf der Dispatcherebene festgelegt haben, gelten für alle Services, die dem Dispatcher zugeordnet sind. Die Protokollierungsstufen, die Sie für einzelne Services festlegen, gelten für den Service auf allen Dispatchern.

Protokollierungsstufen, die für Dispatcher festgelegt sind, überschreiben Protokollstufen, die für das System festgelegt sind. Protokollierungsstufen, die für Services festgelegt sind, überschreiben Protokollierungsstufen, die für Dispatcher oder das System festgelegt sind.

Wenn Sie die Protokollierung für Fehlerbehebungszwecke verwenden, finden Sie unter „Protokollierungsstufen“ auf Seite 16 Richtlinien zum Festlegen der Protokollierungsstufen. Wenn Sie Prüfberichte verwenden, lesen Sie den Abschnitt „Prüfberichterstellung einrichten“ auf Seite 19.

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen", auf Seite 207.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Alle Dispatcher** oder **Dienstleistungen**, je nachdem, wo Sie Protokollierungsstufen festlegen möchten.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie für das Element, dessen Protokollierungsstufen Sie festlegen möchten, in seinem **Aktionen** -Menü auf **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Um die Liste zu filtern, klicken Sie im Menü **Kategorie** auf **Protokollierung**.
6. Suchen Sie in der Liste den gewünschten Service und wählen Sie im **Wert** -Menü die Protokollierungsstufe aus, die Sie für den Service wünschen.
7. Wenn die native Abfrageprotokollierung für den Service verfügbar ist und Sie sie verwenden möchten, wählen Sie das Kontrollkästchen **Native Abfrage für Stapelberichtsservice prüfen** aus.

   Weitere Informationen finden Sie unter „Native Abfrageprotokollierung" auf Seite 18.
8. Klicken Sie auf **OK**.

Prüfberichte

Mithilfe von Prüfberichten können Sie Informationen zu den Berichten, Dashboards und Story-Aktivitäten in der Protokollierungsdatenbank anzeigen.

Prüfberichte enthalten Informationen zum Zugriff auf Berichte, Dashboards und Storys. Diese Informationen werden in der Protokollierungsdatenbank aufgezeichnet, wenn ein Bericht, ein Dashboard oder eine Story erstellt, ausgeführt oder geändert wird. Sie enthält den Namen und die Position des Berichts, des Dashboards oder der Story, den Namen des Benutzers, der ihn ausgeführt oder geändert hat, sowie den Zeitpunkt und das Datum, zu dem das Ereignis eingetreten ist.

Zu den möglichen Verwendungen von Prüfinformationen gehören:

· Kapazitätsplanung

· Lizenzierungskonformität

· Leistungsüberwachung

· Nicht verwendete Inhalte ermitteln

Erweiterte IBM Cognos Analytics -Beispiele umfassen Beispielprüfberichte. Weitere Informationen finden Sie im *Beispiele für IBM Cognos Analytics -Handbuch*.

Prüfberichterstellung einrichten

Before you can create audit reports or use the sample audit reports that come with IBM Cognos software, you must set up audit reporting.

Um die Prüfberichterstellung zu aktivieren, legen Sie die Protokollierungsstufe für alle oder ausgewählten IBM Cognos -Services auf **Basis** (Prüfung aktiviert) oder **Anforderung**fest. Wenn Sie die Protokollierungsstufe auf **Minimal**setzen, ist die Prüfung inaktiviert. Verwenden Sie die **Voll** -Protokollierungs-und **Trace** -Versionen nur für detaillierte Fehlerbehebungszwecke unter der Anleitung der Kundenunterstützung. Sie können die Serverleistung erheblich beeinträchtigen.

Vorgehensweise

1. Konfigurieren Sie eine Protokolldatenbank in dem Datenbanksystem, das von Ihrer Organisation verwendet wird.

   Weitere Informationen finden Sie in den Richtlinien für die Erstellung einer Protokollierungsdatenbank in der *IBM Cognos Analytics Installation und Konfiguration*.
2. In IBM Cognos Konfiguration konfigurieren Sie unter **Umwelt** > **Protokollierung**Protokollnachrichten, die an die Datenbank gesendet werden sollen, die Sie in Schritt 1 erstellt haben.
3. Legen Sie in **Cognos-Verwaltung**die entsprechenden Protokollierungsstufen für die Cognos -Services fest.
   a) Rufen Sie **Verwalten** > **Verwaltungskonsole**auf.
   b) Wählen Sie auf der Registerkarte **Status** die Option **System**aus.
   c) Wählen Sie im Teilfenster **Scorecard** die Ansicht **Alle Dispatcher** aus.
   d) Klicken Sie im Menü "Dispatcheraktionen" auf **Eigenschaften festlegen**, und klicken Sie auf die Registerkarte **Einstellungen** .
   e) Wählen Sie in der Dropdown-Liste **Kategorie** die Option **Protokollierung**aus.
   f) Legen Sie die Protokollierungsstufe für die folgenden Services auf **Basis** fest: Content Manager-Cache-Service, Content Manager-Service, Abfrageservice. Sie können die Prüfprotokollierung für andere Services aktivieren, abhängig von Ihren Organisationsanforderungen oder sogar für alle Services, wenn Sie sich nicht um die Auswirkungen auf die Serverleistung kümmern.
   g) Um die native Abfrageprotokollierung in CQM (Compatible Query Mode) zu aktivieren, wählen Sie die beiden folgenden Kontrollkästchen aus:
      - **Native Abfrage für Stapelberichtsservice prüfen**
      - **Native Abfrage für Berichtsservice prüfen**
   h) Wenn Sie die native Abfrageprotokollierung im dynamischen Abfragemodus (DQM) aktivieren möchten, setzen Sie **Prüfprotokollebene für Abfrageservice** auf **Anforderung** oder höher.
   i) Klicken Sie auf **OK**.
4. Starten Sie in der Konfiguration von Cognos den **IBM Cognos** -Service erneut.

Vollständige Details für Secure Error-Nachrichten anzeigen

Sie können vollständige Fehlerdetails anzeigen, die sensible Informationen enthalten können.

Einige IBM Cognos -Fehlernachrichten enthalten möglicherweise sensible Informationen, wie z. B. Servernamen. By default, the IBM Cognos Application Firewall secure error messages option is enabled. Benutzer werden mit Informationen angezeigt, die nur darauf hinweisen, dass ein Fehler aufgetreten ist.

Wenn Sie über die entsprechenden Berechtigungen verfügen, können Sie vollständige Fehlerdetails abrufen. Möglicherweise möchten Sie auch Protokollnachrichten anzeigen. Weitere Informationen hierzu finden Sie im Artikel „Protokollnachrichten” auf Seite 16.

Vorgehensweise

1. Suchen Sie die Fehlercode-ID in der Fehlernachricht des Benutzers. Die Fehlernummer in der folgenden Nachricht lautet z. B. secureErrorID: 2004-05-25-15:44:11.296-#9:

   Es ist ein Fehler aufgetreten. Wenden Sie sich an Ihren Administrator. Der vollständige Fehler wurde von CAF mit SecureErrorID: 2004-05-25-15:44:11.296-#9 protokolliert.
2. Öffnen Sie die `cogaudit.log` -Datei im Verzeichnis *`Installationsposition`*`/logs` .
3. Suchen Sie nach der Fehlercode-ID, um die gültige Fehlernachricht zu suchen.

Erstellung von Kernspeicherauszugsdateien inaktivieren

Kernspeicherauszugsdateien werden für schwerwiegende Probleme erstellt, z. B. eine nicht behandelte Ausnahme oder eine abnormale Beendigung eines IBM Cognos -Prozesses.

Tritt ein solches Problem auf, erhalten Sie die folgende Fehlernachricht:

`Berichtsserver antwortet nicht.`

Da die Kernspeicherauszugsdateien groß sind und jedes Mal, wenn das Problem erneut auftritt, eine neue Speicherauszugsdatei erstellt wird, können Sie sie inaktivieren. Sie können die Kernspeicherauszugsdateien erneut aktivieren, wenn Probleme auftreten, für die sie erforderlich sind.

Sie können auch alle vorhandenen Kernspeicherauszugsdateien aus dem Verzeichnis `\bin` der IBM Cognos -Serverinstallation löschen, wenn sie nicht für Fehlerbehebungszwecke erforderlich sind. In einer Microsoft Fenster -Umgebung verfügen die Kernspeicherauszugsdateien über eine Erweiterung .dmp und den Dateinamen *`Prozess-ID`*`.dmp`, wie z. B. BIBusTKServerMain_seh_3524_3208.dmp. In einer UNIX -Umgebung werden die Dateien als "core" bezeichnet. In einer Linux -Umgebung werden die Dateien mit dem Namen `Kern.`*`Prozess-ID`*bezeichnet.

Vorgehensweise

1. Öffnen Sie auf dem Server, auf dem IBM Cognos Analytics installiert ist, die `cclWinSEHConfig.xml` -Datei aus dem Verzeichnis *`Installationsposition`*`\configuration` .
2. Ändern Sie im Konfigurationselement den Wert der Einstellung für die Umgebungsvariable auf 0 (null), so dass er liest.

   ```
   <env_var name="CCL_HWE_ABORT" value="0"/>
   ```

3. Speichern Sie die Datei.

Verwendung der Protokollierung für die Diagnose eines Problems für einen bestimmten Benutzer

Sie können Protokolle verwenden, um ein Problem zu diagnostizieren, das für einen oder mehrere bestimmte Benutzer auftritt.

Sie können die Protokollierung vorübergehend nur für die angegebenen Benutzer festlegen. Nachdem das Problem behoben wurde, inaktivieren Sie die benutzerspezifische Protokollierung und nehmen die normale Protokollierung wieder auf, ohne dass die vorhandenen Protokollierungseinstellungen beeinträchtigt werden.

Sie aktivieren und inaktivieren die Protokollierung für bestimmte Benutzer, indem Sie den Remote Process Service for Java Management Extensions (JMX) verwenden, eine Technologie, die Tools für die Verwaltung und Überwachung von Anwendungen und serviceorientierten Netzen bereitstellt. Sie stellen eine Verbindung zum JMX-Remote-Prozess-Service her, indem Sie die ausführbare Datei jconsole verwenden, die mit dem JDK von Java bereitgestellt wird. Die Ausgabe aus der benutzerspezifischen Protokollierung wird standardmäßig im Verzeichnis *`Installationsposition`*`\logs` gespeichert.

Vorbereitende Schritte

Sie müssen zuerst die benutzerspezifische Protokollierung für IBM Cognos Analyticsaktivieren. Weitere Informationen finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Vorgehensweise

1. Stellen Sie eine Verbindung zum JMX-Remote-Prozess-Service her, indem Sie die ausführbare Datei `Jconsole` starten und die folgenden Informationen angeben:

   · Die URL für die Verbindung zu den Daten. Beispiel:

`service:jmx:rmi://Content_Manager_Server/jndi/rmi://Monitoring_server:<JMXport> /proxyserver`

where *JMXport* is the value from **Externer JMX-Port** in IBM Cognos Configuration, and *Content_Manager_Server* and *Monitoring_server* are computer names. Verwenden Sie den Namen 'localhost' nicht, auch wenn Sie eine lokale Verbindung herstellen.

- Die Benutzer-ID und das Kennwort, um die Verbindung zu sichern.
- The values from **Externer JMX-Berechtigungsnachweis** in IBM Cognos Configuration.

2. Erweitern Sie im Verbindungsfenster des fernen Prozessservers den Eintrag **com.cognos**, **Metriken**, **CamAsyncAA**, `http://Servername:Portnummer/p2pd` und wählen Sie den **Operationen** -Knoten aus.
3. Kopieren Sie die CAMID des Benutzers in das Feld **enableDyeTrace** und klicken Sie auf die Schaltfläche **enableDyeTrace** .

   Tipp: In IBM Cognos Administration können Sie die CAMID finden, indem Sie die folgenden Schritte ausführen:

   - Klicken Sie auf die Registerkarte **Sicherheit** , und klicken Sie dann auf **Benutzer, Gruppen und Rollen**.
   - Klicken Sie auf **Eigenschaften festlegen** für den Benutzer und klicken Sie dann auf **Suchpfad, ID und URL anzeigen** .

   Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf **IBM Cognos Administration**verfügen. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen”, auf Seite 207.
4. Um zu überprüfen, ob Sie den Benutzer ordnungsgemäß aktiviert haben, navigieren Sie zu **Attribute** , und zeigen Sie den Inhalt der Einstellung **DyeTracedUsers** an.

Protokollierung für einen bestimmten Benutzer ausführen, indem komponentenspezifische ipf-Dateien bearbeitet werden

Sie können die Protokollierung für einen angegebenen Benutzer starten und die Traceerstellung für den Farbstoff implementieren, indem Sie komponentenspezifische ipf-Dateien bearbeiten.

Vorgehensweise

1. Fügen Sie ein < `filter`> -Element zu einer vorhandenen < `appender`> -Definition hinzu oder fügen Sie eine neue < `appender`> -Definition hinzu.

   Sie müssen sicherstellen, dass Kategorien auf eine < `appender`> -Definition verweisen, die das Element < `filter`> verwendet.
2. In den Fällen, in denen eine < `appender`> -Definition einen Protokollserver angibt, ändern Sie die Portwerte in Ihren konfigurierten Protokollserverport.

Protokollierung für einen bestimmten Benutzer unter Verwendung ausgewählter Kategorien ausführen

Um die Protokollierung für einen bestimmten Benutzer zu starten, implementieren Sie die Traceerstellung für den Farbstoff, und passen Sie die Ausgabe an, indem Sie ausgewählte Kategorien verwenden und die Ausgabe an eine oder mehrere Appender-Definitionen verteilen.

Vorgehensweise

1. Suchen Sie im Verzeichnis *Installationsposition*`\configuration` die `Ipf` -Tracedatei für die Komponente, die Sie verfolgen möchten. Die Dateien werden als `ipf`*Komponente*`clientconfig.xml.sample`bezeichnet. Beispiel: `ipfAAAclientconfig.xml`.

2. Erstellen Sie eine Kopie der angegebenen ipf*Komponente*clientconfig.xml.sample -Datei mit dem Namen ipfclientconfig.xml.off.
3. Öffnen Sie mithilfe eines Texteditors die ipfclientconfig.xml.off -Datei und nehmen Sie die folgenden Änderungen vor:
   - Fügen Sie die Protokollebene der von Ihnen benötigten < categories> hinzu oder ändern Sie sie.
   - Führen Sie eine der beiden folgenden Aktionen aus:

     Fügen Sie einen neuen Abschnitt < appender> unter dem letzten vorhandenen Element < appender> wie folgt hinzu:

     ```
     <appender name="DyeTraceOutput" class="org.apache.log4j.RollingFileAppender">
             <param name="File" value="../logs/dyetrace_output.log"/>
             <param name="MaxBackupIndex" value="1"/>
             <param name="MaximumFileSize" value="10485760"/>
             <layout class="org.apache.log4j.PatternLayout"/>
           <param name="ConversionPattern" value="%m%n"/>
        </layout>
        <filter class="com.cognos.indications.LogIPFDyeTraceFilter"/>
     </appender>
     ```

     oder ändern Sie eine der vorhandenen Appender-Definitionen, indem Sie die Zeile hinzufügen

     ```
     <filter class="com.cognos.indications.LogIPFDyeTraceFilter"/>
     ```

     vor dem Schließen des Tags < /appender> .
4. Bearbeiten Sie für die < categories> -Abschnitte, auf die Sie den Farbspurenfilter anwenden möchten, die Eigenschaft < appender-ref> , um auf den DyeTraceOutput-Appender oder den Appender zu verweisen, der den Filter dazu hinzugefügt hat. Beispiel:

   ```
   <category name="Audit.RTUsage.CAM.AAA" class="com.cognos.indications.
   LogTypedLogger" additivity="false">
      <level value="debug"/>
      <appender-ref ref="DyeTraceOutput"/>
   </category>
   ```
5. Speichern Sie die Datei ipfclientconfig.xml.off .
6. Um diese Datei zu aktivieren, benennen Sie sie inipfclientconfig.xml um.
7. Sie können die benutzerspezifische Protokollierung inaktivieren und die normale Protokollierung wieder aufnehmen, indem Sie die ipfclientconfig.xml -Datei erneut in ipfclientconfig.xml.offumbenennen. Setzen Sie die von Ihnen angewendeten Benutzer DyeTracing auf, nachdem Sie das Produkt erneut gestartet haben.

Ergebnisse

Innerhalb von 60 Sekunden wird die nutzerspezifische Protokollierung automatisch aktiviert und die Ausgabe generiert. Für den hier beschriebenen Appender wird die Ausgabe in der *Installationsposition*\logs\dyetrace_output.log -Datei gespeichert. Bei anderen Appendern wird das für diesen Appender konfigurierte Ziel verwendet. Wenn eine authentifizierte Sitzung mit IBM Cognoserstellt wird, werden nur Aktionen des angegebenen Benutzers protokolliert.

Möglicherweise erhalten Sie einige Hinweise, die nicht mit dem angegebenen Benutzer in Beziehung stehen. Dies kann beispielsweise auftreten, wenn Sie das Produkt starten oder wenn Hinweise protokolliert werden, bevor die Authentifizierung des Benutzers abgeschlossen ist. Sie können die Protokollebene der Kategorien ändern, um eine überwältigende Anzahl von Indikationen zu vermeiden.

Protokollierung für einen bestimmten Benutzer inaktivieren

Sie können die Protokollierung für einen bestimmten Benutzer inaktivieren.

Vorgehensweise

Löschen Sie die `ipfclientconfig.xml` -Datei, die Sie in „Verwendung der Protokollierung für die Diagnose eines Problems für einen bestimmten Benutzer” auf Seite 21erstellt haben.

Ergebnisse

Die normale Protokollierung aller Benutzer wird fortgesetzt. Es kann bis zu 30 Sekunden dauern, bis die benutzerspezifische Protokollierung gestoppt wird.

Kapitel 4. Systemleistungsmetriken

Sie können die Systemleistung mithilfe von Metriken in IBM Cognos Administration überwachen, die Ihnen die schnelle Diagnose und Behebung von Problemen ermöglicht.

Sie können beispielsweise wissen, ob es mehr als 50 Elemente in einer Warteschlange gibt oder ob ein Element länger als eine angegebene Zeit in einer Warteschlange gewartet hat.

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf **IBM Cognos Administration** Kapitel 13, „Funktionen", auf Seite 207verfügen.

Mithilfe von Metriken können Sie den Status des Systems als Ganzes und den Status einzelner Server, Dispatcher und Services bewerten. Sie können die Attribute für jede Metrikbewertung anzeigen, die Schwellenwerte festlegen, die zum Berechnen der Metrikbewertungen und zum Zurücksetzen der Messwerte verwendet werden. Möglicherweise möchten Sie die Berichtsserviceverbindungen aktualisieren, wenn ein PowerCube erneut erstellt wurde.

Sie können auch Funktionen wie das Starten und Stoppen von Dispatcher oder Services „Stoppen und Starten von Disponenten und Services" auf Seite 45und die Registrierung von Dispatchern „Dispatcher aus der Umgebung entfernen" auf Seite 47ausführen.

Sie können Protokolldateien verwenden, um die Langstreckenleistung und die Verwendung von Kapitel 3, „Protokollierung konfigurieren", auf Seite 15zu analysieren.

Sie können eine Metrikspeicherauszugsdatei für Fehlerbehebungszwecke erstellen.

Erfasste Metrikdaten

Die Daten für Messwerte werden je nach Messgröße, Zeitbereich und Erfassungszeit, die der Metrik zugeordnet sind, unterschiedlich erfasst.

Weitere Informationen dazu, wie diese auf einzelne Metriken angewendet werden, finden Sie unter „Systemmetriken" auf Seite 26.

Metrikänderungstyp

Der Wert, der für einen Messwert angezeigt wird, hängt vom Änderungstyp ab, wie in der folgenden Tabelle dargestellt.

Tabelle 7. Metrikänderungstypen

Änderungstyp	**Beschreibung**
Zähler	Der Wert ist eine Summe, die mit jeder Änderung zunimmt. Beispiel: Die Anzahl der Anforderungen ist ein Gegenänderungstyp.
Messanzeige	Der Wert kann, abhängig von den Ereignissen, im Laufe der Zeit erhöht oder verringert werden. Die Anzahl der Prozesse, die zu einem beliebigen Zeitpunkt ausgeführt werden, ist beispielsweise ein Messwertänderungstyp.

Metrikzeitbereich

Das Intervall, in dem ein Metrikwert erfasst wird, unterscheidet sich nach Messgröße, wie in der folgenden Tabelle dargestellt.

Tabelle 8. Metrikzeitbereiche	
Zeitbereich	**Beschreibung**
Zeitpunkt	Der Wert wird zu einem bestimmten Zeitpunkt erfasst, z. B., wenn Sie eine Metrikgruppe zurücksetzen oder einen Service erneut starten.
Seit dem Zurücksetzen	Der Wert wird über das Intervall seit dem letzten Zurücksetzen des Messwerts erfasst.

Metriksammlungszeit

Die Zeit, zu der ein Metrikwert erfasst wird, unterscheidet sich nach metrischen Wert, wie in der folgenden Tabelle dargestellt.

Tabelle 9. Metriksammlungszeiten	
Zeitpunkt der Erfassung	**Beschreibung**
Bei Änderung	Der Wert wird erfasst, wenn eine Änderung eintritt, z. B. wenn sich die Anzahl der Anforderungen ändert.
Auf Anfrage	Der Wert wird erfasst, wenn Sie ein neues Element im Fenster 'Scorecard' auswählen oder eine Metrikgruppe zurücksetzen. Weitere Informationen finden Sie unter „Teilfenster auf der Seite 'Status System'" auf Seite 36 und „Metriken zurücksetzen" auf Seite 39.
Unbekannt	Die Sammelzeit ist unbekannt

Systemmetriken

Es gibt eine große Auswahl an Metriken, die Ihnen bei der Überwachung der Leistung Ihrer IBM Cognos -Softwareinstallation helfen.

Weitere Informationen finden Sie unter „Erfasste Metrikdaten" auf Seite 25.

Einige Metriken werden zurückgesetzt, wenn der Service erneut gestartet wird. Sie können einige Metriken auch manuell „Metriken zurücksetzen" auf Seite 39zurücksetzen.

Auf System-und Serverebene schließen die Metriken alle zugeordneten Dispatcher ein. Auf der Dispatcherebene schließen Metriken alle zugehörigen Services ein. Für Servergruppen gelten Metriken für alle Dispatcher in der Gruppe.

Sitzungsmetriken

Sie können Sitzungsmessdaten verwenden, um Benutzersitzungen zu überwachen. Dies ist hilfreich für die Überwachung von Systemtrends wie z. B. Nutzungsmuster nach Tageszeit und Wochentag. Sitzungsmetriken sind auch nützlich, um den Kontext anderer Metriken zu verstehen. Beispiel: Wenn die Anzahl der Sitzungen außergewöhnlich hoch ist, könnte die Anzahl der Warteschlangenlängenmesswerte höher als normal sein. Weitere Informationen finden Sie unter „Warteschlangenmetriken" auf Seite 27 .

Die folgenden Sitzungsmessdaten sind verfügbar:

- **Anzahl Sitzungen**

Gibt die Anzahl der momentan aktiven Benutzersitzungen an.

Tabelle 10. Anzahl Sitzungen

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System	Messanzeige	Zeitpunkt	Auf Anfrage

- **Anzahl der Sitzungen mit hohem Wasserzeichen**

  Gibt die maximale Anzahl aktiver Benutzersitzungen seit dem letzten Zurücksetzen an.

Tabelle 11. Anzahl der Sitzungen mit hohem Wasserzeichen

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

- **Anzahl der Sitzungen mit niedrigem Wasserzeichen**

  Gibt die minimale Anzahl aktiver Benutzersitzungen seit dem letzten Zurücksetzen an.

Tabelle 12. Anzahl der Sitzungen mit niedrigem Wasserzeichen

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

Warteschlangenmetriken

Sie können Warteschlangenmetriken verwenden, um festzustellen, ob das System mit der Nachfrage Schritt halten kann. Wenn z. B. Anforderungen zu viel Zeit in einer Warteschlange verbringen, verfügen Sie möglicherweise nicht über ausreichende Ressourcen, um die Nachfrage zu decken.

Warteschlangenmessdaten sind für Services verfügbar, die Warteschlangen verwenden, wie z. B. den Berichtsservice und den Berichtsdatenservice.

Auf Systemebene stehen Warteschlangenmetriken für die folgenden Einträge zur Verfügung:

- Job

  Jobwarteschlange enthält Metriken, die sich auf die interne Warteschlange beziehen, die von allen Ereignismanagementservices verwendet wird.

- Aufgabe

  Taskwarteschlange enthält Messwerte, die sich auf die interne Warteschlange beziehen, die von allen Überwachungsservices verwendet wird. Diese Warteschlange enthält Tasks, bis sie erfolgreich abgeschlossen wurden.

- SMTP

  SMTP-Warteschlange enthält Messwerte, die sich auf die interne Warteschlange beziehen, die von allen Bereitstellungsservices verwendet wird. Diese Warteschlange enthält E-Mail-Nachrichten, bis sie gesendet werden.

Einige der Metriken, die für diese Warteschlangenmetrikgruppen verfügbar sind, müssen aktiviert werden. Weitere Informationen finden Sie unter „Messwerte für Job-, SMTP-und Taskwarteschlange aktivieren" auf Seite 94.

Die folgenden Warteschlangenmetriken sind verfügbar:

· **Latenz**

Gibt die durchschnittliche Zeit an, die Anforderungen in der Warteschlange verbracht haben (in Sekunden).

Tabelle 13. Latenz

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Service	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

· **Anzahl Warteschlangenanforderungen**

Gibt die Anzahl der Anforderungen an, die die Warteschlange durchlaufen haben.

Tabelle 14. Anzahl Warteschlangenanforderungen

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Service	Zähler	Seit dem Zurücksetzen	Bei Änderung

· **Länge der Warteschlange**

Gibt die Anzahl der Elemente an, die sich momentan in der Warteschlange befinden.

Tabelle 15. Länge der Warteschlange

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Service	Messanzeige	Zeitpunkt	Auf Anfrage

· **Hochwasserzeichen für Warteschlangenlänge**

Gibt die maximale Anzahl der Einträge in der Warteschlange seit dem letzten Zurücksetzen an.

Tabelle 16. Hochwasserzeichen für Warteschlangenlänge

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Service	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

· **Niedrige Länge des Warteschlangenlänge**

Gibt die minimale Anzahl von Elementen in der Warteschlange seit dem letzten Zurücksetzen an.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Service	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

· **Zeit in Warteschlange**

Gibt die kumulative Zeit an, die Anforderungen in der Warteschlange verbracht haben (in Tagen, Stunden, Minuten und Sekunden).

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Service	Zähler	Seit dem Zurücksetzen	Bei Änderung

· **Zeit in Warteschlangenhochwasserzeichen**

Gibt die maximale Zeitdauer an, die eine Anforderung in der Warteschlange gewartet hat (in Tagen, Stunden, Minuten und Sekunden).

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Service	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

· **Zeit in Warteschlange mit niedrigem Wasserzeichen**

Gibt die Mindestlänge (in Tagen, Stunden, Minuten oder Sekunden) an, die eine Anforderung in der Warteschlange gewartet hat.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Service	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

JVM-Metriken

Sie können JVM-Messwerte verwenden, um die Java Virtual Machine und die zugehörige Heapspeichergröße zu überwachen, die die Menge an Speicher angibt, die derzeit im Gebrauch ist. Wenn z. B. ein Dispatcher für eine lange Zeit ausgeführt wird und die Heapspeicherbelegung hoch ist, können Sie den Dispatcher erneut starten. Die Metrik "Maximale Größe des Heapspeichers" teilt Ihnen mit, ob Sie der JVM auf der Basis der verfügbaren Hardwarespeichermenge eine geeignete Speicherkapazität zugeordnet haben. Die aktuelle Größe des Heapspeichers, bezogen auf die maximale Größe des Heapspeichers, ermöglicht es Ihnen, zu wissen, ob verfügbarer Speicher verwendet wird. Wenn die aktuelle Größe des Heapspeichers in der Nähe der maximalen Größe des Heapspeichers liegt, können Sie die Einstellungen für die Optimierung anpassen, um die Belastung für eine bestimmte JVM zu reduzieren.

Die aktuelle Größe des Heapspeichers kann in Abhängigkeit von der aktuellen Belastung des Systems stark variieren.

Weitere Informationen zur Optimierung finden Sie im Artikel „Serverleistung optimieren“ auf Seite 63.

Die folgenden JVM-Metriken sind verfügbar:

- **Aktuelle Größe des Heapspeichers (Byte)**

  Gibt die aktuelle Größe des JVM-Heapspeichers (in Byte) an.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
Dispatcher	Messanzeige	Zeitpunkt	Auf Anfrage

- **Anfänglich angeforderte Heapspeichergröße (Byte)**

  Gibt die Anfangsgröße des Speichers an, den die JVM beim Start vom Betriebssystem anfordert (in Byte).

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
Dispatcher	Messanzeige	Zeitpunkt	Auf Anfrage

- **Maximale Größe des Heapspeichers (Byte)**

  Gibt die maximale Speichermenge an, die von der JVM (in Byte) verwendet werden kann.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
Dispatcher	Messanzeige	Zeitpunkt	Auf Anfrage

- **Zeit bis zu**

  Die Zeitdauer, die die JVM ausgeführt hat (in Tagen, Stunden, Minuten und Sekunden).

  Auf System-, Server-und Servergruppenebenen ist dies der höchste Wert von allen zugeordneten Dispatchern.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher	Zähler	Zeitpunkt	Auf Anfrage

- **Festgeschriebene Heapspeichergröße**

  Gibt die Menge an Speicher an, die für die Verwendung durch die JVM (in Byte) garantiert verfügbar ist.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
Dispatcher	Messanzeige	Zeitpunkt	Auf Anfrage

Anforderungsmessdaten

Sie können Request Metrics verwenden, um den Umfang der Anforderungen, den Betriebsstatus der Services, die Antwortzeiten und die Verarbeitungszeiten zu überwachen. Allgemeine Anforderungsmetriken umfassen Daten für alle Services und sind eine Konsolidierung von Metriken für alle Dispatcher. Anforderungsmessdaten, die für einen Service spezifisch sind, enthalten nur Daten für diesen Service.

Auf System-, Server-und Servergruppenebenen enthalten die Messwerte Daten von allen zugeordneten Dispatchern. Auf der Dispatcherebene schließen Metriken alle zugehörigen Services ein.

Die folgenden Request-Metriken sind verfügbar:

- **Aktuelle Uhrzeit**

  Gibt das aktuelle Datum und die aktuelle Uhrzeit an, die der Service verwendet, um Zeitwerte zu interpretieren.

  Verwenden Sie nur, wenn der Service keinen Taktsynchronisationsmechanismus hat.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
Service	Zähler	Zeitpunkt	Auf Anfrage

- **Letzte Antwortzeit**

  Gibt die Verarbeitungszeit für die letzte erfolgreiche oder fehlgeschlagene Anforderung an (in Tagen, Stunden, Minuten und Sekunden).

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher Service	Messanzeige	Zeitpunkt	Bei Änderung

- **Anzahl der fehlgeschlagenen Anforderungen**

  Gibt die Anzahl der Serviceanforderungen an, die fehlgeschlagen sind (ein Fehler wurde zurückgegeben).

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher Service	Zähler	Seit dem Zurücksetzen	Bei Änderung

- **Anzahl verarbeiteter Anforderungen**

  Gibt die Anzahl der verarbeiteten Anforderungen an.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher Service	Zähler	Seit dem Zurücksetzen	Bei Änderung

· **Anzahl erfolgreicher Anforderungen**

Gibt die Anzahl der Serviceanforderungen an, die erfolgreich ausgeführt wurden (es wurde kein Fehler zurückgegeben).

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher Service	Zähler	Seit dem Zurücksetzen	Bei Änderung

· **Prozentsatz fehlgeschlagener Anforderungen**

Gibt den Prozentsatz verarbeiteter Anforderungen an, die fehlgeschlagen sind.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher Service	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

· **Prozentsatz erfolgreicher Anforderungen**

Gibt den Prozentsatz verarbeiteter Anforderungen an, die erfolgreich ausgeführt wurden.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher Service	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

· **Hochwasserzeichen für Antwortzeit**

Gibt die maximale Dauer an, die für die Verarbeitung einer erfolgreichen oder fehlgeschlagenen Anforderung (in Tagen, Stunden, Minuten und Sekunden) benötigt wird.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher Service	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

· **Niedriges Wasserzeichen für Antwortzeit**

Gibt die Mindestlänge an, die für die Verarbeitung einer erfolgreichen oder fehlgeschlagenen Anforderung (in Tagen, Stunden, Minuten und Sekunden) benötigt wird.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher Service	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

· **Sekunden pro erfolgreicher Anforderung**

Gibt die durchschnittliche Dauer an, die für die Verarbeitung einer erfolgreichen Anforderung (in Sekunden) benötigt wird.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher Service	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

· **Servicezeit**

Gibt die Zeit an, die zum Verarbeiten aller Anforderungen (in Tagen, Stunden, Minuten und Sekunden) benötigt wird.

Eintrag	Änderungszeit	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher Service	Zähler	Seit dem Zurücksetzen	Bei Änderung

· **Anforderung für Servicezeit fehlgeschlagen**

Gibt die Zeit an, die zum Verarbeiten aller fehlgeschlagenen Serviceanforderungen (in Tagen, Stunden, Minuten und Sekunden) benötigt wird.

Eintrag	Änderungszeit	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher Service	Zähler	Seit dem Zurücksetzen	Bei Änderung

- **Servicezeit-erfolgreiche Anforderungen**

  Gibt die Zeit an, die zum Verarbeiten aller erfolgreichen Serviceanforderungen (in Tagen, Stunden, Minuten und Sekunden) benötigt wird.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher Service	Zähler	Seit dem Zurücksetzen	Bei Änderung

- **Erfolgreiche Anforderungen pro Minute**

  Gibt die durchschnittliche Anzahl der erfolgreichen Anforderungen an, die in einer Minute verarbeitet wurden.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Dispatcher Service	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

Prozessmetriken für Bericht-und Stapelberichtsservice und Metadaten-Service

Die folgenden Prozessmessdaten stehen für den Berichtsservice und den Stapelberichtsservice und den Metadatenservice zur Verfügung:

- **Anzahl der Prozesse**

  Gibt die Anzahl der Prozesse an, die momentan ausgeführt werden.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Berichtsservice und Stapelberichtsservice Metadatenservice	Messanzeige	Zeitpunkt	Auf Anfrage

· **Anzahl konfigurierter Prozesse**

Gibt den gleichen Wert an, der für die folgenden Eigenschaften von betroffenen Services konfiguriert wurde:

- "Maximale Anzahl der Prozesse für den [Servicename] während der Spitzenzeit"
- "Maximale Anzahl der Prozesse für den [Servicename] während der Nicht-Spitzenzeit" als Nicht-Standardwert sein

Dieser Wert kann nicht zurückgesetzt werden.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Berichtsservice und Stapelberichtsservice Metadatenservice	Messanzeige	Zeitpunkt	Auf Anfrage

· **Anzahl der Prozesse hohe Wasserzeichen**

Für System-, Server-und Servergruppe wird die Gesamtzahl aller Prozesse für die Anzahl der Prozesse mit hohem Wasserzeichen für alle zugeordneten Ressourcen angegeben.

Bei Services wird die maximale Anzahl der Prozesse angegeben, die zu einem beliebigen Zeitpunkt seit dem letzten Zurücksetzen ausgeführt wurden.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Berichtsservice und Stapelberichtsservice Metadatenservice	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

· **Anzahl der Prozesse mit niedrigem Wasserzeichen**

Für System-, Server-und Servergruppe wird die Gesamtzahl aller Prozesse mit niedriger Wasserzeichenmetrik für alle zugeordneten Ressourcen angegeben.

Bei Services ist die minimale Anzahl der Prozesse, die zu einem beliebigen Zeitpunkt seit dem letzten Zurücksetzen ausgeführt wurden, angegeben.

Eintrag	Änderungstyp	Zeitbereich	Zeitpunkt der Erfassung
System Server-/Servergruppe Berichtsservice und Stapelberichtsservice Metadatenservice	Messanzeige	Seit dem Zurücksetzen	Bei Änderung

Teilfenster auf der Seite 'Status System'

Die Seite "System" verfügt über drei Teilfenster "Scorecard", "Kennzahlen" und "Einstellungen", die Sie zum Auswerten des Systemstatus verwenden.

Sie können einige Spalten sortieren, indem Sie auf den Titel klicken. Standardmäßig werden Spalten in aufsteigender Reihenfolge sortiert. Um in aufsteigender Reihenfolge zu sortieren, klicken Sie einmal an. Um in absteigender Reihenfolge zu sortieren, klicken Sie erneut an. Wenn Sie zur Standardreihenfolge zurückkehren möchten, klicken Sie auf ein drittes Mal. Sie können jedes Teilfenster unabhängig aktualisieren.

Scorecard-Teilfenster

Im Teilfenster **Scorecard** werden Einträge aufgelistet: System, Server, Servergruppen, Dispatcher und Services. Für jeden Eintrag wird ein Metrikscore und ein Betriebsstatus angezeigt, sodass Sie die Systemleistung bewerten können. Weitere Informationen finden Sie unter „Systemleistung bewerten" auf Seite 37.

Jede Metrikbewertung wird durch eines der folgenden Symbole dargestellt:

- ein grüner Kreis für gute 
- Gelber Diamant für durchschnittlich 
- ein rotes Quadrat für arme 

Sie müssen Metrikschwellenwerte festlegen, bevor Metrikbewertungen angezeigt werden. Weitere Informationen finden Sie unter „Werte für Metrikschwellenwert festlegen" auf Seite 38.

Wenn ein Service in IBM Cognos -Konfiguration inaktiviert ist, wird er nicht aufgelistet.

Die Metrikbewertung für jeden Eintrag basiert auf der Leistung einzelner untergeordneter Einträge. Der Status, der für jeden Eintrag angezeigt wird, ist der niedrigste Status der untergeordneten Einträge. Wenn zum Beispiel alle Messwerte für einen Dispatcher gut sind, aber ein Service für diesen Dispatcher eine schlechte Metrik hat, ist die Metrikbewertung für den Dispatcher schlecht.

Der Status ist einer der folgenden Werte:

- **Verfügbar** , wenn alle Komponenten verfügbar sind
- **Teilweise verfügbar** , wenn mindestens eine Komponente verfügbar ist und mindestens eine Komponente nicht verfügbar oder teilweise nicht verfügbar ist.
- **Nicht verfügbar** , wenn alle Komponenten nicht verfügbar sind

Über das Menü "Gruppenaktionen" können Sie Funktionen ausführen, wie z. B. das Starten und Stoppen von Dispatchern oder Services „Stoppen und Starten von Disponenten und Services" auf Seite 45, die Registrierung von Dispatchern „Dispatcher aus der Umgebung entfernen" auf Seite 47und das Testen von Dispatcher „Dispatcher testen" auf Seite 53. Jeder Eintrag verfügt außerdem über ein Menü "Aktionen", auf das Sie zugreifen können, indem Sie auf den Pfeil neben dem Eintrag klicken.

Sie verwenden das Teilfenster **Scorecard** , um zu dem Eintrag zu navigieren, den Sie anzeigen möchten. Sie können die Ansicht auswählen, die Sie über das Menü Ansicht ändern in der linken oberen Ecke anzeigen möchten. Sie können auf Einträge klicken, um sie auszuwählen und die nächste Ebene von Einträgen anzuzeigen. Klicken Sie zum Beispiel auf einen Server, um zugeordnete Dispatcher anzuzeigen, oder klicken Sie auf einen Dispatcher, um die zugehörigen Services anzuzeigen.

Sie können das Teilfenster **Scorecard** maximieren, um eine konsolidierte Ansicht von Informationen anzuzeigen, die im Teilfenster **Scorecard** angezeigt werden, sowie wichtige Messwerte aus dem Teilfenster **Metriken** . Die konsolidierte Ansicht enthält die folgenden Informationen:

- Für Server und Servergruppen: Metrikbewertung, Betriebsstatus, Auflaufzeit, Servicezeit, Anzahl verarbeiteter Anforderungen und Prozentsatz erfolgreicher Anforderungen.

- Für Dispatcher: Metrikbewertung, Betriebsstatus, Anzahl der Prozesse, Servicezeit, aktuelle Größe des Heapspeichers (Byte), Anzahl der verarbeiteten Anforderungen und Prozentsatz der erfolgreichen Anforderungen.
- Für Services sind die Informationen von dem Service abhängig.

Teilfenster 'Metriken'

Im Teilfenster **Metriken** werden die Metriken für den ausgewählten Eintrag angezeigt. Sie können Metrikgruppen erweitern, um die einzelnen Metrikbewertungen und -werte anzuzeigen. Sie können jede Metrikgruppe unabhängig von „Metriken zurücksetzen" auf Seite 39zurücksetzen.

Wählen Sie zum Auswählen der Messwerte, die angezeigt werden sollen, mindestens ein Kontrollkästchen für die Werte "Gut", "Durchschnitt", "Armen" oder " **Keine Metrikbewertung** " aus. Standardmäßig werden alle Messwerte angezeigt. Zu den Metriken ohne Metrikbewertung gehören solche, für die Sie keine Schwellenwerte festlegen können und für die Sie noch keine Schwellenwerte für die Messgröße festgelegt haben. Für Letzteres müssen Sie sie anzeigen, indem Sie auf das Markierungsfeld **Keine Metrikbewertung** klicken, bevor Sie sie festlegen können.

Teilfenster 'Einstellungen'

Im Teilfenster **Einstellungen** werden die Einstellungen angezeigt, die dem ausgewählten Eintrag im Modus 'Nur Ansicht' zugeordnet sind. Um die Einstellungen zu ändern, klicken Sie auf die Schaltfläche 'Eigenschaften festlegen'  .

Weitere Informationen zu den Einstellungen im Teilfenster " **Einstellungen** " finden Sie unter Kapitel 5, „Serververwaltung", auf Seite 41.

Systemleistung bewerten

Um zu bewerten, wie die IBM Cognos -Software ausgeführt wird, können Sie Metrikbewertungen anzeigen, die auf den von Ihnen festgelegten Schwellenwerten basieren. Sie können auch den Betriebsstatus von Systemkomponenten anzeigen.

Sie müssen Metrikschwellenwerte festlegen, bevor Metrikbewertungen angezeigt werden. Weitere Informationen finden Sie unter „Werte für Metrikschwellenwert festlegen" auf Seite 38. Wenn Dispatcher und Services nicht so ausgeführt werden, wie sie sollten, können Sie die Serverleistung optimieren „Serverleistung optimieren" auf Seite 63. Weitere Informationen zu Protokollierungseinstellungen finden Sie unter Kapitel 3, „Protokollierung konfigurieren", auf Seite 15.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.

   Das Metrikpunktsymbol für den **System** -Eintrag zeigt den Gesamtsystemstatus an. Das Metrikpunktsymbol für jeden Server zeigt den Status dieses Servers an. Im Teilfenster **Metriken** werden einzelne Metriken aufgelistet.
2. Klicken Sie im Teilfenster ' **Scorecard** ' im Menü der Änderungsansicht der aktuellen Ansicht auf **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.

   Wenn Sie **Alle Servergruppen**auswählen, zeigen Sie die Dispatcher an, die nicht nach Server gruppiert sind, indem Sie auf **Standardservergruppe**klicken.
3. Klicken Sie auf den Eintrag, um die Metriken für ein ausgezeigtes Element anzuzeigen.
4. Um die untergeordneten Elemente eines angezeigten Eintrags anzuzeigen, klicken Sie auf den Eintrag.

   Tipp: Sie können einzelne Teilfenster aktualisieren, indem Sie in der Anzeige auf die Schaltfläche zum Aktualisieren klicken.
5. Wenn Sie die Eigenschaften eines Eintrags anzeigen oder ändern möchten, klicken Sie auf die Schaltfläche 'Aktionen' neben dem Eintrag und klicken Sie dann auf **Eigenschaften festlegen**.

6. Um die konsolidierte Ansicht anzuzeigen, klicken Sie auf die Schaltfläche 'Maximieren' im Teilfenster '**Scorecard** '.

   Tipp: Wenn Sie zur vorherigen Ansicht zurückkehren möchten, klicken Sie auf die Schaltfläche 'Zurückspeichern'.

Attribute für Metrikbewertungen anzeigen

Sie können das letzte Mal anzeigen, dass ein Messwert zurückgesetzt und aktualisiert wurde. Sie können auch die aktuelle Schwellenwerteinstellung für jede Metrikbewertung anzeigen, für die ein Schwellenwert festgelegt ist. Für Messwerte, die in regelmäßigen Intervallen erfasst werden, können Sie auch den Zeitraum anzeigen, für den der Wert gilt.

Vorbereitende Schritte

Weitere Informationen zu Schwellenwerteinstellungen finden Sie unter „Werte für Metrikschwellenwert festlegen" auf Seite 38.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf die gewünschte Ansicht.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Erweitern Sie im Teilfenster **Metriken** die  -Metrikgruppe, die Sie anzeigen möchten.
4. Halten Sie in der Spalte **Wert** des Teilfensters **Metriken** den Zeiger auf den Wert für den Messwert, den Sie anzeigen möchten.

   Der Name des Messwerts wird angezeigt.
5. Wenn Sie weitere Informationen zu einigen Metriken anzeigen möchten, klicken Sie auf **Mehr**.

Werte für Metrikschwellenwert festlegen

Sie können Schwellenwerte festlegen, die für einige Metrikbewertungen verwendet werden.

Zulässige Schwellenwerte hängen von Ihrer Betriebsumgebung ab. Wenn ein Schwellenwert überschritten wird, ändert sich der Status der Metrikbewertung.

Beispiel: Sie legen fest, dass die maximal zulässige Warteschlangenlänge 50 Elemente beträgt. Sie wählen **Niedrige Werte sind gut**aus. Sie setzen den oberen Wert auf 50 und den unteren Wert auf 40. Wenn die Warteschlange unter 40 Elementen in der Länge bleibt, ist die Metrikbewertung grün (gut). Wenn die Warteschlangenlänge über 40 Einträge überschreitet, ist die Metrikbewertung gelb (Durchschnitt). Wenn die Warteschlangenlänge über 50 Einträge überschreitet, ist die Metrikbewertung rot (schlecht).

Oder für den Prozentsatz der erfolgreichen Anforderungen, wählen Sie **Hohe Werte sind gut**aus. Sie setzen den oberen Wert auf 98 und den unteren Wert auf 95. Wenn der Prozentsatz der erfolgreichen Anforderungen unter 95 Prozent liegt, ist die Metrikbewertung rot (schlecht). Wenn der Prozentsatz der erfolgreichen Anforderungen zwischen 95 und 98 Prozent liegt, ist die Metrikbewertung gelb (Durchschnitt). Wenn der Prozentsatz der erfolgreichen Anforderungen über 98 bleibt, ist die Metrikbewertung grün (gut).

Änderungen an Schwellenwerten sind sofort wirksam.

Es sind keine Schwellenwerte für Schwellenwerte vorhanden. Sie müssen Schwellenwerte für die Anzeige von Metrikbewertungen festlegen.

Vorbereitende Schritte

Protokolleinträge Kapitel 3, „Protokollierung konfigurieren”, auf Seite 15 treten unter den folgenden Umständen auf:

- Wenn Messschwellenwerte verletzt werden
- wenn Aufzählungsmetriken, wie z. B. Betriebsstatus, geändert werden

Protokolle werden nicht generiert, wenn Metrikwerte sich ändern, aber im selben Bereich bleiben.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf die gewünschte Ansicht.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Wenn Sie den Schwellenwert für einen Messwert ändern möchten, klicken Sie im Teilfenster **Metriken** auf die Schaltfläche Schwellenwerte bearbeiten  für den Messwert.
4. Klicken Sie auf das gewünschte Leistungsmuster: **Hohe Werte sind gut**, **Mittelwerte sind gut**oder **Niedrige Werte sind gut**.
5. Wenn Sie einen Schwellenwert angeben möchten, klicken Sie in das Schwellenwertfeld und geben Sie die gewünschte Schwellenwertnummer ein.
6. Klicken Sie auf den Pfeil für den Schwellenwert, um anzugeben, in welchen Bereich der Wert selbst fällt.

   Wenn Ihr Maximalwert beispielsweise 50 beträgt und Sie möchten, dass Werte von 50 in die durchschnittliche Kategorie und nicht in die Kategorie "Arme" fallen, klicken Sie auf den Pfeil, um den Schwellenwert in die durchschnittliche Kategorie zu verschieben.
7. Klicken Sie **OK.**

Metriken zurücksetzen

Sie können eine Gruppe von Messwerten jederzeit zurücksetzen.

Wenn Sie eine Gruppe von Metriken zurücksetzen, werden alle Metriken in der Gruppe zurückgesetzt. Beispiel: Für einen Server können Sie die Servicegruppe 'Warteschlangenberichtsservice' von Metriken zurücksetzen.

Einige Metriken können nicht zurückgesetzt werden. Die JVM-Metriken können beispielsweise nicht zurückgesetzt werden, weil sie nach dem letzten Zurücksetzen neu berechnet wurden.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf die gewünschte Ansicht.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im Teilfenster **Metriken** auf die Schaltfläche 'Zurücksetzen'  für die Gruppe der Messwerte, die zurückgesetzt werden sollen.

Metriken für das System zurücksetzen

Sie können alle Messwerte für das System gleichzeitig zurücksetzen.

Einige Metriken können nicht zurückgesetzt werden. Die JVM-Metriken können beispielsweise nicht zurückgesetzt werden, weil sie nach dem letzten Zurücksetzen erneut berechnet wurden.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** auf **Aktionen**, **Alle Metriken des Systems zurücksetzen**.

Berichtsserviceverbindungen aktualisieren

Wenn ein PowerCube erneut erstellt wurde, können Sie die Verbindungsinformationen aktualisieren, ohne die aktuellen Benutzer zu beeinträchtigen.

Sie müssen die Verbindungsinformationen zuerst auf den wiederaufgebauten PowerCube aktualisieren und dann die Berichtsserver aktualisieren, damit der neu erstellte PowerCube für neue Verbindungen verwendet werden kann.

Weitere Informationen finden Sie unter „Aktualisierte PowerCubes implementieren” auf Seite 156.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Wenn alle Server angezeigt werden, klicken Sie auf das Kontrollkästchen für die gewünschten Server und klicken Sie im Menü "Gruppenaktionen" auf Serviceverbindungen für Berichtsservices aktualisieren.

   Tipp: Sie können dies auch über das Menü "Aktionen" neben System-, Server-und Dispatcher-Dispatchern ausführen. Sie können auch auf die Registerkarte "Konfiguration" klicken und anschließend auf "Dispatcher und Services" klicken und dann auf die Schaltfläche **Berichtsserviceverbindungen aktualisieren-Konfiguration** klicken.
3. Wenn die Seite **Ergebnisse anzeigen** angezeigt wird, stellen Sie sicher, dass die Operation erfolgreich ausgeführt wurde, und klicken Sie anschließend auf Schließen.

Kapitel 5. Serververwaltung

Die Serververwaltung umfasst das Verwalten und Verwalten Ihres IBM Cognos -Systems und die Optimierung der Systemleistung.

Sie sollten mit den IBM Cognos -Komponenten vertraut sein und wie sie installiert und konfiguriert werden. Wenn Sie IBM Cognos -Server oder -Komponenten auf mehr als einem Computer installiert haben, können alle Funktionen über die Systemadministration gesteuert werden. Informationen zur Umgebung von IBM Cognos finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Für einige Serververwaltungstasks verwenden Sie die Verwaltungskomponenten und müssen über die erforderlichen Berechtigungen für die Zugriffsverwaltungsfunktionalität Kapitel 13, „Funktionen” , auf Seite 207verfügen.

Dispatcher und Services

Der Dispatcher ist der Eingangspunkt für IBM Cognos -Serviceanforderungen, die von einem Web-Server-Gateway oder einer anderen Software gesendet werden. Der Dispatcher verarbeitet die Routing-Anforderungen und gleicht die Last der Benutzeranforderungen an die verschiedenen IBM Cognos -Services aus.

Sie können mehr als einen Dispatcher in Ihrer IBM Cognos -Umgebung haben. In solchen verteilten Installationen wird ein Dispatcher für jede Instanz der Content Manager-oder Application-Tier-Komponenten konfiguriert, die in Ihrer Umgebung installiert und konfiguriert sind.

Nachdem Sie IBM Cognos -Software installiert 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.

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 17. 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.
Content Manager-Cacheservice	Verbessert die Gesamtsystemleistung und die Content Manager-Skalierbarkeit, indem häufige Abfrageergebnisse in den einzelnen Dispatchern zwischengespeichert werden.

Tabelle 17. IBM Cognos services (Forts.)

Service	**Zweck**
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.
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

Tabelle 17. IBM Cognos services (Forts.)	
Service	**Zweck**
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.
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.

Tabelle 17. IBM Cognos services (Forts.)	
Service	**Zweck**
Verwaltungskonsolenservice planen	Verwaltet die Kommunikation mit der Contributor Administration Console.
Planungsdatenservice	Verwaltet die Kommunikation für die Echtzeitberichterstellung von Contributor-Plandaten.
Planungsjobservice	Verwaltet die Kommunikation mit dem Subsystem Planning Job Server.
Web-Service planen	Verwaltet die Kommunikation mit Contributor Web und Contributor Add-in für *Excel* -Benutzer.
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.

Tabelle 17. IBM Cognos services (Forts.)	
Service	**Zweck**
Systemservice	Definiert den Bus-API-konformen Service, der zum Abrufen von anwendungsweiten Konfigurationsparametern verwendet wird. Außerdem werden Methoden bereitgestellt, die Ländereinstellungszeichenfolgen normalisieren und validieren und Ländereinstellungen für Ländereinstellungen, die von Ihrer Anwendung unterstützt werden, zugeordnet werden.
Visualisierungsgalerie-Service	Wird zum Laden und Abrufen von RAVE1-Visualisierungen in die Visualisierungsgalerie in Reportingverwendet. Er ist für den Berichtsservice erforderlich.

Stoppen und Starten von Disponenten und Services

Sie können Disponenten und Services manuell stoppen und starten. Wenn ein Service nicht mehr antwortet, müssen Sie ihn stoppen und erneut starten.

Jeder Disponent und jeder Service kann

- Gestartet
- Sofort gestoppt und alle Anforderungen, die ausgeführt oder in die Warteschlange gestellt wurden, gelöscht, ohne diese Anforderungen zu beenden.
- Gestoppt, nachdem aktive und eingereihte Anforderungen verarbeitet wurden

Sie können alle Dispatcher und Services in der IBM Cognos -Umgebung auf einmal stoppen oder starten.

Wenn Sie die IBM Cognos -Software mit dem Konfigurationstool starten, werden alle Dispatcher und Services gestartet, sofern sie nicht im Konfigurationstool inaktiviert sind. Weitere Informationen finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Standardmäßig starten alle Services, wenn Sie den Computer erneut starten, auf dem sie installiert sind.

Vorbereitende Schritte

Das Stoppen eines Service stoppt auch alle seine Prozesse. Wenn Sie einen Dispatcher stoppen, werden alle zugehörigen Services gestoppt. Wenn der abgehängte Dispatcher über einen aktiven Content Manager verfügt, sind alle Benutzer mit Ausnahme von Administratoren gesperrt.

Nachdem ein Service gestoppt wurde, verfügt er über einen ausgesetzten Status Kapitel 4, „Systemleistungsmetriken”, auf Seite 25.

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Siehe Kapitel 13, „Funktionen”, auf Seite 207.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf die Dispatcher oder Services, die Sie möchten.

   Klicken Sie auf **Alle Server**, **Alle Servergruppen**oder **Alle Dispatcher**. Wenn Sie einen Service auswählen möchten, halten Sie den Mauszeiger über **Dienstleistungen** und klicken Sie auf den erforderlichen Service.

3. Klicken Sie auf den Menüpfeil 'Aktionen' für den Dispatcher oder den Service, und wählen Sie die Aktion aus, die Sie ausführen möchten.

   Abhängig vom Dispatcher oder Service können Sie die folgenden Aktionen ausführen:

Tabelle 18. Dispatcher und Services stoppen und starten: Ziele, Ansichten und Aktionen

Ziel	Sicht 'Scorecard'	Aktion
Alle Disponenten im System starten	**Alle Server**	Klicken Sie im Menü "Gruppenaktionen" auf **Dispatcher starten**. **Tipp:** Wenn Sie eine Aktion nur auf einige Einträge anwenden möchten, wählen Sie Kontrollkästchen für mindestens einen Eintrag aus, und klicken Sie dann auf die gewünschte Aktion.
Starten Sie alle Dispatcher für eine Servergruppe.	**Alle Servergruppen**	Klicken Sie im Menü "Aktionen" der Servergruppe auf **Dispatcher starten**.
Alle Dispatcher für einen Server starten	**Alle Server**	Klicken Sie im Menü "Serveraktionen" auf **Dispatcher starten**.
Starten eines bestimmten Dispatchers	**Alle Dispatcher**	Klicken Sie im Menü "Dispatcheraktionen" auf **Start**.
Einen bestimmten Service starten	**Alle Services**	Klicken Sie im Menü "Serviceaktionen" auf **Start**.
Alle Dispatcher im System stoppen	**Alle Server**	Klicken Sie im Menü "Gruppenaktionen" auf **Dispatcher sofort stoppen** oder **Dispatcher nach Ausführung und Verarbeitung der Warteschlange stoppen**.
Stoppen Sie alle Dispatcher für eine Servergruppe.	**Alle Servergruppen**	Klicken Sie im Menü "Aktionen" der Servergruppe auf **Dispatcher sofort stoppen** oder **Dispatcher nach Ausführung und Verarbeitung der Warteschlange stoppen**.
Stoppen Sie alle Dispatcher für einen Server.	**Alle Server**	Klicken Sie im Menü "Serveraktionen" auf **Dispatcher sofort stoppen** oder **Dispatcher nach Ausführung und Verarbeitung der Warteschlange stoppen**.
Einen bestimmten Dispatcher stoppen	**Alle Dispatcher**	Klicken Sie im Menü "Dispatcheraktionen" auf **Sofort stoppen** oder **Nach Ausführung und Verarbeitung der Warteschlange stoppen**.

Tabelle 18. Dispatcher und Services stoppen und starten: Ziele, Ansichten und Aktionen (Forts.)		
Ziel	**Sicht 'Scorecard'**	**Aktion**
Einen bestimmten Service stoppen	**Alle Services**	Klicken Sie im Menü "Serviceaktionen" auf **Sofort stoppen** oder **Nach Ausführung und Verarbeitung der Warteschlange stoppen**.

Daraufhin wird ein Dialogfenster angezeigt, in dem die Aktion bestätigt wird.

4. Klicken Sie auf **Schließen**.

Active Content Manager-Service

Sie können einen Content Manager-Service, der sich im Standby-Modus befindet, manuell aktivieren.

Ein Content Manager-Service wird beim Start als aktiv bezeichnet. Alle anderen Content Manager-Services starten im Standby-Modus. Nur ein Content Manager-Service kann jederzeit aktiv sein. Wenn Sie einen Service aktivieren, wechselt jeder derzeit aktive Service in den Standby-Modus.

Sie können auch einen Content Manager-Service angeben, der derzeit beim Start als aktiver Standardservice Standby ist.

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf **IBM Cognos Administration**verfügen. Siehe Kapitel 13, „Funktionen”, auf Seite 207.

Standard-Content-Manager-Service angeben

Sie können einen Standard-Content-Manager-Service angeben.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Dienstleistungen** > **Content Manager**.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im Menü **ContentManagerService Aktionen** auf **Standardmäßig als aktiv festlegen**.

   Tipp: Im Menü "Aktionen" werden nur Content Manager-Services angezeigt, die nicht bereits die Standardservices sind **Standardmäßig als aktiv festlegen**

Content Manager-Service aktivieren

Sie können einen bestimmten Content-Manager-Service aktivieren.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Dienstleistungen** > **Content Manager**.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im Menü **ContentManagerService Aktionen** auf **Start**.

Dispatcher aus der Umgebung entfernen

Sie können einen Dispatcher entfernen, wenn er in der IBM Cognos -Umgebung nicht mehr benötigt wird.

Sie können den IBM Cognos -Service mit IBM Cognos -Konfiguration stoppen. Dadurch wird auch der Dispatcher gestoppt. Wenn Sie einen Dispatcher löschen, ohne zuerst den IBM Cognos -Service zu stoppen, wird der Dispatcher automatisch in 30 Sekunden wieder eingesetzt.

Vorbereitende Schritte

Um einen Dispatcher zu entfernen, müssen Sie den Dispatcher zunächst von dem Computer aus stoppen, auf dem er installiert ist. Nach dem Stoppen des Dispatchers müssen Sie den Dispatcher aus dem Content-Store entfernen, indem Sie ihn in IBM Cognos Administration zurücknehmen.

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Siehe Kapitel 13, „Funktionen”, auf Seite 207.

Vorgehensweise

1. Stop the IBM Cognos service using IBM Cognos Configuration.

   Dadurch wird auch der Dispatcher gestoppt. Informationen zum Stoppen des IBM Cognos -Service finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.
2. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
3. Bestimmen Sie die Dispatcher, die Sie abmelden möchten. Sie können die Registrierung aller Dispatcher im System aufheben, die Registrierung aller Dispatcher für einen Server aufheben oder die Registrierung aller Dispatcher für eine Servergruppe aufheben.
4. Klicken Sie im Teilfenster ' **Scorecard** ' im Menü der Änderungsansicht der aktuellen Ansicht auf **Alle Server**, **Alle Servergruppen**oder **Alle Dispatcher**. Die Ansicht, die Sie auswählen, hängt davon ab, welche Dispatcher Sie abmelden möchten.

   Tabelle 19. Erforderliche Aktionen zur Erreichung der Ziele für die Registrierung von Disponenten

Ziel	**Aktion**
Die Registrierung aller Dispatcher im System aufheben	Klicken Sie in der Ansicht **Scorecard**, **Alle Dispatcher** auf den Pfeil, um das **Gruppenaktionen** -Menü anzuzeigen, und klicken Sie dann auf **Registrierung von Dispatchern aufheben**. **Tipp:** Wenn Sie eine Aktion nur auf einige Einträge anwenden möchten, wählen Sie Kontrollkästchen für mindestens einen Eintrag aus, und klicken Sie dann auf die gewünschte Aktion.
Aufheben der Registrierung aller Dispatcher für einen Server	Klicken Sie in der Ansicht **Scorecard**, **Alle Server** , in einem Servermenü **Aktionen** Servers auf **Registrierung von Dispatchern aufheben**.
Aufheben der Registrierung aller Dispatcher für eine Servergruppe	Klicken Sie in der Ansicht **Scorecard**, **Alle Servergruppen** , im Menü des Dispatchers **Aktionen** auf **Registrierung von Dispatchern aufheben**.
Registrierung eines bestimmten Dispatchers aufheben	Klicken Sie in der Ansicht **Scorecard**, **Alle Dispatcher** , im Menü des Dispatchers **Aktionen** auf **Registrierung aufheben**.

   Es wird ein Dialogfenster angezeigt, in dem die Aktion bestätigt wird.
5. Klicken Sie auf **OK**.

Die Dispatcherinformationen werden aus dem Content Store entfernt.

Dispatcher in Konfigurationsordnern gruppieren

Konfigurationsordner sind für die Organisation von Dispatchern nützlich, wenn Ihre Installation viele Dispatcher enthält. Sie können Dispatcher so gruppieren, dass Sie dieselben Konfigurationseinstellungen einmal auf alle Dispatcher und Services im Ordner anwenden können.

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Siehe Kapitel 13, „Funktionen”, auf Seite 207.

Informationen zu diesem Vorgang

Wenn Sie einen Dispatcher zu einem Konfigurationsordner hinzufügen, übernimmt er automatisch die Konfigurationseinstellungen des Ordners. Wenn Sie jedoch zuvor die Standardwerte dieses Dispatchers oder Service geändert haben, werden die geänderten Werte beibehalten.

Wenn Sie die Konfigurationseinstellungen eines Dispatchers oder Konfigurationsordners ändern, erfassen die Services für den Dispatcher und alle untergeordneten Einträge für den Ordner automatisch die neuen Werte. Wenn Sie jedoch die Werte der Services ändern, werden die geänderten Werte beibehalten.

Sie können einen neuen Konfigurationsordner im Stammverzeichnis des Konfigurationsbereichs oder in einem vorhandenen Konfigurationsordner erstellen.

Tipp:

- Um die Konfigurationseigenschaften des übergeordneten Elements eines Eintrags anzuzeigen und zu bearbeiten, der im Pfad in der Symbolleiste angezeigt wird, klicken Sie auf die Schaltfläche **Eigenschaften festlegen-Konfiguration**  . Sie können Konfigurationseinstellungen für alle Dispatcher und Services im Konfigurationsbereich ändern und anwenden, wenn Sie sich im Stammverzeichnis des Konfigurationsbereichs befinden.
- Verwenden Sie den Pfad in der Symbolleiste, um die verschiedenen Ebenen Ihrer Konfiguration zu untersuchen. Der Pfad beginnt mit der Konfiguration und, wenn der Pfad zu lang wird, wird der Pfad eingeschlossen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Dispatcher und Services**.
2. Klicken Sie auf die neue Ordnerschaltfläche.
3. Geben Sie einen Namen und, wenn Sie möchten, eine Beschreibung ein, und geben Sie an, wo der Konfigurationsordner gespeichert werden soll.
4. Klicken Sie auf **Fertigstellen**.

   Sie können jetzt Disponenten zum Konfigurationsordner hinzufügen, indem Sie sie von ihrer ursprünglichen Position abschneiden und sie anschließend im Ordner einfügen. Sie können auch Einstellungen auf der Ebene des Konfigurationsordners ändern.

   Tipp: Wenn Sie einen Dispatcher in einen anderen Ordner verschieben möchten, klicken Sie neben dem Dispatcher auf **Mehr** und klicken Sie dann auf **Verschieben**.

Dispatcher-Routing

Je nachdem, wie Ihr System eingerichtet ist, können Sie steuern, wie Berichte auf die Server verteilt werden.

Beispiel: Sie verfügen über verschiedene Abteilungen, die ihre eigenen Server verwalten, oder Sie verfügen über bestimmte Server, die für einen bestimmten Datenzugriff eingerichtet sind, wie z. B.

Microsoft Fenster -Server für Microsoft SQL Server-Datenbanken und Linux -Server, die für den Zugriff von IBM Db2 konfiguriert sind. You can set up IBM Cognos software so that report requests are processed by specific servers by applying routing rules.

Affinitätseinstellungen haben Vorrang vor erweiterten Routing-Einstellungen. Weitere Informationen finden Sie unter „Maximale Anzahl Prozesse und Verbindungen“ auf Seite 68.

Wenn Sie die Routing-Regeln definieren, müssen Sie eine Servergruppe auswählen. Servergruppennamen sind eine Eigenschaft eines Dispatchers oder der Konfigurationsordner, in die die Dispatcher organisiert werden. Weitere Informationen zum Festlegen von Servergruppennamen finden Sie im Artikel „Servergruppen für das erweiterte Dispatcherrouting erstellen“ auf Seite 63.

Um zu bestimmen, welche Servergruppen bestimmte Berichte verarbeiten, müssen Sie den Servergruppen Routing-Tags für Datenobjekte, wie z. B. Pakete, Datenmodule oder hochgeladene Dateien, sowie für Benutzergruppen oder Rollen zuordnen. Anschließend müssen Sie angeben, wie die Routing-Tags unter den Dispatchern in Ihrer Umgebung verteilt werden. Die Verteilung wird durch Routing-Regeln gesteuert, die Sie für die Routing-Tags erstellen. Die Berichtsanforderung wird von einem bestimmten Server abhängig von den Routing-Tags verarbeitet, die dem Datenobjekt zugeordnet sind, von dem aus der Bericht erstellt wurde, und/oder der Benutzer oder die Gruppe, auf dem bzw. der der Bericht ausgeführt wird.

Tipp: Ein Routing-Tag kann durch ein beliebiges Wort oder einen beliebigen Ausdruck, aber als bewährtes Verfahren einen Tag angeben, der für Ihre Umgebung aussagekräftig ist. Sie können Tags wie `Verkaufsberichte`, `DB2-Daten`, `Europa`haben.

Wenn Sie die Routing-Regeln erstellen, erstellen Sie Bedingungen, die die Servergruppen bestimmen, mit denen die Berichte verarbeitet werden sollen. Beispielsweise können Sie Routing-Regeln so konfigurieren, dass Berichte aus einem Finanzpaket, die von einem Benutzer in der Finanzgruppe erstellt wurden, von Finanzservern verarbeitet werden. Alternativ können Sie Routing-Regeln so konfigurieren, dass Berichte, die von allen Sales-Benutzern erstellt wurden, unabhängig davon, welches Datenobjekt für die Erstellung des Berichts verwendet wurde, von den Sales-Servern verarbeitet werden. Im ersten Beispiel würden Sie Routing-Tags sowohl für die Gruppe als auch für die Rolle und das Paket angeben. Im zweiten Beispiel würden Sie jedoch nur einen Routing-Tag für die Gruppe oder die Rolle angeben und den Wert für das Paket-Routing-Tag leer lassen. Sie müssen weder für das Datenobjekt als auch für die Gruppe oder Rolle in den Routing-Regeln einen Routing-Tag angeben.

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen“, auf Seite 207.

Routing-Tags für Gruppen oder Rollen festlegen

Sie können Routing-Tags für Gruppen oder Rollen festlegen. Die Routing-Tags werden verwendet, um Routing-Regeln für Dispatcher anzugeben.

Vorgehensweise

1. Öffnen Sie **IBM Cognos Administration**von **Verwalten** > **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Sicherheit** auf **Benutzer, Gruppen und Rollen**.
3. Klicken Sie auf den **Cognos** -Namespace, um die Gruppen und Rollen anzuzeigen.
4. Klicken Sie auf die Schaltfläche 'Eigenschaften festlegen'  für eine Gruppe oder Rolle.
5. Klicken Sie unter **Erweiterte Weiterleitung** > **Routing-Sets**auf **Festlegen**.

   Die Seite **Routing-Sets zuordnen** wird angezeigt.
6. Wählen Sie einen Routing-Tag für die Rolle oder Gruppe der Benutzer in **Verfügbare Routing-Sets**aus, oder geben Sie ihn in **Routing-Sets eingeben**ein, und klicken Sie auf die Schaltfläche Hinzufügen, um den Tag zum Feld **Zugewiesene Routing-Sets** hinzuzufügen. Wenn Sie mehrere Tags eingeben, trennen Sie die einzelnen Tags mit einem Semikolon. Beispiel: `Vertriebsgruppen; Marketing; Entwicklung`.

7. Wiederholen Sie Schritt 5, um weitere Routing-Schlüsselwörter hinzuzufügen, die Sie auf die Gruppe oder die Rolle anwenden möchten.

   Die Reihenfolge, in der die Routing-Tags hinzugefügt werden, spielt keine Rolle.
8. Klicken Sie auf **OK**.

   Die Routing-Tags werden unter **Erweiterte Weiterleitung** in der Gruppe-oder Rolleneigenschaftenseite angezeigt.
9. Klicken Sie in der **Seite 'Eigenschaften festlegen'**auf **OK**.

Ergebnisse

Die Routing-Tags werden verwendet, wenn „Routing-Regeln für Dispatcher festlegen" auf Seite 51verwendet wird.

Routing-Regeln für Dispatcher festlegen

Sie können Routing-Regeln für Dispatcher oder Konfigurationsordner festlegen.

Servergruppen sind eine Eigenschaft von Dispatchern oder Konfigurationsordnern und müssen eingerichtet werden, bevor Sie Routing-Regeln für Servergruppen festlegen können. Weitere Informationen finden Sie unter „Servergruppen für das erweiterte Dispatcherrouting erstellen" auf Seite 63.

Vorgehensweise

1. Öffnen Sie **IBM Cognos Administration**von **Verwalten** > **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Dispatcher und Services**.

   Die Dispatcher und alle erstellten Konfigurationsordner werden angezeigt.

   Tipp: Es müssen bereits Servergruppen eingerichtet werden. Weitere Informationen finden Sie unter „Servergruppen für das erweiterte Dispatcherrouting erstellen" auf Seite 63.
3. Wählen Sie in der Symbolleiste die Schaltfläche "Routing-Regeln"  aus.

   Die Seite **Routing-Regeln angeben** wird angezeigt.
4. Klicken Sie auf **Regel hinzufügen**.
5. Geben Sie die Routing-Regeln an, indem Sie die Routing-Tags mit Servergruppen anpassen. Eine Routing-Regel kann eine Kombination aus den folgenden Tags und Servergruppen sein:
   - **Datenroutingtag** und **Servergruppe**
   - **Gruppenleitungs-Tag** oder **Rollenroutingtag** und **Servergruppe**
   - **Datenroutingtag** und **Gruppenleitungs-Tag** oder **Rollenroutingtag** und **Servergruppe**
6. Klicken Sie in der Spalte **Aktionen** auf die Schaltfläche "Mitglieder anzeigen", um einen Überblick über die Mitglieder anzuzeigen.
7. Wenn Sie die Reihenfolge der Routing-Regeln ändern möchten, wählen Sie **Reihenfolge ändern**aus. Wählen Sie die Regel aus, die verschoben werden soll, und klicken Sie auf **Nach oben**, **Nach unten**, **Nach oben**oder **Nach unten**.

   Wichtig: Im Gegensatz zu Routing-Tags wirkt sich die Reihenfolge, in der die Routing-Regeln aufgelistet werden, auf die Art der Anwendung aus.

   Eine Regel wird abgeglichen, wenn Eigenschaften, die dem Datenobjekt oder der Gruppe oder Rolle zugeordnet sind, die an der Anforderung beteiligt sind, die Kriterien der Regel erfüllen. Die Regeln werden in der Reihenfolge ausgewertet, bis die erste Übereinstimmung erreicht ist, und die Anforderung wird an die Servergruppe weitergeleitet, die von der ersten Übereinstimmung benannt wurde, die abgeglichen wurde.
8. Klicken Sie auf **OK**.

Gatewayzuordnungen für IBM Cognos Series 7 PowerPlay -Daten angeben

Sie können die Position eines Series 7 PowerPlay -Servers angeben.

IBM Cognos for Microsoft Office users may send requests to Report data service (RDS) for data that resides on a Series 7 PowerPlay server. Der Berichtsdatenservice (der auf dem IBM Cognos -Anwendungsserver ausgeführt wird) kommuniziert mit Series 7 PowerPlay über das Series 7 PowerPlay Enterprise Server Gateway.

Wenn die Netzkonfiguration den Anwendungsserverzugriff auf den Web-Tier-Server verbietet, auf dem das Series 7 PowerPlay Enterprise Server-Gateway installiert ist, muss ein zweites internes Series 7 PowerPlay Enterprise Server-Gateway in der Anwendungsserverschicht installiert sein. In diesem Typ der Konfiguration können Sie die Position des Series 7 PowerPlay -Servers angeben.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Dienstleistungen** > **Berichtsdaten**.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im Menü **reportDataService Aktionen** auf **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Klicken Sie in der Spalte **Wert** für Gateway-Zuordnungen auf **Bearbeiten** .
6. Klicken Sie auf das Kontrollkästchen **Über den übergeordneten Eintrag erfasste Einstellungen außer Kraft setzen**.
7. Klicken Sie auf **Zuordnung hinzufügen**.
8. Geben Sie für **Application Gateway (extern)**die Adresse des Web-Servers ein.
9. Geben Sie für **Application Gateway (intern)**die Adresse des Series 7 PowerPlay -Servers ein.
10. Klicken Sie auf **OK**.

Dispatcher umbenennen

Als Sicherheitsmaßnahme können Sie Dispatcher umbenennen, wenn Sie den Hostnamen des Hosts, die Portnummer, das Servlet oder den Pfad des Dispatchers nicht anzeigen möchten.

Weitere Informationen finden Sie unter „Dispatcher sichern” auf Seite 54 .

In der Regel können Serveradministratoren den Namen der Dispatcher anzeigen und ändern.

Bei der Umbenennung eines Dispatchers wird empfohlen, keine Informationen zu verwenden, die den Hostnamen oder den Port des Hosts oder andere System-oder Pfadinformationen enthüllen. Es ist jedoch wichtig, sich daran zu erinnern, wo der Dispatcher installiert ist, und zwar zu Überwachungszwecken.

Tipp: Wenn Sie einen Dispatcher umbenennen und auf die Host-, Port-und Pfadinformationen zugreifen müssen, können Sie die Methoden des Software Development Kit verwenden, um diese Informationen in der Eigenschaft "dispatcherPath" des Dispatcherobjekts zu finden.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Alle Dispatcher**.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im Menü des Dispatchers **Aktionen** auf **Eigenschaften festlegen**.
4. Geben Sie in das Feld **Name** den neuen Namen des Dispatchers ein.

Verwenden Sie einen aussagekräftigen Namen, um die Dispatcher zu unterscheiden. Geben Sie keine Systeminformationen im Namen an.

5. Wenn Sie möchten, fügen Sie eine Bildschirmtipp-und Beschreibungsinformationen hinzu.
6. Klicken Sie auf **OK**.

Dispatcher testen

Um die Leistung von IBM Cognos -Software zu bewerten, können Sie den Status der Dispatcher testen.

Sie können auch sicherstellen, dass die Dispatcher antworten und die Betriebszeit anzeigen, d. h. die Zeit in Sekunden, in der die Dispatcher ohne Fehler arbeiten.

Sie können den Status von Dispatcher und Service und Protokollnachrichten prüfenanzeigen.

Vorbereitende Schritte

Beim Testen eines Dispatchers testen Sie auch die Services, die zu diesem Dispatcher gehören.

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf **IBM Cognos Administration** Kapitel 13, „Funktionen” , auf Seite 207verfügen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Bestimmen Sie die Dispatcher, die Sie testen möchten, und befolgen Sie die Anweisungen in dieser Tabelle. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf die Elemente, die angezeigt werden sollen.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.

   Tabelle 20. Ziele, Ansichten und Aktionen zum Testen von Dispatchern

Ziel	**Sicht 'Scorecard'**	**Aktion**
Alle Dispatcher im System testen	**Alle Server**	Klicken Sie im Menü "Gruppenaktionen" auf **Test**. **Tipp:** Wenn Sie eine Aktion nur auf einige Einträge anwenden möchten, wählen Sie Kontrollkästchen für mindestens einen Eintrag aus, und klicken Sie dann auf die gewünschte Aktion.
Alle Dispatcher für eine Servergruppe testen	**Alle Server**	Klicken Sie im Menü "Gruppenaktionen" auf **Testdispatcher**.
Alle Dispatcher für einen Server testen	**Alle Server**	Suchen Sie den Server, den Sie testen möchten. Klicken Sie im Menü "Serveraktionen" auf **Test**.
Testen eines bestimmten Dispatchers	**Alle Dispatcher**	Suchen Sie den Dispatcher, den Sie testen möchten. Klicken Sie im Menü "Dispatcheraktionen" auf **Test**.

   Daraufhin wird ein Dialogfenster angezeigt, in dem die Aktion bestätigt wird.
3. Klicken Sie auf **OK**.

Wenn die Dispatcher nicht so ausgeführt werden, wie sie sollten, können Sie die Serverleistung optimieren, indem Sie ihre Konfigurationseinstellungen ändern. Weitere Informationen finden Sie unter „Serverleistung optimieren“ auf Seite 63.

Failover für mehrere Dispatcher

In einer verteilten IBM Cognos -Softwareinstallation können Sie jede Ihrer Gateway-Komponenten so konfigurieren, dass sie mit mehr als einem Dispatcher für Failover-Zwecke kommunizieren.

Die Gateway-Komponenten scannen ihre zugeordneten Dispatcher, um sicherzustellen, dass Anforderungen an Dispatcher weitergeleitet werden, die im Service sind und ordnungsgemäß reagieren. Sie können die Häufigkeit festlegen, mit der diese Scans ausgeführt werden.

Informationen zum Konfigurieren mehrerer Dispatcher finden Sie im Artikel "Gateway-Computer konfigurieren" in der *IBM Cognos Analytics Installation und Konfiguration*.

Häufigkeit der Dispatcher-Statussuchen festlegen

Sie können angeben, wie oft Dispatcher gescannt werden, um ihren aktuellen Status für Failover-Zwecke zu bestimmen.

Verwenden Sie die folgenden Parameter:

- VerbindungCheckingSleepTime

  Gibt in Sekunden das Intervall zwischen den Scanvorgängen für den Status der Dispatcher an.

  Gültige Einstellungen sind 1 bis 2147483647. Einstellungen, die kleiner als 5 sind, können zu viele Ressourcen (CPU-Zeit und Netzbandbreite) verbrauchen. Die Standardeinstellung ist 30.

- VerbindungCheckingQuickSleepTime

  Gibt in Sekunden das Intervall zwischen den Scans an, wenn keine Betriebszuteiler gefunden werden. Dieser Wert für diesen Parameter muss kleiner als ConnectionCheckingSleepTime sein.

  Gültige Einstellungen sind 1 bis 2147483647. Einstellungen, die kleiner als 5 sind, können zu viele Ressourcen (CPU-Zeit und Netzbandbreite) verbrauchen. Die Standardeinstellung ist 5.

Vorgehensweise

1. Kopieren Sie die Beispieldatei *Installationsposition*/cgi-bin/cognoscgi.conf. in das Verzeichnis " *Installationsposition*/bin" und benennen Sie sie in "cognoscgi.conf." um.
2. Öffnen Sie die Datei 'cognoscgi.conf' in einem Editor, der Dateien im UTF-8-Format speichern kann.
3. Fügen Sie der Datei die folgenden Zeilen hinzu:

   ```
   ConnectionCheckingSleepTime=time in seconds
   ```

   ```
   ConnectionCheckingQuickSleepTime=time in seconds
   ```

4. Speichern Sie die Datei 'cognoscgi.conf' im UTF-8-Format.

Dispatcher sichern

Sie können den Standarddispatchernamen ändern, um Sicherheitsrisiken zu vermeiden.

Benutzer der IBM Cognos -Software können XPath-Suchpfade im Adressfeld eines Web-Browsers oder in Hyperlinks eingeben. Die Benutzer können eine beliebige Suchpfadsyntax für Suchpfadparameter in der Benutzerschnittstelle eingeben. IBM Cognos software relies on the Content Manager Access Control List (ACL) to check the objects that are returned to the user.

In einigen Fällen konnten heimtückische Benutzer den Namen des Dispatchers sehen. Dies kann ein Sicherheitsrisiko darstellen, auch wenn die Benutzer nicht auf den Namen des Dispatchers klicken können oder keine Aktionen darauf ausführen.

Um diese Art des Sicherheitsrisikos zu vermeiden, ändern Sie den Standarddispatchernamen. Der Standarddispatcher-Name ist *Computername*: 9300. Er kann beispielsweise in *server1* geändert werden, um die Portnummer und den Hostnamen zu maskieren. Weitere Informationen finden Sie unter „Dispatcher umbenennen" auf Seite 52 .

Dispatcher für den Host des JMX-Proxy-Servers angeben

Administratoren können eine Liste mit einem oder mehreren Dispatchern als Kandidaten erstellen, um den JMX-Proxy-Server (Java Management Extensions) zu hosten. Dies hilft, die Anzahl der Threads zu reduzieren, die zum Erfassen von JMX-Metriken erforderlich sind, und erhöht die Anzahl der Threads, die für Content Manager verfügbar sind.

Der JMX-Proxy-Server kommuniziert mit Dispatchern und erfasst deren JMX-Metriken. Für diese Kommunikation sind etwa vier Threads pro Dispatcher erforderlich. Eine verteilte Installation mit einer großen Anzahl von Dispatchern erfordert einen großen Thread-Datenträger, der die Leistung des Content-Managers beeinflusst. Um dieses Problem zu beheben und die Leistung von Content Manager zu verbessern, können Administratoren einen oder mehrere Dispatcher als Kandidaten für den Host des JMX-Proxy-Servers (Java Management Extensions) auswählen.

Dispatcher auswählen

Da IBM Cognos Administration den Präsentationsservice verwendet und über eine Verbindung zum Proxy-Server verfügt, wählen Sie Dispatcher aus, die den Präsentationsservice ausführen. Dadurch werden lokale Aufrufe an den Proxy-Server bereitgestellt.

Verwenden Sie IBM Cognos Administration, um eine Liste mit mindestens einem Dispatcher für den Host des JMX-Proxy-Servers (Java Management Extensions) zu erstellen. Der Dispatcher, der sich am Anfang der Liste befindet und derzeit ausgeführt wird, ist der Dispatcher, der für den Host des JMX-Proxy-Service ausgewählt wird.

Wenn keiner der Dispatcher in der bevorzugten Liste aktiv ist, wird jeder beliebige verfügbare Dispatcher für den Host des JMX-Proxy-Servers ausgewählt. Beachten Sie, dass dies das Standardverhalten ist, wenn Sie keine Liste von Dispatchern erstellen.

JMX-Host-Dispatcher bearbeiten

Verwenden Sie IBM Cognos Administration, um einen oder mehrere Dispatcher zu der Liste der Dispatcher-Kandidaten hinzuzufügen, die der Host für den JMX-Proxy-Server (Java Management Extensions) sein können.

Vorgehensweise

1. Starten Sie IBM Cognos Administration.
2. Klicken Sie auf der Registerkarte **Status** auf **System**.
3. Klicken Sie im Teilfenster **Scorecard** für den Eintrag **System** auf den Menüpfeil 'Aktionen', und klicken Sie auf **Eigenschaften festlegen**.
4. Klicken Sie auf der **Eigenschaften festlegen-Konfiguration** -Seite auf die Registerkarte **Einstellungen** .
5. Klicken Sie auf **Bearbeiten** , um die **JMX-Proxy-Host-Dispatcher**festzulegen.

   Die Seite **Konfiguration des JMX-Proxy-Host-Dispatchers festlegen** wird angezeigt.
6. Klicken Sie auf **Hinzufügen** , um einen Dispatcher hinzuzufügen.
7. Wählen Sie die Disponenten aus, die Sie hinzufügen möchten.
8. Klicken Sie auf die Schaltfläche mit der Rechtspfeiltaste, und klicken Sie auf **OK**, wenn die gewünschten Einträge im Feld **Ausgewählte Einträge** angezeigt werden.
9. Klicken Sie auf **OK**.
10. Klicken Sie auf **Nach oben**, **Nach unten**, **Nach oben**oder **Nach unten** , um die Dispatcher zu bestellen.

11. Klicken Sie auf **OK**.

Ergebnisse

Der Dispatcher, der sich am Anfang der Liste befindet und derzeit ausgeführt wird, ist der Dispatcher, der für die Ausführung des JMX-Proxy-Service ausgewählt wird. Sie können die Reihenfolge der Disponenten jederzeit ändern. Wenn keiner der Dispatcher in dieser Liste ausgeführt wird, wird jeder beliebige verfügbare Dispatcher für den Host des JMX-Proxy-Servers ausgewählt.

Content Manager-Positionen

Ihre Installation kann mehr als einen Content Manager enthalten, jeder an einer anderen Position. Ein Content Manager-Computer ist aktiv und eine oder mehrere Content Manager-Komponenten befinden sich im Standby-Modus.

Stellen Sie sicher, dass die Uhren auf jedem Computer, auf dem Content Manager installiert ist, synchronisiert sind. Wenn dies nicht der Fall ist, kann es zu einem ungeraden Verhalten kommen, wenn ein Failover auftritt. Es kann beispielsweise eine Verzögerung geben, bevor der Status eines neu inaktivierten Servers in der IBM Cognos Administration aktualisiert wird. Weitere Informationen zu Content Manager finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Weitere Informationen zum Festlegen von Content Manager-Parametern finden Sie im Artikel „Erweiterte Content Manager-Parameter festlegen” auf Seite 56.

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität Kapitel 13, „Funktionen”, auf Seite 207verfügen.

Erweiterte Content Manager-Parameter festlegen

Sie können erweiterte Content Manager-Parameter festlegen.

Zu den erweiterten Content Manager-Parametern gehören Einstellungen für den Datenbankverbindungspool, sortierte Einträge für nicht-englische Ländereinstellungen, Synchronisation und Browsing von externen Namespaces.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Dienstleistungen** > **Content Manager**.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im Menü **ContentManagerService Aktionen** auf **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Klicken Sie neben **Erweiterte Einstellungen**auf **Bearbeiten** .
6. Wählen Sie **Über den übergeordneten Eintrag erfasste Einstellungen außer Kraft setzen**aus.
7. Geben Sie in der Spalte **Parameter** den Parameternamen ein.

   Geben Sie beispielsweise `CM.DbConnectPoolCleanUpPeriod`ein.
8. Geben Sie in der Spalte **Wert** den zugeordneten Wert für die Einstellung ein.
9. Setzen Sie die Eingabe von Namen und Werten nach Bedarf fort.
10. Klicken Sie auf **OK**.
11. Klicken Sie auf der **Eigenschaften festlegen** -Seite auf **OK**.

Einstellungen für Datenbankverbindungspools für Content Manager verwalten

Content Manager verwendet Datenbankverbindungen, um auf den Content Store zuzugreifen. Sie können die Verbindungspooleinstellungen für Content Manager ändern, um die Leistung zu erhöhen.

Bei gepoolten Verbindungen muss Content Manager keine Verbindungen für neue Anforderungen erstellen und öffnen. Dies ermöglicht schnellere Antwortzeiten. Die gepoolten Verbindungen reservieren jedoch Datenbankressourcen, so dass inaktive Verbindungen geschlossen werden sollten, wenn sie nicht benötigt werden.

Sie können die Anzahl der Verbindungen zum Content-Store verwalten, indem Sie die maximale Anzahl von Verbindungen begrenzen und angeben, wie lange Verbindungen im Pool verbleiben, bevor sie automatisch geschlossen werden.

Die folgenden Parameter sind verfügbar:

- **CM.DbConnectPoolMax**

  Gibt die maximale Anzahl gleichzeitiger Datenbankverbindungen an, die der Content Store zulässt.

  Dieser Parameter gilt nur für die Einstellungen des Content Manager-Verbindungspools. Wenn Sie über andere Services verfügen, die auf denselben Content-Store zugreifen, kann es zu mehr gleichzeitigen Datenbankverbindungen kommen, als in diesem Parameter angegeben wurden.

  Gültige Einstellungen sind -1, oder 5 bis 2147483647, oder die Datenbankeinstellung, je nachdem, welcher Wert kleiner ist. Der Standardwert ist -1 (unbegrenzt).

- **CM.DbConnectPoolTimeout**

  Gibt die maximale Zeitdauer in Millisekunden an, die ein Thread wartet, bis eine Verbindung aus dem Pool verfügbar ist.

  Die gültigen Einstellungen sind -1 bis 2147483627. Eine Einstellung von 0 gibt an, dass Threads nie auf eine Verbindung warten, wenn eine Verbindung nicht sofort verfügbar ist. Der Standardwert ist -1 (unbegrenzt).

- **CM.DbConnectPoolIdleTime**

  Gibt in Millisekunden die Mindestlänge an, die eine Verbindung im Pool inaktiv bleibt. Dieser Parameter wird nur verwendet, wenn der Wert für die Einstellung DbConnectPoolCleanUpPeriod positiv ist.

  Die gültigen Einstellungen sind -1 bis 2147483647. Eine Einstellung von 0 oder -1 gibt an, dass inaktive Verbindungen beim Neustart von Content Manager geschlossen werden. Der Standardwert ist 300000 (5 Min.).

- **CM.DbConnectPoolCleanUp-Zeitraum**

  Gibt in Millisekunden an, wie lange zwischen Aufrufen eines Bereinigungsthreads, der inaktive Verbindungen im Pool schließt, die die Einstellung von DbConnectPoolIdleTime überschreiten, die Zeitdauer angegeben wird.

  Die gültigen Einstellungen sind -1 bis 2147483647. Der Standardwert ist 300000 (5 Min.).

Sortieren von Einträgen für "Non-English Locales"

Sie können Sortierprobleme in anderen Ländereinstellungen als Englisch für einen Oracle-oder Microsoft SQL-Content-Store korrigieren.

Um ein Sortierproblem zu korrigieren, verwenden Sie den Parameter CM.SortCollation. Wenn Sie beispielsweise Einträge in einer Oracle-Datenbank mithilfe einer chinesischen phonetischen Sortierfolge sortieren möchten, setzen Sie den Parameter CM.SortCollation auf SCHINESE_PINYIN_M.

Informationen zu unterstützten Sortierfolgen finden Sie in der Oracle-und SQL Server-Dokumentation. Die Einstellung des Werts für CM.SortCollation hat keine Auswirkung auf Content Manager, der mit IBM Db2 -oder Sybase-Datenbanken ausgeführt wird.

Content Manager-Synchronisation verwalten

Wenn Ihre Installation Bereitschafts-Content-Manager-Computer enthält, können Sie Parameter festlegen, die Content Manager-Standby-Aktivitäten angeben.

Sie können angeben, wie oft Prüfungen auftreten, um sicherzustellen, dass der aktive Dispatcher nicht ausgefallen ist, wie lange es dauert, bis bestimmt wird, welcher Content Manager beim Failover und beim Start aktiv ist, wie oft ein aktiver Content Manager eine Antwort sendet, wenn er ausgelastet ist, und wie lange eine kurze Netzunterbrechung sein kann, ohne dass ein Failover verursacht wird.

Die folgenden Parameter sind verfügbar:

- **CM.CMSync_NegotiationTime**

  Gibt die Zeitdauer in Millisekunden an, die erforderlich ist, um den aktiven Content Manager zu bestimmen, wenn ein Failover stattfindet.

  Die gültigen Einstellungen sind 1 bis 9223372036854775807. Der Standardwert ist 2000.

- **CM.CMSync_NegotiationTimeForStartUp**

  Gibt in Millisekunden an, wie lange es dauert, bis der aktive Content Manager beim Start bestimmt wird.

  Die gültigen Einstellungen sind 1 bis 9223372036854775807. Der Standardwert ist 60000.

- **CM.CMSync_CheckActive Time**

  Gibt in Millisekunden an, wie lange es dauert, bis ein aktiver Content Manager in den Standby-Modus versetzt wird, wenn ein anderer Content Manager aktiv wird.

  Der Standardwert ist 10000.

- **CM.CMSync_PingTimeout**

  Gibt die Zeitdauer in Millisekunden an, die für einen ausgelasteten Content Manager erforderlich ist, um eine Antwort zu senden, wenn diese aktiv ist.

  Die gültigen Einstellungen sind 1 bis 9223372036854775807. Der Standardwert ist 120000.

- **CM.CMSync_ShortNetworkInterruptionTime**

  Gibt in Millisekunden an, wie lange eine kurze Netzunterbrechung auftreten kann, ohne dass ein Failover verursacht wird.

  Die gültigen Einstellungen sind 1 bis 9223372036854775807. Der Standardwert ist 3000.

Steuern des Browsens von externen Namensbereichen

Sie können steuern, ob Benutzer externe Namespaces durchsuchen können.

Wenn die Einstellung "CM.SecurityQueryRequiresRead" auf "true" gesetzt ist, verhindert Content Manager das Durchsuchen externer Namespaces, wenn die Richtlinie für externe Namespaces aktualisiert wird, um Leseberechtigungen für Benutzer oder Gruppen zu verweigern. Diese Einstellung steuert, ob der Content Manager einen Leseberechtigungsfilter für die Abfrageergebnisse für externe Namespaces erzwingt. Der Standardwert ist 'false'.

Grenzwert für die Cachegröße für den Content Manager-Cache festlegen

Sie können den oberen Grenzwert für die Cachegröße als Prozentsatz der Größe des JVM-Heapspeichers angeben.

Der Standardwert ist 10%. Gültige Werte sind 0 bis 100. Durch die Vergrößerung der Cachegröße kann der Content Manager die Last reduzieren, sodass er mehr verteilte Knoten bedienen kann. Wenn Sie diesen Wert jedoch zu hoch setzen, können Fehler aufgrund von Speicherausgriffen im Dispatcher auftreten.

Wenn Sie den Wert auf 0 (null) setzen, wird der Cache systemweit inaktiviert, indem alle Abfrageanforderungen direkt an den Content Manager gesendet werden, wodurch die Systemleistung

beeinträchtigt werden kann. Dies ist jedoch nützlich, um die Leistung mit und ohne den Cache zu vergleichen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Dienstleistungen** > **Content Manager-Cache**.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im Menü **ContentManagerCacheService Aktionen** auf **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Ändern Sie in der Spalte **Wert** die Nummer für **Heapspeichergrenzwert für den Content Manager-Cache-Service**.
6. Geben Sie die gewünschte Einstellung ein, und klicken Sie auf **OK**.

Content Manager-Ladevorgang reduzieren, indem Benutzersitzungsdateien lokal gespeichert werden

Sie können die Position ändern, an der Benutzersitzungsdateien gespeichert werden.

Wenn ein Benutzer einen interaktiven Bericht ausführt, sendet der Berichtsserver eine Anforderung an den Content Manager, in der er aufgefordert wird, die Berichtsausgabe im Sitzungscache für den Benutzer zu speichern. Eine solche Berichtsausgabe kann in einem der folgenden Formate enthalten sein: PDF, HTML mit Bildern, Microsoft Excel-speadsheet-Software, CSV oder XML.

Um die Verarbeitungslast für den Content Manager zu reduzieren, werden Benutzersitzungsdateien auf dem lokalen Dateisystem des Berichtsservers gespeichert. Diese Position befindet sich standardmäßig auf dem Berichtsserver. Sie können die Position auf einen fernen Computer ändern, z. B. ein gemeinsam genutztes Verzeichnis auf dem Betriebssystem Microsoft Fenster oder ein gemeinsam genutztes Verzeichnis auf dem Betriebssystem UNIX . Weitere Informationen finden Sie im Artikel zum Ändern der Position der temporären Berichtsausgabe in der *IBM Cognos Analytics Installation und Konfiguration*.

Wenn Sie ein Upgrade durchführen, werden Benutzersitzungsdateien in Content Manager gespeichert. Sie müssen das lokale Dateisystem des Berichtsservers ändern, wenn Sie den Content Manager-Ladevorgang reduzieren möchten.

Das Speichern temporärer Dateien kann zu einer erhöhten Plattenbelegung führen. Stellen Sie sicher, dass genügend Speicherplatz für die Dateien zugeordnet ist.

Dies beeinträchtigt nicht die älteren Versionen von Anwendungen, wie z. B. Software Development Kit, die noch Anforderungen an den Content Manager senden.

Die folgenden Parameter sind verfügbar:

- **Position der temporären Objekte**

  Gibt die Position der temporären Cachedateien an. Wenn Sie die temporären Cachedateien auf dem Berichtsserver speichern möchten, wählen Sie **ServerFileSystem**aus. Wählen Sie **ContentStore**aus, um die temporären Cachedateien auf dem Content Manager zu speichern.

  Der Standardwert ist **ServerFileSystem**.

- **Lebensdauer der temporären Objekte**

  Gibt in Stunden an, wie lange temporäre Cachedateien aufbewahrt werden. Wenn Sie diesen Wert auf null setzen, werden die Dateien so lange aufbewahrt, bis sie manuell gelöscht werden.

  Diese Einstellung wird nur vom Dispatcher verwendet. Der Berichtsserver löscht temporäre Cachedateien, wenn der Browser geschlossen wird oder wenn der Benutzer auf die Schaltfläche

'Zurück' im Browser klickt. Wenn der Berichtsserver die Dateien nicht löscht, verwendet der Dispatcher diese Einstellung, um die Dateien zu löschen.

Der Standardwert ist 4 Stunden.

Es gibt auch eine Einstellung in Cognos -Konfiguration zum Verschlüsseln von temporären Dateien, die nicht von den **Lebensdauer der temporären Objekte** -oder **Position der temporären Objekte** -Einstellungen betroffen sind. Weitere Informationen finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Dispatcher und Services**.
2. Klicken Sie auf die **Eigenschaften festlegen-Konfiguration** -Schaltfläche  und anschließend auf **Einstellungen**.
3. Klicken Sie im Menü **Kategorie** auf **Optimierung**.
4. Ändern Sie die Einstellungen für **Position der temporären Objekte** und **Lebensdauer der temporären Objekte**nach Bedarf.
5. Klicken Sie auf **OK**.

Standardländereinstellungsverarbeitung im Eingabeaufforderungscache überschreiben

Sie können die Ländereinstellung für die Ländereinstellung im Eingabeaufforderungscache für alle Berichte überschreiben.

Dies kann mit Hilfe der erweiterten Einstellung RSVP.PROMPTCACHE.LOCALE erfolgen. Wenn diese Einstellung konfiguriert ist, wird die angegebene Ländereinstellung anstelle der im Bericht angegebenen Ländereinstellung verwendet, wenn Eingabeaufforderungscachedaten erstellt, aktualisiert oder verwendet werden. Dies bedeutet, dass für jeden Bericht unabhängig von der Ländereinstellung des Berichtsbenutzers ein einzelner Eingabeaufforderungscache verwendet wird.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Services konfigurieren” auf Seite 519aus.
2. Geben Sie für den **ReportService**in der Spalte **Parameter** den Wert **RSVP.PROMPTCACHE.LOCALE**ein.
3. Geben Sie in der Spalte **Wert** den zugehörigen Wert für den Parameter ein, und klicken Sie auf **OK**.

Wartungstasks für Content-Store

Sie können Inhaltserwartungstasks erstellen und diese auf Anforderung zu einem geplanten Zeitpunkt oder auf der Basis eines Triggers ausführen.

Zum Beispiel eine Datenbankaktualisierung oder eine E-Mail. Sie können Wartungstasks für Inhalte als Teil eines Jobs oder als Teil eines Agenten planen. Sie können auch das Ausführungsprotokoll für die Inhaltserwartungs-Tasks anzeigen.

Sie können Inkonsistenzen innerhalb des Content-Stores oder zwischen dem Content-Store und externen Namespaces finden und beheben.

Inhalte-Verwaltungstasks können aufgrund fehlender Daten oder veralteter Daten oder zwischen dem Content-Store und externen Namespaces auf Inkonsistenzen innerhalb des Content-Stores hin überprüfen.

Bei Bedarf können Sie auch Hintergrundtasks starten und stoppen , die im Content-Store ausgeführt werden, verwenden.

Informationen zur Verwendung von Content-Store-Verwaltungstasks in einer Multi-Tenant-Umgebung finden Sie unter „Konsistenzprüfung für Content Store erstellen und ausführen" auf Seite 357.

Vor dem Starten der internen Content-Store-Wartung

Um sicherzustellen, dass keine Daten verloren gehen, die Sie beibehalten möchten, sollten Sie zuerst den Suchmodus auswählen und die Ergebnisse überprüfen, bevor Sie den Content-Store festlegen.

Fehlende Daten im Content Store können dazu führen, dass Aktualisierungen fehlschlagen. Veraltete Daten verhindern möglicherweise, dass Sie neue Objekte erstellen. Wenn eine Wartungstask für den Content-Store den Content-Store festlegt, fügt er Standardwerte für die fehlenden Daten hinzu, die Sie später aktualisieren können. Außerdem werden alle veralteten Daten dauerhaft gelöscht.

Wenn Sie die Daten suchen und korrigieren, wird der Content Store nicht behoben, während die Content-Maintenance-Task ausgeführt wird. Stattdessen behebt Content Manager die Inkonsistenzen im Content-Store, wenn das nächste Mal gestartet wird.

Wichtig: Nachdem Sie eine Task zur Inhaltsverwaltung ausgeführt haben, um den Content-Store zu suchen und zu beheben, sichern Sie Ihren Content-Store, bevor Sie Content Manager erneut starten.

Wir empfehlen, dass Sie interne Wartungsprüfungen regelmäßig durchführen, aber es ist besonders wichtig, dies zu tun, bevor Sie ein Upgrade durchführen, um die Konsistenz der Content-Stores zu gewährleisten.

Content Store Maintenance on External Namespaces

Sie können die Verwaltung von IBM Cognos für die Verwaltung von Content-Stores für externe Namespaces verwenden.

Wenn Sie Benutzer in Ihrem Authentifizierungsprovider löschen, verbleiben die Benutzeraccountinformationen im Content-Store. Sie können die IBM Cognos Administration verwenden, um Benutzerinformationen zu suchen, die noch im Content Store vorhanden sind, und den Content Store zu korrigieren, indem Sie alle Benutzer löschen, die in Ihren externen Namespaces nicht vorhanden sind. Sie können auch einzelne Benutzerprofile aus den Content-Stores löschen.

Führen Sie einen der folgenden Schritte aus, wenn Sie eine Task zur Verwaltung von Inhalten für mehr als einen Namensbereich ausführen möchten:

- Wenn Sie die Task für die Inhaltsverwaltung jetzt ausführen möchten, melden Sie sich einfach bei den Namespaces an und erstellen Sie die Task zum Erstellen von Inhalten.
- Wenn Sie eine Wartungstask für Inhalte planen möchten, die in der Zukunft oder auf einer wiederkehrenden Basis ausgeführt werden soll, müssen Sie beachten, dass eine geplante Task zur Verwaltung von Inhalten mit den Namespaces ausgeführt wird, die Sie bei der Erstellung der Content-Maintenance-Task ausgewählt haben. Bevor Sie eine Task zur Verwaltung von Inhalten terminieren, müssen Sie sicherstellen, dass Ihre Berechtigungsnachweise Anmeldedaten für jeden Namensbereich enthalten, indem Sie die Berechtigungsnachweise erneuern, nachdem Sie sich an jedem Namespace angemeldet haben, für den Sie die Task zum Ausführen der Inhaltserwartungen ausführen.

  Tipp: Click **Meine Area-Optionen**, **Eigene Vorgaben**, click the **Personal** tab, and then click **Berechtigungsnachweise erneuern**.

Sie müssen über Zugriffsberechtigungen für jeden ausgewählten externen Namespace und Leseberechtigungen für alle Benutzerkonten in jedem externen Namespace verfügen. Wenn Sie keine Leseberechtigungen für ein Benutzerkonto haben, wird davon ausgegangen, dass der Benutzer aus dem Namespace gelöscht wurde. Wenn Sie einen Job für die Inhaltsverwaltung ausführen, werden die Benutzerinformationen im Content-Store entweder als inkonsistent aufgelistet (für **Nur suchen** oder automatisch gelöscht (für **Suchen und beheben**).

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf **IBM Cognos Administration**verfügen. Weitere Informationen hierzu finden Sie im Artikel Kapitel 13, „Funktionen", auf Seite 207.

Wartungstask für Content Store erstellen

Sie können eine Wartungstask für den Content Store erstellen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
2. Klicken Sie in der Symbolleiste auf den Pfeil auf der neuen Schaltfläche für die Inhaltsverwaltung  und klicken Sie dann auf **Neue Konsistenzprüfung**.
3. Geben Sie einen Namen und, wenn Sie möchten, eine Beschreibung und einen Anzeigentipp ein, und klicken Sie auf **Weiter**.
4. Wählen Sie die Konsistenzprüfung aus, die Sie wünschen:
   - Um den Content-Store auf Inkonsistenzen zu überprüfen, klicken Sie auf **Interne Referenzen**.
   - Klicken Sie auf **Verweise auf externe Namespaces** und wählen Sie die gewünschten Namespaces aus, um die Inhaltsverwaltung für Namespaces auszuführen.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie die Aktion aus, die Sie ausführen möchten:
   - Wenn Sie die Task jetzt oder später ausführen möchten, klicken Sie auf **Speichern und einmal ausführen** und dann auf **Fertigstellen**. Geben Sie eine Uhrzeit und ein Datum für die Ausführung an. Klicken Sie auf **Nur suchen** oder **Suchen und beheben**, und klicken Sie dann auf **Ausführen**. Überprüfen Sie die Laufzeit und klicken Sie auf **OK**.
   - Wenn Sie die Task zu einem wiederkehrenden Zeitpunkt planen möchten, klicken Sie auf **Speichern und planen** und dann auf **Fertigstellen**. Wählen Sie dann Frequenz und Start-und Enddatum aus. Klicken Sie auf **Nur suchen** oder **Suchen und beheben** und anschließend auf **OK**.

     Tipp: Wenn Sie den Zeitplan vorübergehend inaktivieren möchten, wählen Sie das Kontrollkästchen **Zeitplan inaktivieren** aus.
   - Klicken Sie auf **Nur speichern** , und klicken Sie auf **Fertigstellen**, um die Task ohne Planung oder Ausführung zu speichern.

Führen Sie eine Content Store-Wartungstask aus

Sie können eine Wartungstask für den Content Store ausführen.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
2. Klicken Sie auf **Mit Optionen ausführen** neben der Task für die Inhaltsverwaltung.
3. Wählen Sie das Markierungsfeld **Jetzt** aus, um die Inhaltsverwaltungsaufgabe sofort auszuführen, oder wählen Sie das Kontrollkästchen **Später** aus, um einen Tag und eine Uhrzeit festzulegen.
4. Klicken Sie auf **Suchen** oder **Suchen und beheben**.
5. Klicken Sie auf **Ausführen**.

Hintergrundaktivitäten starten und stoppen

Sie können Hintergrundaktivitäten starten und stoppen, die in Content Manager ausgeführt werden.

Informationen zu diesem Vorgang

Durch das Stoppen von Hintergrundaktivitäten wird die Verarbeitungslast für Content Manager verringert, wodurch die Leistung erhöht werden kann. Sie können Hintergrundaktivitäten starten, nachdem Content Manager den Job beendet hat, der eine höhere Ressourcenmenge erforderte.

Vorgehensweise

1. Starten Sie IBM Cognos Administration.
2. Klicken Sie auf der Registerkarte **Status** auf **System**.
3. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Dienstleistungen** > **Content Manager**.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
4. Klicken Sie auf den Pfeil, um das Menü "Aktionen" neben dem Content Manager-Service anzuzeigen, und klicken Sie anschließend auf **Hintergrundaktivitäten starten** oder **Hintergrundaktivitäten stoppen**.

Serverleistung optimieren

Sie sollten die Leistungsoptimierung als regulärer Teil der Verwaltungsserver einschließen.

Durch die Optimierung der Konfigurationseinstellungen von Dispatchern und Services können Sie die Geschwindigkeit und die Effizienz von IBM Cognos -Software optimieren. Für Benutzer bedeutet eine optimale Leistung, dass ihre Berichte schnell und fehlerfrei laufen. Für Sie bedeutet dies, dass IBM Cognos -Software stabil ist und dass die Benutzer glücklich sind.

Im Idealfall möchten Sie die Server so optimieren, dass sie die Benutzeranforderung zu den Zeiten für die maximale Nutzung erfüllen.

Möglicherweise müssen Sie die Dispatcher zu Ihrer Installation hinzufügen, um die Anforderungen der Benutzer zu erfüllen. Sie müssen möglicherweise Ihre Installation verteilen oder den Computer aktualisieren, auf dem die IBM Cognos -Software installiert ist. Weitere Informationen finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Die Stufe der Protokollierung „Protokollierungsstufen festlegen“ auf Seite 18 kann die Leistung beeinträchtigen. Wenn die Softwareprotokolle von IBM Cognos ausführlicher protokolliert werden, werden mehr Ressourcen für die Protokollierung zugeordnet, und es stehen dann weniger Ressourcen für die Ausführung von Berichten zur Verfügung.

Bevor Sie Einstellungen ändern, müssen Sie sicherstellen, dass Sie die Dispatcher getestet und die zugehörigen Protokollnachrichten „Protokollnachrichten“ auf Seite 16geprüft haben. Weitere Informationen zum Testen von Dispatchern finden Sie unter „Dispatcher testen“ auf Seite 53. Sie sollten auch Ihre Leistungsanforderungen verstehen.

Modelle

Stellen Sie sicher, dass Ihre Modelle für die Berichterstellung optimiert sind. Weitere Informationen finden Sie im *IBM Cognos Framework Manager-Benutzerhandbuch*.

Betriebssysteme

How IBM Cognos software performs is tightly related to the performance of the operating system of the computer where IBM Cognos software is installed. Stellen Sie daher sicher, dass Ihr Betriebssystem optimiert ist.

Servergruppen für das erweiterte Dispatcherrouting erstellen

Wenn Sie Routing-Regeln für Berichte definieren möchten, müssen Sie Servergruppen für die Dispatcher- oder Konfigurationsordner erstellen, an die Berichte weitergeleitet werden sollen.

Informationen zum Definieren von Routing-Regeln finden Sie im Artikel „Dispatcher-Routing“ auf Seite 49.

Tipp: Wenn Sie das erweiterte Dispatcher-Routing einrichten und PowerPlay verwenden, müssen Sie sicherstellen, dass die Servergruppe mindestens einen PowerPlay-Server zum Verarbeiten von PowerPlay-Anforderungen enthält.

Informationen zu diesem Vorgang

Sie können

Vorgehensweise

1. Öffnen Sie **IBM Cognos Administration**von **Verwalten** > **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Status** auf **System**.
3. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Alle Dispatcher**.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
4. Klicken Sie im Menü **Aktionen** des Dispatchers auf **Eigenschaften festlegen**.
5. Klicken Sie auf die Registerkarte **Einstellungen** .
6. Wählen Sie **Optimierung** in der Liste **Kategorie** aus.
7. Geben Sie einen Namen in die Spalte **Wert** für die Eigenschaft **Servergruppe** ein.

   Wichtig: Der Name darf maximal 40 Zeichen enthalten.
8. Klicken Sie auf **OK**.

   Sie verwenden diese Servergruppe, wenn Sie Routing-Regeln definieren, wie im Thema *Routing-Regeln für Dispatcher festlegen*im Thema ../com.ibm.swg.ba.cognos.ag_manage.doc/t_set_routing_rules.htmldokumentiert.

Anforderungen zwischen den Dispatchern verteilen

Wenn Ihre Installation mehr als einen Dispatcher enthält, können Sie den Anteil der Anforderungen angeben, die jeder Dispatcher verarbeitet, indem Sie die Verarbeitungskapazität ändern.

Dies wird allgemein als Lastausgleich bezeichnet. In der Regel legen Sie die Kapazität eines Dispatchers auf der Basis der CPU-Geschwindigkeit des Computers fest, auf dem er installiert ist.

Beispielsweise wird ein erster Dispatcher auf einem 2-GHz-Computer und ein zweiter Dispatcher auf einem 1-GHz-Computer installiert. Sie legen die Verarbeitungskapazität des ersten Dispatchers auf 2,0 und die zweite auf 1.0 fest. Der erste Dispatcher verarbeitet zwei Drittel der Anforderungen, während der zweite für ein Drittel der Anforderungen zuständig ist. Wenn Sie die Kapazität der beiden Dispatcher auf 1.0 setzen, werden die Anforderungen abwechselnd an jeden Dispatcher gesendet.

Die Standardverarbeitungskapazität für jeden Dispatcher ist 1.0.

Affinitätseinstellungen haben Vorrang vor den Einstellungen für die Kontoanfrage. Weitere Informationen finden Sie unter „Maximale Anzahl Prozesse und Verbindungen“ auf Seite 68.

Sie können den Lastausgleichs für den Dispatcher auch steuern, indem Sie den Anforderungsfaktor in Bearbeitung festlegen. Siehe „Lastausgleich des Dispatchers mit In-Progress-Anforderungsfaktor“ auf Seite 65. Sie können auch das gewichtete Round-Robin-Format des Lastausgleichs für den Dispatcher inaktivieren. Siehe „Eigenschaft zum Lastausgleich des Dispatchers auf den Cluster-kompatiblen Modus setzen“ auf Seite 66.

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Siehe Kapitel 13, „Funktionen“, auf Seite 207.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie auf den Pfeil für das Menü "Aktionen" neben **System** , und klicken Sie auf **Eigenschaften festlegen**.
3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Wählen Sie **Optimierung** in der Liste **Kategorie** aus.
5. Geben Sie in der Spalte **Wert** einen neuen Wert für die **Verarbeitungskapazität**ein, und klicken Sie anschließend auf **OK**.

   Der neue Wert wird sofort wirksam.

Lastausgleich des Dispatchers mit In-Progress-Anforderungsfaktor

Sie können den Anforderungsfaktor "in-progress" so festlegen, dass ein Feedback zum Umlaufalgorithmus bereitgestellt wird, in dem angegeben wird, wie gut jeder Dispatcher gerade arbeitet.

Das gewichtete Round-Robin-Format des Lastausgleichs behandelt alle Anforderungen als gleich, und alle Dispatcher können die Anzahl der Anforderungen, die sie empfangen, genauso handhaben wie sie verarbeiten können. Unterschiedliche Anforderungen erfordern jedoch mehr oder weniger Verarbeitungsleistung. Die Dispatcher werden auch auf verschiedenen Servern ausgeführt, wobei unterschiedliche Verarbeitungsfunktionen zur Verfügung stehen. Wenn beispielsweise ein Dispatcher zurückbleibt, weil er auf einem langsameren Server ausgeführt wird oder weil er eine Menge Anforderungen erhält, die eine Menge Verarbeitungsleistung erfordern, behandelt das Round-Robin-Format alle Dispatcher-Disponenten immer noch. Dispatcher, die zurückfallen, verfügen über eine höhere Anzahl an Verarbeitungsanforderungen in der Warteschlange. Der Round-Robin-Algorithmus kann diese Informationen verwenden, um zu vermeiden, dass neue Anforderungen an diese Dispatcher gesendet werden, bis sie nicht mehr überlastet sind.

Die erweiterte Einstellung "inProgressRequestFactor" steuert, wie viel Feedback an den Umlaufalgorithmus "round robin" gesendet wird. Je größer der Wert ist, desto geringer ist die Wahrscheinlichkeit, dass ein Knoten mit mehr in Bearbeitung befindlichen Anforderungen verwendet wird. Unsere Forschung zeigt, dass die ideale Menge an Feedback ist der Standardwert von 2.0. Um ein einfaches Round-Robin-Format zu verwenden, müssen Sie es auf Systemebene auf 0.0 setzen.

Sie können den Wert auf Systemebene oder auf Serviceebene festlegen. Die Einstellung auf Systemebene wird als Standard für alle Services verwendet. Die Serviceeinstellungen haben Vorrang vor der Einstellung auf Systemebene.

Sie können den Lastausgleich für den Dispatcher auch steuern, indem Sie die Kapazitätsverarbeitung festlegen. Siehe „Anforderungen zwischen den Dispatchern verteilen” auf Seite 64. Sie können auch das gewichtete Round-Robin-Format des Lastausgleichs für den Dispatcher inaktivieren. Siehe „Eigenschaft zum Lastausgleich des Dispatchers auf den Cluster-kompatiblen Modus setzen” auf Seite 66. Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Siehe Kapitel 13, „Funktionen”, auf Seite 207.

Definieren der Eigenschaft 'In Bearbeitung befindliche Anforderungsfaktor' systemweit

Sie können die Anforderungsfaktoreigenschaft "In Bearbeitung" für alle Services angeben.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen global konfigurieren” auf Seite 517aus.
2. Geben Sie in der Spalte **Parameter** den Wert **`DISP.default.inProgressRequestFactor`**ein.
3. Geben Sie in der Spalte **Wert** den Wert ein, der als Standardwert für alle Services verwendet werden soll. Informationen zu den Werten, die angegeben werden können, finden Sie unter „Lastausgleich des Dispatchers mit In-Progress-Anforderungsfaktor” auf Seite 65.

4. Klicken Sie auf **OK**.

   Der neue Wert wird sofort angewendet.

Definieren Sie die Eigenschaft "In Bearbeitung" für einen bestimmten Service.

Sie können die Faktoreigenschaft "in-progress" für einen bestimmten Service angeben.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Services konfigurieren” auf Seite 519aus.
2. Geben Sie für den Service, den Sie konfigurieren möchten, in der Spalte **Parameter** den Wert **DISP.servicename.inProgressRequestFactor**ein, wobei *Servicename* für den Namen des Service steht.

   Geben Sie zum Beispiel für den Berichtsservice **DISP.reportService.inProgressRequestFactor**ein.
3. Geben Sie in der Spalte **Wert** den zugeordneten Wert ein, der als Standardwert für den Service verwendet werden soll. Informationen zu den Werten, die angegeben werden können, finden Sie unter „Lastausgleich des Dispatchers mit In-Progress-Anforderungsfaktor” auf Seite 65.
4. Klicken Sie auf **OK**.

   Der neue Wert wird sofort angewendet.

Eigenschaft zum Lastausgleich des Dispatchers auf den Cluster-kompatiblen Modus setzen

Wenn Ihre IBM Cognos -Server innerhalb einer Lastausgleichsinfrastruktur arbeiten, können Sie das gewichtete Round-Robin-Format des Lastausgleichs für den Dispatcher inaktivieren.

Wenn Sie diesen Parameter nicht festlegen, kann der Lastausgleich durch den Cluster und durch die IBM Cognos -Software dupliziert werden, was die Leistung beeinträchtigen kann.

Sie können die Dispatchereigenschaft "loadBalancingMode" entweder auf "weightedRoundRobin" oder "clusterCompatible" setzen.

Im Modus "weightedRoundRobin" sprüht der Dispatcher Anforderungen entsprechend den Konfigurationseinstellungen für den Dispatcher in einer gewichteten Umlaufmode. Weitere Informationen finden Sie unter „Anforderungen zwischen den Dispatchern verteilen” auf Seite 64. Dies ist der Standardmodus.

Im Modus "clusterCompatible" werden Anforderungen ohne Affinität lokal verarbeitet, wenn dies möglich ist. Wenn für den lokalen Dispatcher kein Service vorhanden ist, schlägt die Anforderung fehl. Dadurch wird sichergestellt, dass die IBM Cognos -Software alle Lastausgleichsfunktionen, die von Ihrer eigenen Lastausgleichsinfrastruktur ausgeführt werden, berücksichtigt.

Sie können die Eigenschaft "loadBalancingMode" für einzelne Dispatcher oder für eine Gruppe von Dispatchern in einem Konfigurationsordner festlegen. Weitere Informationen finden Sie unter „Dispatcher in Konfigurationsordnern gruppieren” auf Seite 49. Da es sich um eine übernommene Eigenschaft handelt, können Sie Dispatcher in einen Konfigurationsordner verschieben und die Eigenschaft loadBalancingMode für den Ordner so festlegen, dass die Eigenschaft für eine Gruppe von Dispatchern schnell festgelegt wird.

Sie können den Lastausgleich des Dispatchers auch steuern, indem Sie den Anforderungsfaktor in Bearbeitung festlegen (siehe „Lastausgleich des Dispatchers mit In-Progress-Anforderungsfaktor” auf Seite 65) oder indem Sie die Kapazitätsverarbeitung festlegen (siehe „Anforderungen zwischen den Dispatchern verteilen” auf Seite 64).

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Siehe Kapitel 13, „Funktionen”, auf Seite 207.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie auf den Pfeil für das Menü "Aktionen" neben **System** , und klicken Sie auf **Eigenschaften festlegen**.

   Tipp: Sie können auch die Einstellung für den Lastausgleich auf der Dispatcherebene ändern.
3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Wählen Sie **Optimierung** in der Liste **Kategorie** aus.
5. Wählen Sie in der Spalte **Wert** den Wert für **Lastausgleichsmodus**aus, entweder Weighted Round Robin oder Cluster Compatible, und klicken Sie anschließend auf **OK**.

   Der neue Wert wird sofort wirksam.

Nutzungsspitzenzeiträume festlegen

Sie können die Start-und Endstunden für den Spitzennachfragezeitraum für Ihre Organisation angeben.

Die meisten Organisationen haben eine Periode der Spitzennachfrage. Dieser Zeitraum ist in der Regel während der Geschäftszeiten, wenn Mitarbeiter am Arbeitsplatz sind und interaktive Berichte ausführen.

Während des Spitzenzeitraums können Sie die Anzahl der Verbindungen und Prozesse, die niedrig genug sind, festlegen, damit Jobs schneller ausgeführt werden können und Systemressourcen interaktive Anforderungen von Benutzern verarbeiten können. Weitere Informationen finden Sie unter „Maximale Anzahl Prozesse und Verbindungen” auf Seite 68. Während der Nicht-Spitzenzeit können Sie die Anzahl der Verbindungen und Prozesse höher setzen, da die Anforderungen an das System niedriger sind.

Die Standardspitzenperiode ist von 07:00 bis 18:00 Uhr. Die Standardanzahl der Verbindungen für jeden Service während der Spitzenzeit und während der Nicht-Spitzenzeit beträgt vier.

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Siehe Kapitel 13, „Funktionen”, auf Seite 207.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Alle Dispatcher**.

   Tipp: Im Teilfenster ' **Scorecard** ' ist die aktuelle Ansicht einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im Menü **Aktionen** des Dispatchers auf **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Wählen Sie **Optimierung** in der Liste **Kategorie** aus.
6. Geben Sie in der Spalte **Wert** neue Werte für die folgenden Einstellungen ein:

   · **Startzeit der Hauptperiode**

   · **Anfangszeit für Nicht-Spitzenwert**

   Tipp: Wenn Sie eine Konfigurationseinstellung auf ihren Standardwert zurücksetzen möchten, wählen Sie das entsprechende Kontrollkästchen aus, und klicken Sie auf **Auf Standardwert zurücksetzen**.
7. Klicken Sie auf **OK**.

Maximale Anzahl Prozesse und Verbindungen

Sie können die maximale Anzahl von Prozessen und Verbindungen festlegen.

Für den Berichtsservice und den Stapelberichtsservice können Sie die maximale Anzahl der Prozesse und die maximale Anzahl an Verbindungen mit hoher Affinität und niedriger Affinität festlegen, die der Dispatcher für die Bearbeitung von Anforderungen öffnen kann. Für den Agenten, den Content Manager, die Bereitstellungs-, Job-und Berichtsdatenservices können Sie die maximale Anzahl von Verbindungen festlegen.

Es gibt separate Einstellungen für Spitzenzeiten und Nicht-Spitzenzeiten. Weitere Informationen finden Sie unter „Nutzungsspitzenzeiträume festlegen" auf Seite 67.

Maximale Anzahl an Verbindungen

Pro Dispatcher gibt es ein Maximum von jedem dieser Services: Agent, Content Manager, Lieferung, Job, Berichtsdaten. Verbindungen bearbeiten eine Anforderung von einem Service zu einem bestimmten Zeitpunkt.

Sie können die maximale Anzahl der Verbindungen für jeden Service in Spitzenzeiten und Nichtspitzenzeiträumen mit den folgenden Einstellungen angeben:

- **Maximale Anzahl Verbindungen für** *< Servicename>* **Service während eines Zeitraums von nicht**
- **Maximale Anzahl Verbindungen für** *< Servicename>* **Service in Spitzenzeiten**

Die Standardanzahl der Verbindungen ist vier.

Maximale Anzahl Prozesse

Für jeden Dispatcher können mehrere Berichtsserviceprozesse und Stapelberichtsservices verwendet werden. Sie können die maximale Anzahl der Prozesse während der Spitzenzeiten mit den folgenden Einstellungen angeben:

- **Maximale Anzahl der Prozesse für die** *< Servicename>* **während des Spitzenzeitraums**
- **Maximale Anzahl der Prozesse für die** *< Servicename>* **während der Nicht-Spitzenzeit**

Die Standardanzahl der Prozesse für jeden Service ist zwei.

Affinitätsverbindungen

Berichtsserver akzeptieren niedrige und hohe Affinitätsverbindungen, um Anforderungen aus dem Stapelbericht und Berichtsservices verarbeiten zu können.

Anforderungen mit niedriger Affinität können von jedem Berichtsserver verarbeitet werden. Normalerweise werden Anforderungen mit niedriger Affinität verwendet, wenn zunächst eine Berichtsausführung angefordert wird.

Anforderungen mit hoher Affinität werden idealerweise von einem bestimmten Berichtsserver bearbeitet. In der Regel werden hohe Affinitätsanforderungen für bereits angeforderte Berichte verwendet und können Aktionen enthalten, wie zum Beispiel zur nächsten Seite in einem Bericht. Wenn der spezifische Berichtsserver nicht verfügbar oder ausgelastet ist, wird der Bericht erneut ausgeführt (Anforderung mit niedriger Affinität) auf einem Berichtsserver und die nächste Seite (Anforderung mit hoher Affinität) wird an diesen Server weitergeleitet.

Die Einstellungen für die Affinität haben Vorrang vor den Einstellungen für die Kontoanforderungen und den erweiterten Routing-Einstellungen Weitere Informationen finden Sie unter „Anforderungen zwischen den Dispatchern verteilen" auf Seite 64 und „Dispatcher-Routing" auf Seite 49.

Wenn die Affinitätseinstellungen für einen Service geändert werden, während Einträge ausgeführt werden, könnte sich die Anzahl der Serverprozesse verdoppeln. Die Anzahl der Prozesse kann vorübergehend die maximale Einstellung überschreiten, während die Änderung wirksam wird. Dies kann zu Problemen führen, wenn Ihr System für die Übergangszeit nicht genügend Speicher hat.

Sie können die Anzahl der Verbindungen mit niedriger und hoher Affinität für den Berichtsservice und den Stapelberichtsservice angeben, indem Sie die folgende Einstellung verwenden:

Anzahl der <**Niedrig** | **Hoch**> **Affinitätsverbindungen für die** *< Servicename>* **während der Nicht-Spitzenzeit**

Anmerkung: Obwohl die Formulierung dieser Einstellung impliziert, dass sie nur für Zeiträume ohne Spitzenzeiten gilt, gilt sie sowohl für Nicht-Spitzenzeiten als auch für Spitzenzeiten.

Für den Stapelberichtsservice ist die Standardanzahl der Verbindungen mit niedriger Affinität zwei. Für den Berichtsservice ist die Standardanzahl der Verbindungen mit niedriger Affinität vier. Die Standardanzahl der Verbindungen mit hoher Affinität für alle Services ist eine Verbindung.

Maximale Anzahl von Prozessen und Verbindungen festlegen

Sie können die maximale Anzahl von Prozessen und Verbindungen festlegen.

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Siehe Kapitel 13, „Funktionen”, auf Seite 207.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Dienstleistungen** , und klicken Sie anschließend auf den gewünschten Service.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im Menü **Aktionen** des Service auf **Eigenschaften festlegen**.

   Tipp: Für den Berichtsservice und den Stapelberichtsservice können Sie auch einige Einstellungen auf System-oder Dispatcherebene festlegen.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Wählen Sie **Optimierung** in der Liste **Kategorie** aus.
6. Geben Sie in der Spalte **Wert** neue Werte für die Prozesse und Verbindungen ein, die Sie ändern möchten.

   Tipp: Wenn Sie eine Konfigurationseinstellung auf ihren Standardwert zurücksetzen möchten, wählen Sie das entsprechende Kontrollkästchen aus, und klicken Sie auf **Auf übergeordneter Wert zurücksetzen**.
7. Klicken Sie auf **OK**.

Warteschlangenzeitbegrenzungen angeben

Sie können die maximale Anzahl Sekunden angeben, die interaktive Anforderungen von Benutzern in der Warteschlange auf eine verfügbare Berichtsserviceverbindung warten lassen.

Wenn eine Anforderung nicht innerhalb des Zeitlimits verarbeitet werden kann, schlägt die Anforderung fehl und die Benutzer erhalten eine Fehlernachricht. Wenn Ihr Betriebssystem über ausreichende Ressourcen verfügt und die IBM Cognos -Software ordnungsgemäß konfiguriert ist, sollten Anforderungen nicht länger als die Zeitgrenze dauern.

Wenn Sie eine Zeitbegrenzung angeben, sollten Sie die maximale Anzahl an Sekunden berücksichtigen, die Benutzer auf eine Antwort warten möchten. Der Standardwert für die Warteschlangenzeit ist 240 Sekunden.

Anforderungen für den Stapelberichtsservice bleiben auf unbestimmte Zeit in der Warteschlange.

Wenn Sie über eine hohe Benutzerlast (über 165 Benutzer) verfügen und interaktive Berichte in einer verteilten Installation kontinuierlich ausgeführt werden, erhöhen Sie die Warteschlangenzeitbegrenzung

auf 360, um keine Fehlernachrichten zu erhalten. Möglicherweise möchten Sie auch die Einstellung für das asynchrone Zeitlimit erhöhen, um zu vermeiden, dass Fehlernachrichten angezeigt werden. Weitere Informationen finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Siehe Kapitel 13, „Funktionen”, auf Seite 207.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Status** auf **System**.
2. Klicken Sie auf den Pfeil für das Menü "Aktionen" neben **System** , und klicken Sie auf **Eigenschaften festlegen**.

   Tipp: Sie können auch die Einstellungen für die Warteschlangenzeit auf der Dispatcherebene oder auf der Serviceebene ändern.
3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Wählen Sie **Optimierung** in der Liste **Kategorie** aus.
5. Geben Sie in der Spalte **Wert** einen neuen Wert für die Einstellung **Zeitlimit für Warteschlangenzeit des Berichtsservice (Sekunden)**ein.

   Tipp: Wenn Sie eine Konfigurationseinstellung auf ihren Standardwert zurücksetzen möchten, wählen Sie das entsprechende Kontrollkästchen aus und klicken Sie auf **Auf Standardwert zurücksetzen**.
6. Klicken Sie auf **OK**.

PDF-Dateieinstellungen

Es gibt vier Einstellungen für PDF-Dateien, die zusammen die Geschwindigkeit, mit der PDF-Dateien erstellt werden, und die Größe von PDF-Dateien bestimmen.

Die idealen Einstellungen sind für verschiedene Umgebungen unterschiedlich. Wenn Sie z. B. PDF-Dateien als Teil der Stapeljobs über Nacht erstellen, ist es Ihnen möglicherweise nicht möglich, die Geschwindigkeit zu erhöhen. Sie können Einstellungen auswählen, die kleine Dateien erzeugen, die leicht verteilt werden können, aber länger dauern, bis sie generiert werden. Wenn Sie Ad-hoc-PDF-Dateien oder komplexe PDF-Dateien mit vielen Diagrammen und Grafiken erstellen, können Sie mehr über die Geschwindigkeit als die Dateigröße kümmern.

Sie können verschiedene PDF-Dateieinstellungen für den Berichtsservice und für den Stapelberichtsservice verwenden.

PDF-Zeichencodierung

Die PDF-Zeichencodierung bestimmt den Zeichensatz, der zum Erstellen von PDF-Dateien verwendet wird. Sie können auswählen, dass die Codierung Windows1252, die Standardcodierung des Microsoft Fenster -Betriebssystems für lateinische Texte in westlichen Schreibsystemen oder die Unicode-Codierung (UTF-16) verwendet werden soll. Standardmäßig wird die PDF-Zeichencodierung automatisch festgelegt, basierend auf den in der Datei gefundenen Zeichen.

Die Einstellungsnamen lauten wie folgt:

- **PDF-Zeichencodierung für Berichtsservice**
- **PDF-Zeichencodierung für Stapelberichtsservice**.

Wert	Zweck
Windows1252	Wenn Sie wissen, dass Ihre Dateien nur Windows1252-Zeichen enthalten, verwenden Sie diese Einstellung für die schnellere Erstellung von PDF-Dateien. Alle Unicode-Zeichen (UTF-16) ohne Windows1252-Äquivalent werden in einen unbestimmten Windows1252-Charakter konvertiert.
Schriftart	Wenn Sie wissen, dass Ihre Dateien nicht-Windows1252-Zeichen enthalten (z. B. chinesische Zeichen), verwenden Sie diese Einstellung für eine schnellere PDF-Generierung als mit der Einstellung "Auto". Als PDF-integrierte Schriftarten werden alle Windows1252-Zeichen codiert. Fast alle anderen Schriftarten verwenden den Zeichensatz UTF-16. Diese Einstellung erstellt in der Regel größere PDF-Dateien als die Einstellung Windows1252. Es ist möglich, dass UTF-16-codierte Dateien eine bessere Komprimierung erhalten (siehe „Inhaltkomprimierungstyp“ auf Seite 73.
Automatisch	Verwenden Sie diese Einstellung, um automatisch zu bestimmen, ob Windows1252 oder UTF-16 verwendet werden soll, um den Text in dem Dokument zu codieren. Wenn große Textkörper analysiert werden müssen, ist dies der langsamste der drei Einstellungen. Wenn die Geschwindigkeit ein Anliegen ist, können Sie die anderen Werte mit verschiedenen Berichten versuchen, um die beste Einstellung für Ihre Umgebung zu bestimmen. Dies ist der Standardwert.

Schriftarteinbettung

Um sicherzustellen, dass die in einem Bericht verwendeten Schriftarten für alle Leser verfügbar sind, können Schriftarten in PDF-Dateien eingebettet werden. In IBM Cognos Konfiguration gibt es zwei Font-Einbettungslisten, eine für den Berichtsservice und eine für den Stapelberichtsservice.

Schriftarten können so angegeben werden, dass sie immer eingebettet oder nie eingebettet werden. So können beispielsweise Schriftarten, die kein legales Recht auf Umverteilung haben, als nie eingebettet angegeben werden. Schriftarten, die nicht in Ihren Außendienststellen zur Verfügung stehen, aber zum Lesen von PDF-Berichten erforderlich sind, können wie immer eingebettet angegeben werden.

Weitere Informationen zu den Font-Einbettungslisten finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

In **IBM Cognos Administration**können Sie die Schriftarteinbettung in den PDF-Dateien des Berichtsservice und des Stapelberichtsservice zulassen oder nicht zulassen. Sie können auch die automatische Schriftarteinbettung auswählen. Denken Sie daran, dass Dateien mit eingebetteten Schriftarten größer sind und mehr Zeit für die Generierung von Dateien einnehmen. Die Einbettung von

Schriftarten kann zu einer Belastung der Netzressourcen führen. Weniger eingebettete Schriftarten können den Verbrauch von Netzressourcen verringern.

Die Lizenz für einige Schriften verbietet die Einbettung. Stellen Sie sicher, dass Sie über die Berechtigung des Anbieters verfügen, lizenzierte Schriftarten einzubetten.

Die Einstellungsnamen lauten wie folgt:

- **Option, um den Berichtsservice zuzulassen, dass Schriftarten in generierten PDF-Dokumenten eingebettet werden**
- **Option, um den Stapelberichtsservice zuzulassen, dass Schriftarten in generierten PDF-Dokumenten eingebettet werden**.

Es gibt spezielle Schriftarten, wie z. B. Barcodeschriftarten, die bei der Verwendung immer eingebettet werden. Diese Einstellungen steuern die Einbettung spezialisierter Schriftarten nicht. Integrierte PDF-Schriftarten werden nie eingebettet.

Wert	**Zweck**
Zulassen	Wenn Sie wissen, dass Ihr Publikum nicht über alle Schriften verfügt, die sie zum Anzeigen von PDF-Berichten benötigen, verwenden Sie diese Einstellung. Dateien sind größer und die PDF-Ausgabe wird langsamer generiert. Schriftarten, die sich in der nie einembierten Liste in der IBM Cognos -Konfiguration befinden, werden nicht eingebettet. Dies ist der Standardwert.
Nicht zulassen	Wenn Sie wissen, dass Ihr Publikum alle Schriften hat, die sie zum Anzeigen von PDF-Berichten benötigen, verwenden Sie diese Einstellung. Dateien sind kleiner und werden schneller generiert. Schriftarten werden nicht eingebettet, es sei denn, sie befinden sich in der immer einembierten Liste in IBM Cognos Konfiguration.
Automatisch	Bestimmt automatisch, welche Schriftarten eingebettet werden sollen. Diese Einstellung benötigt die längste Zeit, um PDF-Berichte zu generieren. Wenn die Daten nur Windows1252-Zeichen enthalten, werden sowohl die immer embed als auch die nie einembed Liste in IBM Cognos Configuration verwendet. Wenn es einen Konflikt gibt, wird die nie einemierte Liste verwendet. Mit Ausnahme von spezialisierten Schriftarten werden nicht aufgelistete Schriftarten in der Regel nur dann eingebettet, wenn in der Datei UTF-16-Zeichen aus dieser Schriftart verwendet werden.

Inhaltkomprimierungstyp

Sie können den Komprimierungstyp festlegen, der verwendet werden soll, wenn PDF-Berichte erstellt werden. Es dauert länger, die PDF-Ausgabe für Dateien mit einem höheren Komprimierungstyp zu erstellen, aber die resultierenden Dateien sind kleiner.

Der Komprimierungstyp 'Inhalt' gibt an, welche Daten komprimiert werden. Der „Einstellungen für PDF-Dateien angeben" auf Seite 73 gibt an, wie sehr die Daten komprimiert werden. Die Kombination der beiden Einstellungen bestimmt die endgültige Dateigröße.

Die Einstellungsnamen lauten wie folgt:

- **Der PDF-Komprimierungstyp für PDF-Dokumente, die vom Berichtsservice erstellt wurden.**
- **Der PDF-Komprimierungstyp für PDF-Dokumente, die durch den Stapelberichtsservice erstellt wurden**.

Die Auswahlmöglichkeiten für diese Einstellung sind vom niedrigsten bis zum höchsten Komprimierungstyp: **Klassisch**, **Basis**, **Verbessert**, **Erweitert**und **Voll**. **Klassisch** ist der Standardwert.

Der Komprimierungstyp bezieht sich auf die Menge der Daten, die in einem PDF-Bericht komprimiert werden. In der Regel bedeutet weniger Komprimierung eine schnellere Komprimierung und ein größeres Dokument. Versionen von Adobe PDF Acrobat Reader, die älter als Version 6.0 sind, unterstützen keine Komprimierungsarten, die höher sind als Classic.

Es gibt seltene Fälle, in denen die Komprimierung dazu führt, dass kleine Dateien leicht größer werden.

Komprimierungsalgorithmusstufe

Der Komprimierungstyp 'Inhalt' gibt an, welche Daten komprimiert werden. Der „Inhaltkomprimierungstyp" auf Seite 73 gibt an, wie sehr die Daten komprimiert werden. Die Kombination der beiden Einstellungen bestimmt die endgültige Dateigröße.

Die Einstellungsnamen lauten wie folgt:

- **Inhalt Komprimierungsstufe für PDF-Dokumente, die vom Berichtsservice erstellt wurden**
- **Inhalt Komprimierungsstufe für PDF-Dokumente, die vom Stapelberichtsservice erstellt wurden**

Gültige Auswahlmöglichkeiten für die Komprimierungsalgorithmusstufe sind 0 (keine Komprimierung) bis 9 (maximale Komprimierung). Der Standardwert ist 9.

Einstellungen für PDF-Dateien angeben

Sie können PDF-Dateieinstellungen angeben.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Dienstleistungen** , und klicken Sie auf den gewünschten Service.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im Menü **Aktionen** des Service auf **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Wählen Sie **Optimierung** in der Liste **Kategorie** aus.
6. Geben Sie in der Spalte **Wert** den Wert ein, den Sie für jede der Einstellungen für die PDF-Datei wünschen.

   Tipp: Wenn Sie eine Konfigurationseinstellung auf ihren Standardwert zurücksetzen möchten, wählen Sie das entsprechende Kontrollkästchen aus, und klicken Sie auf **Auf Standardwert zurücksetzen**.
7. Klicken Sie auf **OK**.

Maximale Ausführungszeit festlegen

Sie können die maximale Ausführungszeit für den Berichtsservice und den Stapelberichtsservice festlegen.

Sie können beispielsweise die Ausführungszeit einschränken, wenn Sie wissen, dass etwas falsch ist, weil die Aufgaben länger dauern. Sie können auch sicherstellen, dass keine einzige Aufgabe die Serverzeit zum Nachteil der anderen monopolisiert.

Wenn das Zeitlimit überschritten wird, wird die Ausführung abgebrochen. Der Standardwert ist null. Dieser Wert gibt keine Begrenzung für die Ausführungszeit an.

Diese Einstellung hat Vorrang vor der Festlegung des Governor-Grenzwerts. Weitere Informationen finden Sie unter „Grenzwert für Berichtsgröße für den Berichtsdatenservice festlegen" auf Seite 76.

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Siehe Kapitel 13, „Funktionen", auf Seite 207.

Informationen zu diesem Vorgang

Diese Einstellung kann auf System-, Dispatcher-oder Serviceebene geändert werden.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Dienstleistungen** , und klicken Sie auf Service, den Sie möchten.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im **Aktionen** -Menü für den Service auf **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Wählen Sie **Optimierung** in der Liste **Kategorie** aus.
6. In the **Wert** column, type a new value for the **Maximale Ausführungszeit für die** *Servicename* **(Sekunden)** setting.
7. Klicken Sie auf **OK**.

Angeben, wie lange die Ausgabe der Überwachungslistenberichte beibehalten werden soll

Sie können die Ausgabe der Berichtsliste für eine bestimmte Anzahl von Ausführungen oder für eine bestimmte Anzahl von Tagen oder Monaten beibehalten.

Sie können beispielsweise bis zu 10 Versionen beibehalten, oder Sie können die Berichtsausgabeversionen für 2 Tage oder 6 Monate beibehalten.

Es gibt zwei Einstellungen:

- Wenn Sie die maximale Zeitdauer angeben möchten, die die Ausgabe der Überwachungslistenberichte beibehalten soll, verwenden Sie die Einstellung **Periodisches Aufbewahrungszeitalter für Dokumentversion** . Der Standardwert ist 1 Tag. Im Teilfenster ' **Einstellungen** ' wird dies als 1 Tag (n) angezeigt.
- Wenn Sie die maximale Anzahl von Kopien angeben möchten, die beibehalten werden sollen, verwenden Sie die Einstellung **Aufbewahrungszähler für periodische Dokumentversion** . Es ist kein Standardwert vorhanden.

Wenn Sie beide Einstellungen angeben, bestimmt der erste Wert zuerst, wie viele Versionen beibehalten werden.

Die Einstellungen, die Sie auswählen, hängen davon ab, wie oft die Ausgabe von Listenberichten generiert wird und wie Ihre Systemressourcen verwendet werden. Wenn z. B. ein Bericht nächtlich ausgeführt wird, um die Ausgabe während des Tages auf Abruf über das Portal bereitzustellen, und die Beobachtungslisten wöchentlich aktualisiert werden, können Sie nur vier Versionen pro Monat beibehalten, jedoch nicht mehr als 5 Versionen während dieser Zeit. Wenn ein Job zum Ausführen von Berichten verwendet wird und die Beobachtungslisten nur aktualisiert werden, wenn der Job ausgeführt wird, können Sie nur 1 Version jeden Tag behalten.

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Siehe Kapitel 13, „Funktionen”, auf Seite 207.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Status** auf **System**.
2. Klicken Sie auf den Pfeil für das Menü "Aktionen" neben **System** , und klicken Sie auf **Eigenschaften festlegen**.
3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Wählen Sie **Optimierung** in der Liste **Kategorie** aus.
5. Geben Sie in der Spalte **Wert** einen neuen Wert für die Einstellung **Periodisches Aufbewahrungszeitalter für Dokumentversion** ein, und wählen Sie **Tag (n)** oder **Monat (n)** aus dem Dropdown-Menü aus.
6. Geben Sie in der Spalte **Wert** einen neuen Wert für die Einstellung **Aufbewahrungszähler für periodische Dokumentversion** ein.
7. Klicken Sie auf **OK**.

Hotspots begrenzen, die in Analysis Studio-oder Reporting -Diagramm generiert werden

Um die Leistung zu verbessern, können Sie die Anzahl der Hotspots, die für Analysis Studio-und Reporting -Diagramme generiert werden, begrenzen.

Ein Hotspot in einem Diagramm wird angezeigt, wenn Sie einen Zeiger über ihn anhalten. Beispiel: Ein Hotspot auf einem Drilldown-Symbol oder ein QuickInfo gibt Details zu der Spalte, der Linie oder dem Kreissektor an. Die Antwortzeit des Browsers erhöht sich mit der Anzahl der Hotspots. Wenn Diagramme mit vielen Mitgliedern generiert werden, können die Hotspots zu einer zusätzlichen Belastung für die Systemressourcen werden, die den Browser einfrieren können.

Wenn Sie die Anzahl der Hotspots begrenzen, werden Elemente wie z. B. Achsenbeschriftungen und Legendenbeschriftungen vor einzelnen grafischen Elementen wie Balken, Kreisausschnitten usw. Vorrang erhalten. Abhängig von der Anzahl der Elemente in einem Diagramm und der Einstellung für die maximale Anzahl von Hotspots können einige Achsenelemente Hotspots haben, während andere Achsenelemente und alle grafischen Elemente nicht oder alle Achsenelemente und einige grafische Elemente Hotspots aufweisen können, während andere grafische Elemente nicht vorhanden sind.

Die Einstellung für die maximale Hotspot-Einstellung in Reporting überschreibt diese Einstellung. Weitere Informationen finden Sie im *IBM Cognos Analytics - Reporting Benutzerhandbuch*.

Der Standardwert ist eine unbegrenzte Anzahl von Hotspots.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Status** auf **System**.
2. Klicken Sie auf den Pfeil für das Menü "Aktionen" neben **System** , und klicken Sie auf **Eigenschaften festlegen**.

Tipp: Sie können die Hotspot-Einstellung auch auf der Dispatcherebene oder auf der Serviceebene ändern.

3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Wählen Sie **Optimierung** in der Liste **Kategorie** aus.
5. Suchen Sie die Einstellung **Anzahl der in einem Diagramm durch den Stapelberichtsservice generierten Hotspots** oder **Anzahl der Hotspots, die in einem Diagramm vom Berichtsservice generiert wurden** . Klicken Sie in der Spalte **Wert** auf den Pfeil neben **Unbegrenzt** , und klicken Sie dann auf **< Anzahl >**. Geben Sie einen neuen Wert für die maximale Anzahl an Hotspots ein.
6. Klicken Sie auf **OK**.

Grenzwert für Berichtsgröße für den Berichtsdatenservice festlegen

Sie können die Größenbegrenzung für Berichtsdaten erhöhen.

Um die Ressourcen, wie z. B. Speicher, zu begrenzen, die vom Berichtsdatenservice verwendet werden, beschränkt IBM Cognos -Software die Größe der Berichtsdaten, die gesendet werden können. Wenn Sie Fehler in IBM Cognos für Microsoft Office erhalten, dass ein Berichtsergebnis zu groß ist, können Sie die Größenbegrenzung für Berichtsdaten erhöhen, indem Sie die Einstellung für den Governor-Grenzwert ändern.

Die Einstellung für die maximale Ausführungszeit hat Vorrang vor dieser Einstellung. Weitere Informationen finden Sie unter „Maximale Ausführungszeit festlegen" auf Seite 74.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Dienstleistungen** > **Berichtsdaten**.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im Menü **Berichtsdatenservice Aktionen** auf **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Ändern Sie in der Spalte **Wert** die Nummer für **Grenzwert für Governor (MB)**.
6. Klicken Sie auf **OK**.

Mit Ausnahme der Kontext-ID für einen Agenten aus IBM WebSphere -Web-Service-Tasks

Wenn der Agentenservice mit einem Web-Service interagiert, wird standardmäßig die Kontext-ID des Agenten eingeschlossen.

Wenn Sie einen Agenten ausführen, der eine Web-Service-Task in IBM WebSphereenthält, sollten Sie diese Kontext-ID ausschließen, um einen Konflikt mit den WebSphereeigenen Kontext-IDs zu vermeiden.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Services konfigurieren" auf Seite 519aus.
2. Geben Sie für den **AgentService**in der Spalte **Parameter** den Wert **asv.webservice.useRunContext**ein.

   Sie müssen diese Einstellung für jede **AgentService** -Instanz angeben, die ausgeführt wird.
3. Geben Sie **Wahr** als Wert für diesen Parameter ein und klicken Sie auf **OK**.
4. Starten Sie IBM Cognos -Services erneut.

Optimieren Sie den Cache für den Repository-Service

Sie können den Cache für den Repository-Service optimieren. Es gibt verschiedene Dimensionierungseigenschaften, die für lokale Speicher-und Plattenressourcen festgelegt werden können. Einstellungen können für jeden Dispatcher eindeutig sein.

Die folgende Tabelle enthält eine Beschreibung der Typen von Cache, die für den Repository-Service optimiert werden können.

Tabelle 21. Für den Repository-Service verfügbare Cachetypen

Parameter	Beschreibung
Maximale Anzahl Sekunden-Berichte und Berichtselemente können im Cache vorhanden sein.	Die maximale Anzahl Sekunden, die ein Bericht im Cache vorhanden sein kann, unabhängig davon, wie oft er verwendet wird. Nachdem ein Bericht abläuft, wird er aus dem Repository abgerufen und nicht mit dem Cache. Der Standardwert ist 1200 Sekunden (20 Minuten). Der Wert 0 bedeutet, dass der Bericht nicht im Cache gespeichert wird.
Maximale Anzahl von Berichten und Berichtselementen, die auf Platte überlaufen können	Die maximale Anzahl der Cacheeinträge, die im lokalen Speicher gespeichert werden sollen. Der Standardwert ist 1000 Einträge. Der Wert 0 bedeutet, dass die Anzahl der Elemente, die im lokalen Speicher gehalten werden, nicht begrenzt ist.
Maximale Anzahl von Berichten und Berichtselementen, die im Speicher gespeichert werden können	Die maximale Anzahl der Cacheeinträge, die auf der lokalen Platte geschrieben werden können. Wenn der Speichercache den Grenzwert erreicht, werden die Elemente auf die lokale Platte überlaufen. Der Standardwert ist 100 Berichte und Berichtselemente. Eine Einstellung von 0 bedeutet, dass die Anzahl der auf die Platte geschriebenen Elemente nicht begrenzt ist. Die Einträge werden in die Position der Datendateien geschrieben, die in IBM Cognos Configuration definiert sind.

Der Repository-Service verwendet die erweiterte Einstellung **`repository.maxCacheDocSize`** , um die maximale Größe der einzelnen Berichtsausgaben in Megabyte anzugeben, die im Cache gespeichert werden können. Ausgaben, die größer als die angegebene Größe sind, werden nicht zwischengespeichert und müssen immer aus dem Repository oder Content Manager abgerufen werden. Der Standardwert ist 10. Sie können diese erweiterte Einstellung einzeln für einen bestimmten Repository-Service oder einen Dispatcher oder global für die gesamte IBM Cognos -Umgebung angeben. Weitere Informationen finden Sie unter Anhang G, „Konfiguration der erweiterten Einstellungen” , auf Seite 517.

Massenbereinigung von NC-Tabellen

Verwenden Sie den Massenbereinigungsprozess, um fertige Tasks aus NC-Tabellen im Content-Store zu entfernen.

Die Batchverarbeitung wird für verschiedene Tasks und Objekte unterstützt. Ein allgemeines Beispiel kann ein geplanter Job sein, der Berichtsausführungen enthält. Der Monitor-Service speichert die Job-und Berichtsausführungsbefehle in einer Taskwarteschlange in NC-Tabellen. Unter idealen Umständen werden die fertig gestellten Aufgaben von einem Hintergrundthread aus-Eins entfernt. Bei ausgelasteten Servern oder wenn die geplante Ausführungsrate die Systemkapazität überschreitet, ist möglicherweise nicht genügend Zeit, um die beendeten Tasks auf diese Weise zu entfernen. Die Taskwarteschlange wächst ständig und kann zu Problemen bei der Serverleistung führen. Das Problem manifestiert sich als lange Liste der anstehenden Berichtsausführungen, wenn Sie die aktuellen Aktivitäten in der Verwaltungskomponente anzeigen.

Die folgenden NC-Tabellen sind betroffen:

- NC_TASK_ANCESTOR_STOREIDS
- NC_TASK_HISTORY_DETAIL
- NC_TASK_QUEUE
- NC_TSE_STATE_MAP
- NC_TASK_PROPERTY

Der Massenbereinigungsprozess verwendet ein datenbankspezifisches `BulkFinishedTaskCleanerThread` -Script. Dieses Script wird vom Überwachungsservice während des Starts des IBM Cognos -Service eingeleitet. Wenn diese Option aktiviert ist, prüft das Script zunächst, ob eine bestimmte (konfigurierbare) Anzahl von abgeschlossenen Tasks in den NC-Tabellen vorhanden ist. Wenn solche Tasks gefunden werden, werden sie in eine temporäre Tabelle verschoben, und die NC-Tabellen werden alle in einer Transaktion gelöscht. Es ist keine Tabelle erforderlich, die aus dem NC-Schema gelöscht oder erneut erstellt werden muss. Sie müssen auch die IBM Cognos -Services nicht stoppen.

Der Bereinigungsprozess wird aktiviert und konfiguriert, indem die folgenden erweiterten Einstellungen für den Monitor-Service verwendet werden:

- `event.finished.check.active`
- `event.finished.check.interval`
- `event.finished.check.threshold`

Weitere Informationen zu diesen Einstellungen finden Sie im Artikel „Erweiterte Einstellungen für Monitor-Service" auf Seite 539.

Informationen zum Konfigurieren erweiterter Einstellungen finden Sie unter Anhang G, „Konfiguration der erweiterten Einstellungen", auf Seite 517.

Wichtig: Stellen Sie sicher, dass Sie immer eine gültige und aktuelle Sicherung des Content-Stores haben.

Ausführung ablaufender Abfragen

Abhängig von Ihrer Umgebung können Sie die Leistung des Berichts verbessern, indem Sie die gleichzeitige Ausführung der Abfrage aktivieren.

Standardmäßig führt die IBM Cognos -Software Abfragen in einem Bericht nacheinander aus. Sie können dies tun, indem Sie erweiterte Servereigenschaften für den Berichtsservice, den Stapelberichtsservice oder beides festlegen. Wenn die Ausführung gleichzeitig ablaufender Abfragen aktiviert ist, legt der Berichtsserver fest, welche Abfragen im Bericht gleichzeitig ausgeführt werden können.

Der Berichtsersteller muss die Abfragen in einem Bericht angeben, bei denen es sich um Kandidaten für die gleichzeitige Ausführung handelt. Weitere Informationen finden Sie im *IBM Cognos Analytics - Reporting Benutzerhandbuch*.

RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS

Verwenden Sie diesen Parameter, um die gleichzeitige Ausführung von Abfragen zu aktivieren und die maximale Anzahl von Abfrageausführungs-Helfern für jeden Berichtsservice oder Stapelberichtsserviceprozess festzulegen.

Der Standardwert ist 0, d. h. die gleichzeitige Ausführung der Abfrage ist inaktiviert.

Jede Abfrageausführungshilfe führt zu einer zusätzlichen Datenquellenverbindung. Ein Berichtsservice verfügt beispielsweise über vier Prozesse mit zwei Verbindungen mit hoher Affinität und zwei Verbindungen mit niedriger Affinität:

- Wenn die maximale Anzahl an Abfrageausführungs-Helfern auf 0 (inaktiviert) gesetzt ist, beträgt die maximale Anzahl der vom Berichtsservice erstellten Datenquellenverbindungen 16 (zwei Verbindungen

mit niedriger Affinität plus zwei High-Affinitäts-Verbindungen plus null Abfrageausführungshelfer mal vier Prozesse).

- Wenn die maximale Anzahl an Abfrageausführungshelfern auf 2 gesetzt ist, beträgt die maximale Anzahl von Datenquellenverbindungen, die vom Berichtsservice erstellt wurden, 24 (zwei Verbindungen mit niedriger Affinität plus zwei Hochaffinitätsverbindungen plus zwei Abfrageausführungshelfer mal vier Prozesse).

RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT

Verwenden Sie diesen Parameter, um die maximale Anzahl an Abfrageausführungs-Helfern für jeden Bericht anzugeben. Dieser Parameter wird verwendet, um zu verhindern, dass ein einzelner Bericht alle verfügbaren Helfer für die Abfrageausführung konsumiert.

Ein Bericht verfügt beispielsweise über acht Abfragen, die gleichzeitig ausgeführt werden können:

- Wenn RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS und RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT beide auf vier gesetzt sind, verbraucht der Bericht alle Abfragehelfer, wenn sie ausgeführt werden. Es ist kein anderer Bericht möglich, Abfragen gleichzeitig auszuführen, bis der Bericht die Ausführung beendet hat.
- Wenn RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT stattdessen auf zwei gesetzt ist, konsumiert der Bericht zwei Abfragehelfer, sodass zwei für andere Berichte verwendet werden.

Der Standardwert für diesen Parameter ist 1.

Diese Einstellung hat keine Auswirkung, es sei denn, RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS ist auf mehr als 0 gesetzt.

RSVP.CONCURRENTQUERY.ENABLEDFORINTERACTIVEOUTPUT

Verwenden Sie diesen Parameter, um die gleichzeitige Ausführung von Abfragen zu aktivieren, wenn der Berichtsservice interaktive Ausgabe erstellt.

Bei interaktiven Berichten können einige Abfragen, wenn die Ausführung gleichzeitig ablaufender Abfragen aktiviert ist, unnötigerweise ausgeführt werden, da die Ergebnisse nicht verwendet werden. So können beispielsweise alle Abfragen für einen mehrseitigen Bericht mit mindestens einer Abfrage auf jeder Seite ausgeführt werden, der Benutzer kann jedoch nur die erste Seite anzeigen. Wenn Sie keine Ressourcen für Ergebnisse verwenden möchten, die nicht in interaktiven Berichten verwendet werden, inaktivieren Sie diesen Parameter.

Autorisierte Eingabeaufforderungsseiten sind keine interaktive Ausgabe und sind von dieser Einstellung nicht betroffen.

Der Standardwert für diesen Parameter ist 'false', d. h. inaktiviert.

RSVP.PROMPT.EFFECTIVEPROMPTINFO.IGNORE

Verwenden Sie diesen Parameter, um das Absetzen des Attributs 'effectivePromptInfo' in Metadatenanforderungen zu inaktivieren und das Verschieben der Eingabeaufforderungsinformationen unter dem Attribut 'caption' einer Ebene auf die Ebene selbst wirksam zu inaktivieren.

Der Standardwert für diesen Parameter ist 'false', d. h. inaktiviert.

Richtlinien für die gleichzeitige Ausführung von Abfragen

Wir empfehlen Ihnen, diese Richtlinien zu befolgen, um die Effizienz Ihrer gleichzeitigen Abfrageausführung zu verbessern.

Berichtsserver können mehrere Berichte zur gleichen Zeit ausführen. Jeder Bericht wird in einem Thread innerhalb des Berichtsservers ausgeführt. Wenn mehr CPUs vorhanden sind, können weitere Berichte gleichzeitig ausgeführt werden. Da ein Bericht ausgeführt wird, werden Anforderungen für Daten über die Abfrageengine erstellt. In einigen Szenarios kann die Nutzung der Funktion für die gleichzeitige Abfrage

zulassen, dass mehrere Abfragen gestartet werden, bevor die Daten für die Wiedergabe benötigt werden. Dadurch wird die gesamte abgelaufene Zeit für den Abschluss eines Berichts reduziert.

Die gleichzeitige Ausführung von Abfragen ermöglicht es einem einzelnen Bericht, mehr Ressourcen zu verbrauchen, was wiederum die verstrichenen Zeiten verringern kann. Die Erhöhung der Anzahl gleichzeitig ablaufender Aktivitäten kann sich auf den Durchsatz der Cognos-Anwendungs-oder Datenbankebene in einer Umgebung auswirken.

Wenn Sie versuchen, mehr Threads als die tatsächlichen CPUs auf einem Computer zu verwenden, wird die Zeit, die für die Ausführung eines Berichts benötigt wird, nicht reduziert. Sie kann auch dazu führen, dass Berichte langsamer ausgeführt werden, da mehr Konkurrenzsituationen auf dem Speicherheapspeicher im Report Server-Prozess auftreten.

Ein Szenario, in dem gleichzeitige Abfragen die verstrichene Zeit verbessern können, wäre, wenn ein Bericht nur sehr wenige Seiten, vielleicht eine Seite, wiedergibt. Diese Seite kann mehrere Layouts enthalten, deren Abfragen innerhalb der Datenbank schnell ausgeführt werden, wenn sie gleichzeitig ausgeführt werden.

Definieren Sie als Ausgangspunkt die maximale Anzahl an Helfern pro Prozess, die auf die Anzahl der CPUs auf der Maschine gesetzt sind. Cognos Application-Tier-Server führen normalerweise mehrere Services aus. Daher wäre die tatsächliche Anzahl pro Server ein kleinerer Wert.

Wenn ein Berichtsserver häufig mehrere Berichte gleichzeitig ausführt, legen Sie die Anzahl der Helfer pro Bericht auf eine kleinere Zahl fest, so dass jeder Bericht ein paar Threads erhält. Dies wird zu konsistenten Ausführungszeiten führen. Wenn Sie die maximale Anzahl pro Bericht auf maximal pro Prozess setzen, laufen Sie Gefahr, dass ein Bericht alle zusätzlichen Threads abruft, während andere keine zusätzlichen Threads erhalten.

Durch die Erhöhung der Threads, die für "N"verwendet werden, verfügt jeder Report Server-Prozess (BiBusTKServerMain) über "N" -Threads. Die mögliche Last auf dem Computer ist die Summe von `(Berichtsserverprozesse * n)`.

Wenn ein kompatibler Abfragemodus (CQM) verwendet wird, verfügt jeder Berichtsserver über eine eigene In-Prozess-Abfrageengine. Wenn der dynamische Abfragemodus (DQM) verwendet wird, senden die Berichtsserver ihre Datenanforderung an einen DQM-Service. Als Ergebnis kann die Ressourcennutzung und die Auslastung des Dynamic Query-Servers zunehmen.

Gleichzeitige Abfragen in Stapelberichten im Vergleich zu interaktiven Berichten

Um Berichte schneller zu machen, sollten Sie diese in einem nicht interaktiven Modus anstatt im interaktiven Modus ausführen.

Der gleichzeitig ablaufende Abfragemanager verarbeitet Abfragen, die von der letzten Abfrage des Berichts ausgehend verarbeitet werden, und arbeitet den Weg zum ersten Mal. Wenn Berichte in einem nicht interaktiven Modus wiedergegeben werden, führt der Hauptthread des Berichtsservers die ersten Abfragen aus. Es wird auch beginnen, verfügbare Helper-Threads zu verwenden, um Abfragen zu starten, die mit Layouts verknüpft sind, zu denen es sich bewegen wird. Durch das Starten dieser Abfragen können Daten bereitgestellt werden, anstatt auf die Ausführung der Abfrage zu warten, die zu diesem Zeitpunkt ausgeführt werden soll.

Die gleiche Strategie wird auch für interaktive Berichte verwendet. Ein Berichtsentwurf kann jedoch mehrere Seitenlayouts enthalten, zu denen ein Benutzer nie navigiert. In der Folge kann das System mehrere Abfragen ausführen, die nie wiedergegeben werden, da das Layout nicht erforderlich ist. Der interaktive Modus sollte nur aktiviert werden, wenn interaktive Berichte dazu tendieren, vollständig konsumiert zu werden, wie z. B. Einzelseitenlayouts. Sie sollte nicht aktiviert werden, wenn interaktive Berichte dazu neigen, nur wenige Seiten von vielen zu betrachten.

Berichte mit einer Untergruppe von Abfragen, die gleichzeitig aktiviert wurden

Um die Laufzeiten Ihres Berichts zu optimieren, müssen Sie nur eine Untergruppe der Abfragen festlegen, die gleichzeitig verarbeitet werden sollen.

Der Berichtsserver erstellt eine Liste der Abfragen, die an den gleichzeitig ablaufenden Abfragemanager übergeben werden. Abfragen müssen die folgenden Voraussetzungen erfüllen:

- Die **Methode ausführen** -Eigenschaft der Abfrage muss auf **Gleichzeitig**gesetzt sein.
- Sie wird in einer Berichtsseite aus einem Datencontainer (List, Crosstab, Char usw.) referenziert.
- Es handelt sich nicht um ein Detaillayout.
- Auf sie wird von einer Eingabeaufforderungssteuerung verwiesen, die kein untergeordnetes Kaskadenuntergeordnete Element ist.

Wenn die Liste nicht zwei oder mehr Abfragen enthält, ist keine gleichzeitige Abfrageverarbeitung erforderlich.

Ein Bericht verfügt beispielsweise über 3 Listen mit Abfragen Q1, Q2 und Q3. Wenn Q2 und Q3 gleichzeitig markiert sind, werden nur Q2 und Q3 gleichzeitig ausgeführt; Q1 wird es nicht. Wenn Q2 eine Verbindung von Q2.1 und Q2.2 ist, müssen Sie Q2 als gleichzeitig gleichzeitig markieren. Die Markierung von Q2.1 oder Q2.2, die gleichzeitig ausgeführt werden soll, hat keine Auswirkung, da Q2.1 und Q2.2 nicht vom Layout referenziert werden. Das heißt, der Berichtsserver führt Q2 aus, nicht Q2.1 oder Q2.2, es sei denn, einige andere Datencontainer verweisen auf Q2.1 oder Q2.2.

In komplexen Berichten, bei denen viele Seitenlayouts und Abfragen vorhanden sind, können Sie nicht alle Abfragen für die gleichzeitige Ausführung festlegen. Dies kann zu einer übermäßigen Ressourcennutzung (Speicher und CPU) führen und die verstrichenen Zeiten nicht reduzieren. Anwendungen, die die dynamische Abfrage verwenden, sollten überprüft werden, wenn die Verwendung der Master-Detail-Optimierung und die explizite Steuerung der Abfrage erneut verstrichene Zeiten reduzieren können.

Voraussetzungen für gleichzeitige Abfragen

Um gleichzeitig ablaufende Abfragen zu aktivieren, müssen die erweiterten Servereinstellungen und die Ausführungsmethode festgelegt werden.

Bevor Berichtsabfragen gleichzeitig ausgeführt werden können, müssen Sie und der Berichtsersteller die folgenden Tasks ausführen:

- Der Administrator muss Konfigurieren der erweiterten Servereinstellungen für ablaufende Abfragen verwenden.
- Der Berichtsersteller muss die **Ausführungsmethode** -Eigenschaft für die Abfrage in **Gleichzeitig** in der Cognos Analytics-Berichterstellung festlegen.

Parameter für die gleichzeitige Ausführung von Abfragen festlegen

Verwenden Sie die folgende Prozedur, um Parameter für die gleichzeitige Ausführung von Abfragen zu konfigurieren.

Anmerkung:

Eine gleichzeitige Abfrageeinstellung wird ignoriert, wenn

- Eine Abfrage wird von einer Eingabeaufforderungsseite referenziert
- Eine Abfrage wird als Detail in einem Master-Detail-Layout verwendet.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Services konfigurieren" auf Seite 519aus.

2. Konfigurieren Sie für die **ReportService** oder die **BatchReportService**die im Abschnitt „Ausführung ablaufender Abfragen” auf Seite 78beschriebenen Parameter.

   Geben Sie die folgenden Parameter und Werte ein:

Parameter	Wert
RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS	N
RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT	N
RSVP.CONCURRENTQUERY.ENABLEDFORINTERACTIVEOUTPUT	TRUE

3. Klicken Sie auf **OK**.

Abfragepriorisierung festlegen

Sie können Parameter festlegen, die angeben, wie Abfragepriorisierungsarbeiten ausgeführt werden.

Wenn Sie einen Bericht mit definierten Eingabeaufforderungssteuerelementen ausführen, werden alle Parameterinformationen abgerufen, einschließlich Parameterinformationen, die in dem Bericht, dem Modell und der Datenquelle definiert sind. Dies ist für die Dateneingabe und die Ausrichtung von Funktionen für Eingabeaufforderungssteuerungen mit denen des zugehörigen Parameters erforderlich. Diese Operation kann sich auf die Leistung auswirken, insbesondere, wenn es viele oder komplexe Abfragen gibt. Aus der Benutzerperspektive kann es zu lange dauern, bis die erste Eingabeaufforderungsseite oder die erste Berichtsseite vorhanden ist.

Um die Geschwindigkeit zu erhöhen, können Berichtsersteller einen Abfragehinweis in Reporting festlegen, um bei der Bestimmung von Parameterinformationen eine Abfragepriorität zu geben. Abfragen werden auf der Basis der Position, an der sie verwendet werden, und ob sie Filter enthalten, priorisiert. Eine Prioritätsgruppe ist die Gruppe von Abfragen, die ähnliche Attribute gemeinsam nutzen, wie z. B. ein Filter. Anstatt die Parameter für alle Abfragen gleichzeitig abzurufen, werden zunächst Parameter für Abfragen mit der vom Autor definierten Priorität abgerufen, unabhängig davon, wie die automatisierte Abfragepriorisierung festgelegt ist. Weitere Informationen zu Parametern, Filtern und Eingabeaufforderungssteuerelementen finden Sie im *IBM Cognos Analytics - Reporting Benutzerhandbuch*.

Abfragen werden nach Priorität gruppiert, wie in der folgenden Tabelle dargestellt. Wenn eine Abfragengruppe Untergruppen hat, hat die erste Untergruppe Vorrang vor der zweiten Gruppe.

Abfragegruppe	Priorität
Abfragen mit der Eigenschaft **Für Parameterinformationen verwenden** in Reporting auf 'Ja' gesetzt	1
Abfragen mit definierten Filtern, die nicht zum Füllen von Eingabeaufforderungssteuerelementen verwendet werden · Erste Referenz auf solche Abfragen · Nachfolgende Verweise auf solche Abfragen	2
Abfragen mit definierten Filtern, die zum Füllen von Eingabeaufforderungssteuerelementen verwendet werden · Erste Referenz auf solche Abfragen · Nachfolgende Verweise auf solche Abfragen	3

Abfragegruppe	Priorität
Abfragen ohne definierte Filter, die nicht zum Füllen von Eingabeaufforderungssteuerelementen verwendet werden · Erste Referenz auf solche Abfragen · Nachfolgende Verweise auf solche Abfragen	4
Abfragen ohne definierte Filter, die zum Füllen von Eingabeaufforderungssteuerelementen verwendet werden · Erste Referenz auf solche Abfragen · Nachfolgende Verweise auf solche Abfragen	5

Um eine systemweite Konfiguration anzugeben, die definiert, wie Abfragen und Abfragegruppen verarbeitet werden, können Sie der erweiterten Einstellung RSVP.PROMPT.RECONCILIATION. entweder einen Einstellungswert oder einen Namen für die erweiterte Einstellung des Berichtsservers zuordnen. Auf diese Weise können Sie den Grad der Abstimmung zwischen den Eingabeaufforderungssteuerungsfunktionen und dem Datentyp mit der des zugeordneten Parameters angeben. Die Einstellung, die Sie auswählen, legt fest, ob die Genauigkeit oder die Geschwindigkeit der Abstimmung wichtiger ist. Wenn der Berichtsersteller beispielsweise sicherstellt, dass Parameter mit demselben Datentyp und derselben Funktionalität (d. h. Optionalität, Kardinalität und Diskretion) definiert werden, würde die Angabe von CHUNKED oder 3 für alle Abfragen wahrscheinlich die beste Leistung in den unterschiedlichsten Situationen erzielen.

RSVP.PROMPT.RECONCILIATION.CHUNKSIZE ermöglicht die Angabe der Chunkgröße. Diese Einstellung ist anwendbar, wenn CHUNKED GRUPPIERT und CHUNKED verwendet werden. Die Standardblockgröße ist 5.

Die erweiterten Eigenschaften des Berichtsservers und die Hinweise zur Reporting -Abfrage funktionieren kooperativ, um die beste Leistung zu erzielen.

Sie können die in der folgenden Tabelle gezeigten Einstellungen verwenden, um RSVP.PROMPT.RECONCILIATION. zu konfigurieren.

Einstellung	Name	Zweck
0	VOLLSTÄNDIG	Alle Abfragen werden auf einmal gesendet. Das ist die langsamste, präziseste Form der Versöhnung. Dies ist die Standardeinstellung.
1	GRUPPIERT	Abfragen werden von der Prioritätsgruppe gesendet. Diese Einstellung funktioniert am besten für Berichte, die über viele ungefilterte Abfragen und nur wenige gefilterte Abfragen verfügen. Es bietet eine mittlere Geschwindigkeit und eine hohe Aussöhnungsgenauigkeit.
2	CHUNKED GRUPPIERT	Abfragen werden von der Prioritätsgruppe mit einer maximalen Anzahl pro Anforderung gesendet. Die Abfragen erstrecken sich nicht über Gruppen. Diese Einstellung funktioniert am besten in Berichten, die viele Abfragen mit ähnlichen Filterausdrücken haben. Es bietet eine maximale Geschwindigkeit und eine niedrige Abgleichgenauigkeit.
3	CHUNKED	Abfragen werden von der Prioritätsgruppe mit einer maximalen Anzahl pro Anforderung gesendet. Die Abfragen können sich über Gruppen erstrecken.

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf **IBM Cognos Administration** Kapitel 13, „Funktionen”, auf Seite 207verfügen.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Services konfigurieren” auf Seite 519aus.
2. Geben Sie für den **Bericht** -Service in der Spalte **Parameter** einen der in diesem Abschnitt beschriebenen Parameternamen ein.
3. Geben Sie in der Spalte **Wert** einen Wert ein, der der Einstellung zugeordnet ist.
4. Optional: Falls erforderlich, müssen Sie weitere Einstellungen und Werte eingeben.
5. Klicken Sie auf **OK**.
6. Wiederholen Sie dieselben Schritte für die **BatchReportService**.

Konvertierung von numerischen Suchschlüsseln in Zeichenfolgen in Abfragen

Es kann ein Fehler auftreten, wenn Ihre Datenquelle numerische Datenelemente nicht in Zeichenfolgen konvertiert.

Eine Sucheingabeaufforderung ist einer Abfrage zugeordnet, die nicht ausgeführt wird, wenn die Sucheingabeaufforderung das erste Mal wiedergegeben wird. Wenn Sie eine Suchzeichenfolge eingeben, werden die Abfrage gefiltert und die Ergebnisse werden in einem Listenfeld angezeigt. Der Berichtsserver überprüft den Datentyp des gefilterten Abfrageelements nicht, weil die meisten Datenquellen das Datenelement in eine Zeichenfolge (varchar) konvertieren und der Filter gültig wird. Einige Datenquellen, wie z. B. Teradata, machen die Konvertierung jedoch nicht aus, was einen Fehler verursacht.

Die folgende Fehlernachricht wird angezeigt, wenn ein Reporting -oder Query Studio-Bericht ausgeführt wird:

RQP-DEF-0177 Beim Ausführen der Operation 'sqlPrepareWithOptions' status= '-69' UDA-SQL-0043 ist ein Fehler aufgetreten. Die zugrunde liegende Datenbank hat bei der Verarbeitung der SQL-Anforderung einen Fehler festgestellt.[NCR] [ODBC-Teradata-Treiber] [Teradata-Datenbank] Für die Partial-String-Anpassung sind Zeichenoperanden erforderlich.

Um diesen Fehler zu vermeiden, müssen Sie sicherstellen, dass die erweiterte Einstellung **`RSVP.PROMPT.CASTNUMERICSEARCHKEYTOSTRING`** auf `Wahr` (Standardwert) für **ReportService** und **BatchReportService**gesetzt ist. Diese erweiterte Einstellung wird verwendet, um numerische Datenelemente in ein Zeichenfolgeformat (varchar) zu konvertieren. Weitere Informationen zum Konfigurieren erweiterter Einstellungen finden Sie unter „Erweiterte Einstellungen für bestimmte Services konfigurieren” auf Seite 519.

Beispiel für nicht konvertierte Daten

```
[Datenelement] beginnt mit '20'
```

```
[Datenelement] enthält '123'
```

Oder eine boolesche Kombination:

```
[data item] startet mit '2' UND [data item] enthält '009' ODER [data item]
enthält '119'
```

Beispiel für nicht konvertierte Datenelemente mit einer niedrigeren Funktion

Wenn bei der Suche die Groß-/Kleinschreibung nicht beachtet werden muss, enthalten diese Ausdrücke die untere Funktion, die bei der Suche nach Zeichenfolgedatenelementen mehr Sinn ergibt als bei einem numerischen Wert:

```
lower ([data item]) beginnt mit niedriger ('20')

Untere ([Datenelement]) enthält ('123') niedriger

([data item]) beginnt mit niedriger ('2') UND niedriger ([Datenelement])
enthält niedriger ('009') ODER niedriger ([Datenelement]) enthält niedriger
('119')
```

Beispiel für Datenelement, das in eine Zeichenfolge konvertiert wurde

```
gegossen ([data item], varchar (128)) beginnt mit '20'

gegossen ([data item], varchar (128)) enthält '123'

cast ([data item], varchar (128)) starts with '2' AND cast ([data item],
varchar (128)) contains '009' OR cast ([data item], varchar (128)) contains
'119'
```

Sitzungscaching

In Reporting, Query Studio und IBM Cognos Viewer werden die Ergebnisse für vorherige Anforderungen an die Datenbank für die Dauer einer Sitzung zwischengespeichert, wenn das Sitzungscaching aktiviert ist.

Um die Leistung zu erhöhen, verwendet IBM Cognos für nachfolgende Abfragen zwischengespeicherte Ergebnisse für einige Aktionen und nicht für den Zugriff auf die Datenbank. Dies gilt, wenn die gleichen Ergebnisse verwendet werden können oder wenn die neuen Ergebnisse eine Teilmenge der zwischengespeicherten Ergebnisse sind. Sie können das Sitzungscaching auf Serverebene oder auf der Package-oder Berichtsebene inaktivieren.

Da die Leistung möglicherweise beeinträchtigt wird, können Sie das Sitzungscaching auf Serverebene in den folgenden Situationen inaktivieren:

- Benutzer erwarten, dass für jede Abfrage, z. B. neue Datensätze, die in der Zwischenzeit der Datenbank hinzugefügt wurden, für jede Abfrage die Ergebnisse für das Up-to-date direkt aus der Datenbank stammen
- Sie möchten die Häufigkeit begrenzen, mit der auf den Cache während einer Sitzung zugegriffen wird.

Möglicherweise möchten Sie auch das Sitzungscaching für einzelne Berichte inaktivieren, da z. B. der Ressourcenverbrauch hoch ist, z. B. Berichte, die das Bersten verwenden.

Sie können das Sitzungscaching auch für bestimmte Abfragen in Berichten in Reporting (siehe *IBM Cognos Analytics - Reporting Benutzerhandbuch*) und für Modelle in Framework Manager aktivieren und inaktivieren (siehe *IBM Cognos Framework Manager-Benutzerhandbuch*).

Das Sitzungscaching für neue Modelle und Berichte ist standardmäßig aktiviert. Vorhandene Pakete und Berichte behalten die vorhandenen Einstellungen für das Sitzungscaching bei.

Sitzungscaching auf Serverebene inaktivieren

Sie können das Sitzungscaching auf Serverebene inaktivieren.

Vorgehensweise

1. Erstellen Sie im Verzeichnis *Installationsposition*/configuration eine Kopie der CQEConfig.xml.sample -Datei und benennen Sie sie in CQEConfig.xmlum.
2. Öffnen Sie die *Installationsposition*/configuration/CQEConfig.xml -Datei in einem Editor.

   Stellen Sie sicher, dass Ihr Editor das Speichern von Dateien im UTF-8-Format unterstützt.
3. Suchen Sie den Parameter queryReuse in der Datei CQEConfig.xml , und ändern Sie den Wert in 0.
4. Speichern Sie die Datei CQEConfig.xml .

5. Stoppen Sie mit IBM Cognos Konfiguration und starten Sie anschließend den IBM Cognos -Service erneut. Weitere Informationen finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Sitzungscaching auf Paket-oder Berichtsebene inaktivieren

Sie können das Sitzungscaching auf der Paket-oder Berichtsebene inaktivieren.

Vorgehensweise

1. Kopieren Sie die Datei " *Installationsposition*/configuration/CQEConfig.xml.sample" in "install_location/bin" und benennen Sie sie in "CQEConfig.xml" um.
2. Öffnen Sie die Datei *Installationsposition*/bin/CQEConfig.xml in einem Editor.
3. Stellen Sie sicher, dass Ihr Editor das Speichern von Dateien im UTF-8-Format unterstützt.
4. Suchen Sie den Parameter `queryReuse` und entfernen Sie ihn.
5. Speichern Sie die Datei CQEConfig.xml.
6. Using IBM Cognos Configuration, stop and then restart IBM Cognos software. Informationen hierzu finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Aktivieren des Parameters 'HTTPOnly' zur Sicherung des CAM-Passport-Cookies

CAM-Pass identifiziert die Web-Browser-Sitzung des Benutzers mit dem Server. Administratoren können das Attribut HTTPOnly festlegen, um Scripts beim Lesen oder Manipulieren des CAM-Passport-Cookies während der Sitzung eines Benutzers mit dem Web-Browser zu blockieren.

Informationen zu diesem Vorgang

Das Aktivieren des Attributs HTTPOnly verhindert, dass zerstörerische Scripts die Sitzungs-ID des Benutzers stehlen. Wenn ein Administrator dieses Attribut festlegt, kann der Web-Browser das Sitzungscookie nur verwenden, um HTTP-Anforderungen an den Server zu senden.

Wenn Sie das Attribut "HTTPOnly" aktivieren möchten, müssen Sie sicherstellen, dass die Benutzer über einen Web-Browser verfügen, der dieses Attribut unterstützt.

Vorgehensweise

1. Rufen Sie die IBM Cognos Administration auf.
2. Klicken Sie auf der Registerkarte **Status** auf **System**.
3. Klicken Sie im **Scorecard** -Fenster im Dropdown-Menü **System** auf **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Wählen Sie in der Liste **Kategorie** die Option **Umwelt**aus.
6. Wählen Sie für den Parameter **HTTPOnly-Cookie-Unterstützung** das entsprechende Kontrollkästchen in der Spalte **Wert** aus.
7. Klicken Sie auf **OK**.

Dezimalgenauigkeit reduzieren

Sie können Dezimalgenauigkeit in Kreuztabellenberichten festlegen.

In einem Kreuztabellenbericht unterstützen Werte maximal 18 Ziffern und das Dezimalzeichen. Die Dezimalgenauigkeit bestimmt die Anzahl der Ziffern, die reserviert werden, um die Dezimalkomponente einer Zahl auszudrücken. Die übrigen Ziffern sind reserviert, um die ganzzahlige Komponente der Zahl

auszudrücken. Standardmäßig wird die Dezimalgenauigkeit auf 7 Ziffern gesetzt, was die Länge von Ganzzahlen auf 11 Ziffern beschränkt.

Wenn Sie mehr als 11 ganze Zahlen reservieren möchten, um die ganzzahlige Komponente einer Zahl auszudrücken, müssen Sie die Dezimalgenauigkeit reduzieren. Sie können z. B. die Dezimalgenauigkeit auf 2 setzen, wodurch Sie bis zu 16 Ziffern für die ganzzahlige Komponente einer Zahl reservieren können.

Vorgehensweise

1. Suchen Sie in dem Verzeichnis *Installationsposition*\configuration die Datei 'qfs_config.xml'.
2. Kopieren Sie die Datei 'qfs_config.xml' und benennen Sie die kopierte Datei in 'qfs_config.xml.backup' um.
3. Öffnen Sie die ursprüngliche Datei "qfs_config.xml", und suchen Sie die folgende Codezeile:

   ```
   <provider name="CubeBuildProvider"libraryName="qfsCubeBuildProvider"
   serviceProvider="true">
       <providerDetails>
   ```

4. Fügen Sie für das Element `providerDetails` die folgende Zeile hinzu:

   ```
   <scaleOfFloatDouble value="n"/>
   ```

   Dabei steht "n" für den dezimalen Genauigkeitswert, den Sie angeben möchten.

   Der Standardwert ist 7.
5. Speichern Sie die Datei 'qfs_config.xml'.
6. Starten Sie den IBM Cognos -Service erneut.

Externer Objektspeicher zum lokalen Speichern der Berichtsausgabe

Sie können Content Manager so konfigurieren, dass Berichtsausgaben auf einem lokalen Laufwerk oder einem lokalen Netzwerk gespeichert werden, indem Sie einen externen Objektspeicher definieren.

Durch die Verwendung eines externen Objektspeichers für die Berichtsausgabe wird die Größe des Content-Stores reduziert und Leistungsverbesserungen für Content Manager bereitgestellt.

Weitere Informationen zum Einrichten eines externen Objektspeichers finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Gespeicherte Berichtsausgabe

Sie können angeben, wo Kopien von Berichtsausgabedateien gespeichert werden sollen.

Die folgenden Berichtsausgabeformate können gespeichert werden: PDF, CSV, XML, Microsoft Excel 2002, 2007 und 2007 Daten, und HTML, das keine integrierte Grafik enthält.

Sie können die gespeicherten Berichtsausgabedateien gemeinsam mit externen Anwendungen oder mit Benutzern gemeinsam nutzen, die keinen Zugriff auf IBM Cognos -Software haben.

Sie haben die folgenden Optionen, um Berichtsausgabedateien zu speichern:

- Eine Position außerhalb der IBM Cognos -Software

  Mit dieser Option können die Benutzer steuern, welche Berichtsausgabedateien in dem Dateisystem gespeichert werden. Weitere Informationen finden Sie unter „Berichtsausgabedateien außerhalb von IBM Cognos -Software speichern“ auf Seite 88.
- Eine Position in der IBM Cognos -Software

  Mit dieser Option werden alle Berichtsausgabedateien an derselben Dateisystemposition gespeichert, die in Content Manager definiert ist. Dies macht diese Option für Implementierungszwecke nützlich.

Eine Deskriptordatei mit einer `_desc` -Erweiterung, die mit dieser Option erstellt wird, enthält nützliche Informationen für IBM oder die Archivsoftware von Drittanbietern.

Diese Option ermöglicht auch die Ausführung eines vordefinierten Scripts für jede Ausgabedatei, die bei der Integration von Fremdanbietern unterstützt wird.

Weitere Informationen finden Sie unter „Berichtsausgabedateien in IBM Cognos -Software speichern" auf Seite 89 .

Beide Optionen zum Speichern von Berichtsausgabedateien sind unabhängig voneinander, können aber gleichzeitig verwendet werden.

Berichtsausgabedateien außerhalb von IBM Cognos -Software speichern

Berichtsausgabedateien können in einem Dateisystem außerhalb der IBM Cognos -Software gespeichert werden. Benutzer können auswählen, welche Ausgabedateien gespeichert werden sollen.

Informationen zu diesem Vorgang

Diese Option ist nützlich, wenn Benutzer Berichte mit einer externen Anwendung, wie z. B. einer Website, gemeinsam nutzen möchten. Die Berichte werden jedes Mal, wenn sie aktualisiert werden, an dieser Position gespeichert, sodass der aktuelle Inhalt immer verfügbar ist. Sie können Berichte auch in einem lokalen Netz für Benutzer speichern, die keinen Zugriff auf IBM Cognos -Software haben.

Für die Dispatcher und Services können mehrere Standorte angegeben werden.

Vorgehensweise

1. Erstellen Sie ein Verzeichnis, in dem die Berichtsausgaben gespeichert werden sollen.
2. Aktivieren Sie das Speichern der Berichtsausgabe in das Dateisystem.
   a) Starten Sie Cognos Configuration.
   b) Klicken Sie auf **Aktionen** > **Globale Konfiguration bearbeiten**.
   c) Geben Sie auf der Registerkarte **Allgemein** den Pfad zu dem Verzeichnis ein, das Sie in **Dateisystemstammverzeichnis für Archivposition**erstellt haben.

      Der Pfad muss das Format von `file: // (file-system-path)`haben. Beispiel: `file://C: / reports`.
   d) Klicken Sie auf **OK**.
   e) Erweitern Sie im Fenster **Explorer** den Eintrag **Datenzugriff**, und klicken Sie auf **Content Manager**.
   f) Setzen Sie **Berichtsausgaben in einem Dateisystem speichern** auf **Wahr**.
   g) Klicken Sie im Fenster **Explorer** auf **Umwelt**, und stellen Sie sicher, dass der Servername oder die IP-Adresse in den URI-Einstellungen verwendet wird. Die Verwendung von `Localhost` in den URI-Einstellungen kann zu Fehlern führen, wenn Sie die Berichtsausgabe in einem gemeinsam genutzten Verzeichnis speichern.
   h) Klicken Sie auf **Datei** > **Speichern**.
   i) Starten Sie die IBM Cognos -Services erneut.
3. Aktivieren Sie das Speichern von Berichten in IBM Cognos Administration.
   a) Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Dispatcher und Services**.
   b) Klicken Sie in der Symbolleiste auf das Symbol **Dateisystempositionen definieren**  .
   c) Klicken Sie auf **Neu**, und geben Sie dann einen Namen, eine Beschreibung und eine Anzeigenspitze ein.
   d) Geben Sie in das Feld **Dateisystemposition** den Pfad zu dem Verzeichnis ein, das Sie in Schritt 1 erstellt haben.

e) Klicken Sie auf **Fertigstellen**.

4. Wählen Sie die Ausgabeposition für einen Bericht aus.
   a) Wählen Sie im Ordner **Teaminhalt** oder **Mein Inhalt** einen Bericht aus, klicken Sie auf die Schaltfläche mit den Auslassungspunkten, und wählen Sie dann **Eigenschaften**aus.
   b) Klicken Sie auf die Registerkarte **Zeitplan** .
   c) Wählen Sie im Abschnitt **Optionen** die Option **Standardwerte überschreiben**aus.
   d) Aktivieren Sie im Abschnitt **Zustellung** die Option **In Dateisystem speichern**und klicken Sie auf **Optionen bearbeiten**.
   e) Wählen Sie auf der Seite "Optionen" in **Position**die Ausgabeposition aus.
   f) Klicken Sie auf **OK**.

Nächste Schritte

Wenn Benutzer **Bericht als externe Datei speichern** als Berichtsbereitstellungsmethode auswählen, wenn sie einen Bericht ausführen oder planen, werden die Berichtsausgabedateien an dieser Position gespeichert.

Berichtsausgabedateien in IBM Cognos -Software speichern

Benutzer können Kopien von Berichtsausgabedateien in der IBM Cognos -Software speichern. Alle Berichtsausgabedateien werden an einer Position gespeichert, die in Content Manager angegeben ist.

Vorbereitende Schritte

Bevor Sie diese Funktionalität verwenden, müssen Sie die Eigenschaft **Berichtsausgaben in einem Dateisystem speichern** in IBM Cognos auf 'true' setzen. Weitere Informationen finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Informationen zu diesem Vorgang

Sie müssen eine Position in Content Manager angeben, in der Kopien der Berichtsausgabedateien gespeichert werden. Die Position bezieht sich auf die gespeicherte Ausgabe, die aus dem ausgewählten Content Manager-Service stammt. Diese Position wird durch den Parameter **`CM.OutPutLocation`** dargestellt.

Wenn Sie einen Bericht speichern, der auf diese Weise ausgegeben wird, wird auch eine XML-Deskriptordatei für die Ausgabedatei erstellt. Die Deskriptordatei enthält Informationen zur Berichtsausgabe, wie z. B. den Namen, die Ländereinstellung, die Erstellungszeit, den Burstschlüssel, den Suchpfad für den zugehörigen Bericht und den Berichtsversionskontakt. Die Deskriptordatei verwendet den Namen der Ausgabedatei mit dem hinzugefügten Suffix `_desc`. Ein gespeicherter PDF-Bericht mit dem Namen 158_1075940415360.pdf hat beispielsweise eine Deskriptordatei mit dem Namen 158_1075940415360_desc.xml.

Sie können auch ein Script angeben, damit nach der Verarbeitung von Befehlen jedes Mal, wenn eine Berichtsausgabe in das Dateisystem kopiert wird, ausgeführt werden kann.

Berichtsausgaben werden immer in das Verzeichnis geschrieben, das für die einzelnen Delivery Service-Instanzen konfiguriert ist. Um zu vermeiden, dass Berichtsausgaben an mehrere Positionen geschrieben werden, stellen Sie sicher, dass Sie entweder nur eine Instanz des Bereitstellungsservice ausführen oder alle Serviceinstanzen für die Verwendung einer gemeinsam genutzten Netzdateiposition konfigurieren. Jeder Dispatcher, auf dem der Bereitstellungsservice ausgeführt wird, muss Zugriff auf das Dateisystem haben oder auf allen Systemen inaktiviert sein, die nicht zum Speichern der Berichtsausgabe bestimmt sind.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Services konfigurieren” auf Seite 519aus.
2. Definieren Sie für die **ContentManagerService**die folgenden Parameter:
   - **CM.OutPutLocation**

     Gibt eine Position in der IBM Cognos -Software an, in der Kopien von Berichtsausgabedateien gespeichert werden. Alte Berichtsversionen werden von dieser Position nicht gelöscht, wenn neue Versionen gespeichert werden. Diese Position muss ordnungsgemäß verwaltet werden, so dass nur ausgewählte Berichtsversionen aufbewahrt werden.

     Dieser Parameter ist obligatorisch, wenn Sie Berichtsausgabedateien in der IBM Cognos -Software speichern möchten.
   - **CM.OutputScript**

     Gibt die Position und den Namen eines Shell-Scripts an, wie z. B. eine .bat-oder .sh-Datei, die ausgeführt wird, nachdem die Berichtsausgabe in dem Zielverzeichnis gespeichert wurde. Die vollständigen Namen der Berichtsausgabedatei und der zugehörigen Deskriptordatei werden an das Script übergeben. Dieser Parameter ist optional.
   - **CM.OutputByBurstKey**

     Dieser Parameter ist anwendbar, wenn die Berichtsausgabe durch Bersten verteilt wird. Sie gibt an, ob Berichtsausgabedateien in einem Unterverzeichnis mit demselben Namen wie der Burstschlüssel gespeichert werden sollen. Der Standardwert ist 'false', was bedeutet, dass die Ausgabe nicht von den Burstschlüsseln gespeichert wird.

Bericht-und Stapelberichtsservices für die Verwendung großer Arbeitsblätter konfigurieren

Administratoren können die Unterstützung für große Arbeitsblätter von Microsoft Excel 2007 aktivieren. Wenn dies geschehen ist, werden Arbeitsblätter mit bis zu 1 048 576 Zeilen unterstützt.

Um die Unterstützung für große Arbeitsblätter zu aktivieren, geben Sie die erweiterte Einstellung **RSVP.EXCEL.EXCEL_2007_LARGE_ARBEITSBLATT** für die **ReportService** und die **BatchReportService**an. Wenn die Einstellung **RSVP.EXCEL.EXCEL_2007_LARGE_ARBEITSBLATT** angegeben wird, können auch die folgenden Einstellungen angegeben werden:

- **RSVP.EXCEL.EXCEL_2007_WORKSHEET_MAXIMUM_ROWS**

  Gibt die Anzahl der Zeilen an, die ausgegeben werden sollen, bevor sie in ein neues Arbeitsblatt versetzt werden.
- **RSVP.EXCEL.EXCEL_2007_OUTPUT_FRAGMENT_SIZE**

  Passt die interne Speicherfragmentgröße in Zeilen an, die der IBM Cognos Analytics -Server generiert, bevor er auf eine Platte gelöscht wird. Wenn dieser Wert nicht angegeben wird, beträgt der Standardwert ungefähr 45 000 Zeilen. Diese Eigenschaft kann nützlich sein, wenn Probleme auftreten, z. B. bei der Ausführung von Speicherausgriffen, wenn Berichte mit dem Standardwert generiert werden. Möglicherweise müssen die Werte gesenkt werden, damit der Bericht erfolgreich ausgeführt werden kann.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Services konfigurieren” auf Seite 519aus.
2. Geben Sie für den **ReportService**in der Spalte **Parameter** den Wert **RSVP.EXCEL.EXCEL_2007_LARGE_ARBEITSBLATT**ein.
3. Geben Sie in der Spalte **Wert** den Wert true ein.

4. Geben Sie die Einstellungen für **RSVP.EXCEL.EXCEL_2007_WORKSHEET_MAXIMUM_ROWS** und **RSVP.EXCEL.EXCEL_2007_OUTPUT_FRAGMENT_SIZE** in ähnlicher Weise an und geben Sie die erforderlichen Werte für diese Einstellungen ein.
5. Klicken Sie auf **OK**.
6. Wiederholen Sie dieselben Schritte für die **BatchReportService**.

Arbeitsblatt-Registerkarten in Excel 2007-Berichten dynamisch benennen

Wenn in IBM Cognos Analyticsdie erweiterte Eigenschaft RSVP.EXCEL.PAGEGROUP_WSNAME_ITEMVALUE auf "true" gesetzt ist, werden die Registerkarten in Excel 2007-Ausgabe dynamisch entsprechend den angegebenen Seitenumbrüchen benannt.

Anmerkung: Diese Eigenschaft gilt nicht für Analysis Studio.

Informationen zu diesem Vorgang

Wenn Seitenumbrüche durch Produktlinie angegeben werden, haben die Arbeitsblattregisterkarten entsprechende Namen. Zum Beispiel haben Seiten, die mit den Produktlinien Camping Equipment, Mountaineering Equipment, Personal Accessories, Outdoor Protection und Golf Equipment gebrochen sind, Tabs mit den gleichen Namen.

Weitere Informationen zu Registerkartennamen, wenn Berichte zwei Seitengruppen enthalten, die Produktlinie als Gruppierungselement verwenden, oder verschachtelte Seitengruppen enthalten, finden Sie in der *IBM Cognos Reporting Benutzerhandbuch*.

Vorgehensweise

1. Führen Sie die Schritte im Thema „Erweiterte Einstellungen für bestimmte Services konfigurieren” auf Seite 519aus.
2. Geben Sie auf der **Erweiterte Einstellungen festlegen-ReportService** -Seite in der Spalte **Parameter** den Wert `RSVP.EXCEL.PAGEGROUP_WSNAME_ITEMVALUE`ein.
3. Geben Sie in der Spalte **Wert** den Wert `Wahr`ein.

Lineage-Lösung konfigurieren

Die Abstammung enthält Details zu den Daten in einem Bericht, wie z. B. die Datenquelle und die Berechnungsausdrücke. Sie können die IBM Cognos -Standardsoftwareabstammungslösung, das IBM InfoSphere Information Governance Catalog-Abstammungswerkzeug oder eine angepasste Abstammungslösung konfigurieren.

Sie können auf Abstammungsinformationen in IBM Cognos Viewer, Reporting, Query Studio und Analysis Studio zugreifen. To use the default solution or IBM InfoSphere Information Governance Catalog, ensure that the value for the **URI des Metadateninformationsservice** parameter of the **Umwelt** category is configured as specified in the steps in this section.

Um eine angepasste Abstammungslösung implementieren zu können, müssen Sie

- Erstellen Sie eine Webschnittstelle, die die Anforderungsparameter für die Softwareabstammungsanforderung von IBM Cognos übersetzt und die angepasste Linienlösung aufruft.

  Weitere Informationen finden Sie im Abschnitt über die Integration einer angepassten Abstammungslösung in der *IBM Cognos Software Development Kit Developer Guide*.
- Ändern Sie den Wert für den Parameter **URI des Metadateninformationsservice** der Kategorie **Umwelt** in die URL Ihres Abstammungsservers.

Vorbereitende Schritte

Die Funktion **Lineage** muss aktiviert sein. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen”, auf Seite 207und Kapitel 14, „Objektfunktionalität”, auf Seite 219.

Anmerkung: Eine Liste der unterstützten Versionen von InfoSphere Information Server finden Sie im Handbuch Cognos Analytics Software-Produktkompatibilitätsberichte.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Menü 'Aktionen' von **System** auf **Eigenschaften festlegen**.
3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Geben Sie für die **Umwelt** -Kategorie **URI des Metadateninformationsservice**einen der folgenden Werte ein.
   - Wenn Sie die Standardlösung für die IBM Cognos -Softwareabstammungslösung konfigurieren möchten, geben Sie **/lineageUIService**ein.

     Wenn dieser Wert bereits angegeben ist, klicken Sie auf **Abbrechen**. Sie müssen nichts ändern.
   - Wenn Sie IBM InfoSphere Information Governance Catalog als Lineage-Lösung konfigurieren möchten, geben Sie die URL wie folgt ein:

     /lineageUIService? iis=https://*Igc_servername*: 9080/ibm/iis/igc#cognosLineage/*cognos_servername*

     Dabei ist https://*Igc_servername*: 9080/ibm/iis/igc#cognosLineage/*cognos_servername* die URL, auf die der Zugriff auf IBM InfoSphere Information Governance Catalog im Netz möglich ist.

     Igc_servername steht für den Servernamen, in dem IBM InfoSphere Information Governance Catalog installiert ist.

     – Um eine Kombination aus Cognos -Abstammung und InfoSphere Information Governance Catalog-Abstammung zu nutzen, gibt es einen zusätzlichen Parameter, der konfiguriert werden soll. Ein "launchPoint" -Parametersatz mit dem Wert "indirekt" gibt an, dass Cognos -Abstammungslinien für die Abstammung der Cognos -Ebene verwendet werden sollen (d. h. Berichts-und Modellebeneninformationen) und der Information-Governance-Katalog verwendet werden kann, um die Abstammungslinie für die Datenquelle zu untersuchen. Durch Klicken auf das Datenquellenobjekt in der Cognos -Abstammungsanzeigefunktion wird IBM InfoSphere Information Governance Catalog aufgerufen, um die Abstammungsinformationen für die Datenquelle in der Tiefe zu untersuchen.

       /lineageUIService? launchPoint=indirekte & iis=*Information_Governance_Catalog_URL*

       Beispiel: /lineageUIService? launchPoint=indirekt & iis=https://*Igc_servername*: 9080/ibm/iis/igc#cognosLineage/*cognos_servername*

       Igc_servername steht für den Servernamen, in dem IBM InfoSphere Information Governance Catalog installiert ist.
   - Wenn Sie eine angepasste Abstammungslösung konfigurieren möchten, ersetzen Sie den vorhandenen Wert durch den URI, der Ihre Abstammungswebschnittstelle darstellt.

     Geben Sie zum Beispiel https://mycompany.com/ourLineageService.cgi ein.
5. Klicken Sie auf **OK**.

InfoSphere Business Glossary-URI konfigurieren

Für den Zugriff auf das IBM InfoSphere Business Glossary aus dem Viewer in IBM Cognos Analytics und aus der Metadatenbaumstruktur in Reporting, Query Studio und Analysis Studio müssen Sie den URI der Glossarwebseite angeben.

Standardmäßig geben die GlossarSuchergebnisse in der Cognos -Software nur Begriffe zurück, die das in der Suche angegebene Schlüsselwort enthalten. Andere Arten von Assets werden nicht zurückgegeben.

Weitere Informationen finden Sie unter „Zugriff auf das InfoSphere Business Glossary" auf Seite 367.

Vorbereitende Schritte

Für den Zugriff auf das Business-Glossar von InfoSphere müssen Benutzer über Berechtigungen für die Funktionalität von **Glossar** verfügen. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen", auf Seite 207und Kapitel 14, „Objektfunktionalität", auf Seite 219.

Vorgehensweise

1. Öffnen Sie **IBM Cognos Administration**von **Verwalten** > **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Status** auf **System**.
3. Klicken Sie für **System**auf das Menü **Aktionen** , und klicken Sie dann auf **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Geben Sie für die Kategorie **Umwelt IBM Business Glossary-URI**den folgenden URI ein: `https://Igc_servername:Portnummer/ibm/iis/igc/popup/popupSearch.do?exactMatch=1`

   Geben Sie beispielsweise `https://Igc_servername: 9080/ibm/iis/igc/popup/popupSearch.do?exactMatch=1` ein.
6. 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 Connections 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.

Um auf die Homepage und die Aktivitäten-Seite von IBM Connections zugreifen zu können, muss der Administrator die Funktionalität von **Zusammenarbeiten** aktivieren. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen", auf Seite 207.

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**.

Messwerte für Job-, SMTP-und Taskwarteschlange aktivieren

Standardmäßig ist nur die Messgröße für die Warteschlangenlänge für Job-, Task-und SMTP-Warteschlangenmetriken aktiviert. Andere Metriken sind auch für jeden verfügbar, werden jedoch auf null gesetzt und erscheinen nicht in der Benutzerschnittstelle, sofern Sie sie nicht aktivieren.

- **Zeit in Warteschlangenhochwasserzeichen**
- **Zeit in Warteschlange mit niedrigem Wasserzeichen**
- **Zeit in Warteschlange**
- **Anzahl Warteschlangenanforderungen**
- **Hochwasserzeichen für Warteschlangenlänge**
- **Untere Grenze für Warteschlangenlänge**

Weitere Informationen zu diesen Metriken finden Sie unter Kapitel 4, „Systemleistungsmetriken”, auf Seite 25. Beachten Sie, dass die Aktivierung dieser Einstellungen die Leistung beeinträchtigen kann.

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Siehe Kapitel 13, „Funktionen”, auf Seite 207.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Menü 'Aktionen' von **System** auf **Eigenschaften festlegen**.
3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Klicken Sie für die Kategorie **Umwelt** neben **Erweiterte Einstellungen**auf den Link **Bearbeiten** .
5. Wenn sie angezeigt wird, wählen Sie das Kontrollkästchen **Über den übergeordneten Eintrag erfasste Einstellungen außer Kraft setzen** aus. Fahren Sie andernfalls mit dem nächsten Schritt fort.
6. Geben Sie in der Spalte **Parameter** die folgenden Einstellungen ein: **enable.tide.metrics.smtpqueue**, **enable.tide.metrics.jobqueue**und **enable.tide.metrics.taskqueue**.
7. Geben Sie neben jedem Parameter in der Spalte **Wert** den Wert **Wahr** ein, um den Messwert zu aktivieren.
8. Klicken Sie auf **OK**.
9. Öffnen Sie die Datei *Installationsposition*/webapps/p2pd/WEB-INF/classes/iManage-metadata.xml in einem Editor.

   Stellen Sie sicher, dass Ihr Editor das Speichern von Dateien im UTF-8-Format unterstützt.

   Für eine verteilte Installation müssen Sie die Datei "iManage-metadata.xml" auf jedem Computer bearbeiten. Andernfalls können die globalen Messwerte zunächst angezeigt werden, aber nach der Navigation von der Seite nicht persistent bleiben.

10. Entfernen Sie die Kommentarzeichen für die Abschnitte, die mit `<! -- beginnen. Diese Metriken wurden explizit inaktiviert. Bitte konsultieren Sie die Dokumentation, wie Sie sie aktivieren können. -- >`
11. Speichern Sie die Datei.
12. Using IBM Cognos Configuration, stop and then restart IBM Cognos software.

    Informationen zum Stoppen von IBM Cognos -Software finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Lebensdauer der abgeschlossenen Benutzertasks und Anmerkungen festlegen (Kommentare)

Sie können die Lebensdauer von abgeschlossenen Annotationen und Benutzertasks festlegen.

Die Lebensdauer ist die Zeitdauer, nach der der zugeordnete Eintrag gelöscht wird. Wenn die Lebensdauer für eine Anmerkung beispielsweise auf 60 Tage gesetzt ist, wird die Anmerkung 60 Tage nach dem Löschen des zugeordneten Berichts gelöscht. Wenn die Lebensdauer für eine Benutzertask auf 120 gesetzt ist, wird die Benutzertask möglicherweise 120 Tage gelöscht, wenn alle verknüpften Berichte oder Dashboards gelöscht werden.

Die Standardlebensdauer beträgt 90 Tage für abgeschlossene Benutzertasks und 180 Tage für abgeschlossene Anmerkungen.

Weitere Informationen zu Benutzertasks finden Sie unter Kapitel 25, „Menschliche Aufgaben verwalten”, auf Seite 375. Weitere Informationen zu Anmerkungen (Kommentare) finden Sie im *IBM Cognos Arbeitsbereich 'Benutzerhandbuch'*.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Dienstleistungen** > **Benutzertaskservice** oder **Dienstleistungen** > **Anmerkungsservice**.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im Menü **Aktionen** des Service auf **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Suchen Sie bei Anmerkungen die Einstellung **Lebensdauer der Anmerkung abgeschlossen**. Suchen Sie für **HumanTaskService**die Einstellung **Lebensdauer der Benutzertask abgeschlossen**. Legen Sie die Lebensdauer in Tagen oder Monaten fest und klicken Sie auf **OK**.

Ergebnisse

Abgeschlossene Anmerkungen oder Benutzertasks werden nach der von Ihnen angegebenen Anzahl von Tagen gelöscht.

Drillthrough-Filterverhalten ändern

Sie können das Verhalten des dynamischen Drillthrough-Filters ändern, wenn Sie einen Drillthrough durchführen möchten, um einen Filter mit dem Member Business Key anstelle der Standardmitgliedskaption zu generieren.

Setzen Sie den Parameter RSVP.DRILL.DynamicFilterUsesBusinessKey auf 0, um die Member Caption zu verwenden. Setzen Sie diese Option auf 1, um den Business Key zu verwenden.

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf die **IBM Cognos Administration** -Funktionalität verfügen. Siehe Kapitel 13, „Funktionen”, auf Seite 207.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Dienstleistungen** > **Bericht**oder auf **Dienstleistungen** > **Stapelbericht**.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. From the **ReportService** or **BatchReport-Service**, **Aktionen** menu and click **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Klicken Sie neben **Erweiterte Einstellungen**auf **Bearbeiten** .
6. Wählen Sie **Über den übergeordneten Eintrag erfasste Einstellungen außer Kraft setzen**aus.
7. Geben Sie in der Spalte **Parameter** den Wert RSVP.DRILL.DynamicFilterUsesBusinessKeyein.
8. Geben Sie in der Spalte **Wert** den zugeordneten Wert für die Einstellung ein.
9. Klicken Sie auf **OK**.
10. Klicken Sie auf der **Eigenschaften festlegen** -Seite auf **OK**.

Steuern, ob URL-Parameter an Content Manager gesendet werden

Bei Leistungserwägungen werden URL-Parameter nicht in Abfragen an Content Manager eingeschlossen.

Es können jedoch z. B. URL-Parameter erforderlich sein, um Single Sign-on bei Authentifizierungsprovidern zu vermeiden. Wenn URL-Parameter erforderlich sind, können Sie diese angeben, indem Sie den **forwardURLParamsToCM** auf 'true' setzen.

Die Standardeinstellung für diesen Parameter ist 'false'.

Vorgehensweise

1. Klicken Sie in der IBM Cognos Administration auf **Konfiguration** > **Dispatcher und Services**.
2. Gehen Sie wie folgt vor, um die Einstellung **forwardURLParamsToCM** für einen einzelnen Dispatcher anzugeben:
   a) Klicken Sie in der Spalte **Name** auf einen Dispatcher, und klicken Sie auf **Eigenschaften festlegen**.
   b) Rufen Sie die **PresentationService**auf und klicken Sie auf **Eigenschaften festlegen**.
   c) Klicken Sie auf die Registerkarte **Einstellungen** , und klicken Sie für **Umwelt**, **Erweiterte Einstellungen**auf **Bearbeiten**.
   d) Klicken Sie auf **Über den übergeordneten Eintrag erfasste Einstellungen außer Kraft setzen**. Fahren Sie mit Schritt 4 fort.
3. Gehen Sie wie folgt vor, um den globalen Parameter **forwardURLParamsToCM** für mehrere Dispatcher anzugeben:
   a) Klicken Sie in der Symbolleiste von **Konfiguration** auf **Eigenschaften festlegen-Konfiguration**.
   b) Klicken Sie auf die Registerkarte **Einstellungen** , und klicken Sie für **Umwelt**, **Erweiterte Einstellungen**auf **Bearbeiten**.
4. Geben Sie **forwardURLParamsToCM**in das Feld **Parameter** ein und geben Sie im Feld **Wert** den Wert **Wahr**ein.
5. Klicken Sie auf **OK**.

Von UNIX -Betriebssystemen drucken

Die Eigenschaft RSVP.PRINT.POSTSCRIPT steuert, welche Schnittstelle zum Drucken von PDF-Dokumenten aus einem UNIX -Betriebssystem verwendet werden soll. Wenn Sie mit der Adobe -Acrobat-PDF-Schnittstelle fortfahren möchten, setzen Sie den Wert dieser Eigenschaft auf "false".

Die Eigenschaft RSVP.PRINT.POSTSCRIPT gilt nur für UNIX -Betriebssysteme, und ihr Standardwert ist 'true'. Die Beibehaltung des Standardwerts bietet Benutzern die Möglichkeit, PDFs über die interne Postscript-Schnittstelle von einem UNIX -Betriebssystem zu drucken.

Bevor Sie den Eigenschaftswert RSVP.PRINT.POSTSCRIPT in 'false' ändern, müssen Sie sicherstellen, dass Sie die neueste Version von Adobe Acrobat Reader für Ihr Betriebssystem installiert haben.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Services konfigurieren" auf Seite 519aus.
2. Geben Sie für den **BatchReportService**in der Spalte **Parameter** den Wert **`RSVP.PRINT.POSTSCRIPT`**ein.
3. Geben Sie in der Spalte **Wert** den Wert false ein.
4. Klicken Sie auf **OK**.

Cognos -Arbeitsbereichsdomänen zur gültigen Domänenliste hinzufügen

Sie müssen gültige Domänen für URLs in Toolboxwidgets in IBM Cognos Workspace verwenden. Fügen Sie die Domänen hinzu, die von Cognos Workspace-Benutzern für die Liste der gültigen Domänen verwendet werden.

Vorgehensweise

1. Klicken Sie in der IBM Cognos Administration auf **Konfiguration** > **Dispatcher und Services**.
2. Klicken Sie auf das Symbol **Eigenschaften festlegen**  .
3. Öffnen Sie die Registerkarte **Einstellungen** .
4. Wählen Sie die **Erweiterte Einstellungen** aus und klicken Sie auf **Bearbeiten**.
5. Fügen Sie den Parameter **`BUXClientValidDomainList`**hinzu.
6. Fügen Sie in der Spalte **Wert** die Domänen in einer durch Kommas getrennten Liste hinzu.

Verhindern von Content-Store-Sperren, wenn Sie zahlreiche Zeitpläne hinzufügen oder aktualisieren

Wenn in IBM Cognos Analyticszahlreiche Zeitpläne hinzugefügt oder aktualisiert werden, kann die Content-Store-Datenbank sperren, wenn die Zeitpläne ungültige Daten enthalten. Wenn dieses Problem auftritt, können Sie eine erweiterte Eigenschaft festlegen, die die Zeitplaneigenschaften überprüft und ungültige Zeitpläne inaktiviert.

Informationen zu diesem Vorgang

Zeitpläne, die ungültige Daten enthalten, können die Content-Store-Datenbank sperren. Ein Zeitplan kann beispielsweise ungültige Berechtigungsnachweise für den Benutzeraccount enthalten. Wenn Sie Zeitpläne hinzufügen oder aktualisieren und die Berechtigungsnachweiseigenschaft auf ungültige Berechtigungsnachweise für den Benutzeraccount verweist, versucht Content Manager wiederholt, ungültige Zeitpläne ohne Erfolg zu aktualisieren.

Wenn die Eigenschaft emf.schedule.validation.enabled auf 'true' gesetzt ist, werden Zeitplaneigenschaften wie Startdatum, Enddatum, Datentypen und Benutzeraccountberechtigungsnachweise geprüft. Ungültige Zeitpläne, die festgestellt werden, sind inaktiviert, und Details zu den inaktivierten Zeitplänen werden in den Protokolldateien protokolliert.

Der Standardwert für diese Eigenschaft ist 'false'. Um die Zeitplanvalidierung zu aktivieren, setzen Sie die Eigenschaft auf 'true'.

Vorgehensweise

1. Führen Sie die Schritte in dem Thema „Erweiterte Einstellungen für bestimmte Services konfigurieren” auf Seite 519aus.
2. Wählen Sie in der Liste der Dispatcherservices die Option **EventManagementService**aus.
3. Klicken Sie für die **Umwelt** -Konfigurationseinstellung in der Spalte **Wert** auf **Bearbeiten**.
4. Um den Parameternamen hinzuzufügen, geben Sie `emf.schedule.validation.enabled`ein.
5. Um den Wert hinzuzufügen, geben Sie `Wahr`ein.

Kapitel 6. Datenquellen und Verbindungen

Eine Datenquelle definiert die physische Verbindung zu einer Datenbank. IBM Cognos Analytics unterstützt mehrere relationale, OLAP-und DMR-Datenquellen.

Die Datenquellenverbindung gibt die Parameter an, die zum Herstellen einer Verbindung zur Datenbank erforderlich sind, wie z. B. die Position der Datenbank und die Zeitlimitdauer. Eine Datenquellenverbindung kann Berechtigungsnachweisdaten und eine Anmeldedaten enthalten. Eine Datenquelle kann über mehrere Verbindungen verfügen.

Sie können eine oder mehrere Datenquellen verfügbar machen, indem Sie sie zusammen mit anderen Elementen in Paketen kombinieren, die mit Framework Manager erstellt und veröffentlicht werden. Anweisungen zum Erstellen von Paketen finden Sie im *IBM Cognos Framework Manager-Benutzerhandbuch*. Sie können auch Pakete in IBM Cognos -Software für bestimmte Datenquellen erstellen und bearbeiten. Weitere Informationen finden Sie unter Kapitel 20, „Pakete", auf Seite 327.

You can secure data sources using IBM Cognos security. IBM Cognos software also respects any security that is defined within the data source. Weitere Informationen finden Sie unter „Datenquellen sichern" auf Seite 157 .

Sie versetzen Datenquellen von einer Umgebung in eine andere Umgebung, indem Sie den gesamten Content-Store implementieren. Weitere Informationen finden Sie unter Kapitel 19, „Implementierung", auf Seite 299.

Kompatibler Abfragemodus

Dieser Typ der Abfrageverarbeitung wird in IBM Cognos Analytics Version 10.2.2 und früher verwendet. Zum Ausführen von Berichten, die den kompatiblen Abfragemodus verwenden, müssen Sie 32-Bit-Clientbibliotheken für Datenquellen verwenden und den Berichtsserver als 32-Bit-Version konfigurieren. Der kompatible Abfragemodus verwendet native Client-und ODBC-Verbindungen für die Kommunikation mit Datenquellen.

Wenn die Datenquelle 64-Bit ist, stellen Sie sicher, dass Sie die 32-Bit-Clientbibliotheken verwenden, um die Verbindung zur Datenquelle herzustellen, um den Kompatibilitätsabfragemodus zu verwenden.

Dynamischer Abfragemodus

Der dynamische Abfragemodus stellt die Kommunikation mit Datenquellen unter Verwendung von Java- oder XMLA-Verbindungen bereit.

Für unterstützte relationale Datenbanken ist eine JDBC-Verbindung vom Typ 4 erforderlich. Ein JDBC-Treiber des Typs 4 konvertiert JDBC-Aufrufe direkt in das herstellerspezifische Datenbankprotokoll. Es wird in reinem Java geschrieben und ist plattformunabhängig. Für relationale Datenbanken müssen die JDBC-Treiber in das Verzeichnis IBM Cognos Analytics *Installationsposition*`\drivers` kopiert werden. Weitere Informationen finden Sie im Artikel zum Festlegen der Datenbankkonnektivität für Berichtsdatenbanken in der *IBM Cognos Analytics-Installations-und Konfigurationshandbuch*.

Für unterstützte OLAP-Datenquellen optimiert XMLA-Konnektivität den Zugriff, indem es maßgeschneiderte und erweiterte MDX für die spezifische Quelle und Version Ihrer OLAP-Technologie bereitstellt und die smarts der OLAP-Datenquelle festhäht.

Weitere Informationen finden Sie unter „JDBC-Verbindungen für Datenquellen verwenden" auf Seite 130.

Datenquellentypen

IBM Cognos Analytics unterstützt viele verschiedene Typen von Datenquellen, einschließlich relationaler, OLAP-und XML-Datenquellen.

Die Liste der unterstützten Datenquellentypen kann sich von Release zu Release ändern. Informationen zu den derzeit unterstützten Datenquellen finden Sie auf der Website von Unterstützte Softwareumgebungen (www.ibm.com/support/docview.wss?uid=swg27047186). Weitere Informationen finden Sie in der Liste der Kritische Probleme (www.ibm.com/support/docview.wss?uid=swg27047185), die möglicherweise auch Informationen zu Datenquellen enthalten.

Die Informationen zur Datenquellenverbindung für jeden Typ von Datenquelle können unterschiedlich sein. Informationen zu den Parametern, die Sie angeben müssen, um eine Verbindung zu Ihrer Datenquelle herzustellen, finden Sie in der Dokumentation zu den Anbietern.

IBM Db2 -Datenquellen

IBM Cognos Analytics unterstützt Db2 -Datenquellen.

JDBC connections can be used to connect to Db2 for Linux, UNIX, and Microsoft Fenster operating systems, and Db2 for z/OS.

Vertrauenswürdige IBM Db2 -Datenbankverbindungen

Sie können eine Verbindung zwischen der IBM Db2 -Datenbank und der IBM Cognos -Software herstellen, bei der mehrere Benutzer über die Funktion für den gesicherten Datenbankkontext eine Verbindung zu der Datenbank herstellen.

Eine Datenquelle, die für Verbindungen mit vertrauenswürdigen Anwendungen verwendet wird, muss offene Sitzungsblöcke für jeden benutzerspezifischen Datenbankstatus definieren, der definiert werden muss, bevor die Proxy-Benutzer-Abfragen abgesetzt werden. Der zugeordnete Open Connection-Block wird nur einmal ausgeführt, wenn die gesicherte Verbindung versucht wird, während Open-Session-Blöcke viele Male für verschiedene Benutzer ausgeführt werden können.

Die Informationen, die eine Verbindung zum Proxy einer Anforderung im Namen eines Benutzers, der Proxy-Anmeldungen verwenden darf, verwenden, wird der Datenbank mit dem folgenden Sitzungsbefehlsblock bereitgestellt, der an die gesicherte Datenbankverbindung angehängt ist. Der Wert, den Sie für die Sitzungsvariable OCI_ATTR_USERNAME verwenden, muss mit dem Db2 -Benutzernamen übereinstimmen.

```
<commandBlock>
    <commands>
        <sessionStartCommand>
            <arguments>
                <argument>
                    <name>OCI_ATTR_USERNAME</name>
                    <value>#$account.defaultName#</value>
                </argument>
            </arguments>
        </sessionStartCommand>
    </commands>
</commandBlock>
```

Informationen zum Hinzufügen eines Befehlsblocks für eine Datenquellenverbindung finden Sie unter „Hinzufügen von Befehlsblöcken beim Erstellen einer Datenquelle“ auf Seite 151.

Voraussetzungen für die Verwendung von gesicherten Verbindungen

Es gibt einige Voraussetzungen, um zu berücksichtigen, ob Sie vertrauenswürdige Verbindungen verwenden möchten.

- Verwenden Sie auf allen Plattformen den Db2 -Client der Version 9.5 oder höher.
- Verwenden Sie eine Db2 -Aufrufebene (Db2), um eine gesicherte Verbindung zu erstellen.
- Sie müssen eine Anmeldung für die Datenquellenverbindung erstellen, um die Db2 -Berechtigungsnachweise des vertrauenswürdigen Db2 -Benutzers anzugeben.
- Der vertrauenswürdige Kontext, den Sie in Ihrer Db2 -Datenbank definiert haben, darf keine Berechtigungsnachweise für den Benutzer anfordern, der als Proxied ausgeführt wird.

IBM Db2 -Verbindungsparameter

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern.

Weitere Informationen finden Sie unter „Datenquellenverbindungen" auf Seite 130.

Tabelle 22. Verbindungsparameter für Db2

Parameter	Beschreibung
Name der Db2 -Datenbank	Geben Sie den Namen (Aliasname) der Db2 -Datenbank ein, die verwendet wurde, als der Db2 -Client konfiguriert wurde.
Db2 -Verbindungszeichenfolge	Optional. Geben Sie Name/Name-Wert-Paare ein, die von Db2 CLI-oder ODBC-Anbietern akzeptiert werden können.
Sortierfolge	Geben Sie die Sortierfolge ein, die in die Datenbankverbindungszeichenfolge eingeschlossen werden soll. Sortierfolge sind nur in seltenen Fällen erforderlich, in denen möglicherweise Diskrepanzen zwischen IBM Cognos Analytics und einer Datenbank sortiert werden. Die Cognos-Abfrageengine kann bestimmte Typen von Sortierfolgen in einer Db2 -Datenbank erkennen, einschließlich 1252-IDENTITY und 1252-UNIQUE. Die Sortierung zwischen der lokalen Verarbeitung und der Datenbankverarbeitung ist konsistent, wenn die Db2 -Datenbank auf eine dieser Sortierfolgen gesetzt ist.
Asynchron öffnen	Nicht verwendet.
Gesicherter Kontext	Wählen Sie dieses Kontrollkästchen aus, um IBM Cognos Analytics zu ermöglichen, eine gesicherte Verbindung zu einem entsprechend konfigurierten Db2 -Server herzustellen. Weitere Informationen finden Sie in der Db2 -Verwaltungsdokumentation. Wenn Sie dieses Kontrollkästchen mit einem Client oder Server auswählen, der das Feature nicht unterstützt, können Sie einen Verbindungsfehler oder einen Fehler für die Berichtsausführung abrufen.
Zeitlimitüberschreitungen	Geben Sie die Zeit in Sekunden an, in der die Datenbank eine Verbindung herstellen oder auf Ihre Antwort warten soll, bevor Sie das Zeitlimit überschritten haben. Gültige Einträge sind null bis 32.767. Um die Datenbank auf unbestimmte Zeit warten zu lassen, geben Sie null ein. Dies ist der Standardwert.

Tabelle 22. Verbindungsparameter für Db2 (Forts.)	
Parameter	**Beschreibung**
Anmeldung	Weitere Informationen zu Anmeldedaten finden Sie unter „Datenquellen sichern“ auf Seite 157. Wenn keine Authentifizierung erforderlich ist, klicken Sie auf **Keine Authentifizierung**. Wenn die Authentifizierung erforderlich ist, klicken Sie auf **Anmeldungen**. Wenn in der Verbindungszeichenfolge eine Benutzer-ID und ein Kennwort erforderlich sind, wählen Sie das Kontrollkästchen **Benutzer-ID** aus. Wenn ein Kennwort erforderlich ist, wählen Sie das Kontrollkästchen **Kennwort** aus, und geben Sie das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein. Um eine Benutzer-ID und ein Kennwort zu erstellen, die automatisch mit der Datenquelle verbunden werden, klicken Sie auf **Signon erstellen, die die Gruppe "Jeder" verwenden kann**. Geben Sie die **Benutzer-ID** ein, und geben Sie anschließend das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein.

IBM Db2 JDBC-Verbindungsparameter

Wenn Sie das Kontrollkästchen **JDBC-Verbindung konfigurieren** ausgewählt haben, können Sie JDBC-Verbindungsparameter angeben, wenn Sie eine Datenquelle erstellen.

Weitere Informationen finden Sie unter „Datenquellenverbindungen“ auf Seite 130.

IBM Cognos-Cubes

The IBM Cognos cubes that can be used as data sources in IBM Cognos Analytics include IBM Cognos Planning Contributor and IBM Cognos PowerCubes.

Wenn Sie Probleme beim Erstellen von Datenquellenverbindungen zu Cognos -Würfeln haben, lesen Sie den Abschnitt *Handbuch zur Fehlerbehebung für IBM Cognos Analytics*.

For information about connecting to the IBM Cognos Planning - Contributor unpublished (real-time) data, see the IBM Cognos Planning *Installationshandbuch*.

IBM Cognos Planning Contributor

IBM Cognos Analytics unterstützt IBM Cognos Planning Contributor als Datenquelle.

Sie können IBM Cognos Analytics verwenden, um Echtzeit-Contributor-Daten zu erstellen und zu analysieren.

Sie können ein IBM Cognos Contributor-Paket auf eine der folgenden Arten erstellen:

- Mit der Contributor-Verwaltungskonsole können Sie ein Paket erstellen, das alle Cubes in der Anwendung enthält. Wenn ein Benutzer das Paket in einem Studio öffnet, werden sie mit Metadaten für alle Cubes in der Anwendung dargestellt und können aus mehreren Cubes auswählen, um Berichte zu erstellen. Es besteht jedoch die Gefahr, dass Benutzer versehentlich Abfragen erstellen, die versuchen, Werte aus mehr als einem Cube zu verwenden, was zu Berichten ohne Daten führt. Weitere Informationen finden Sie im *IBM Cognos Planning Contributor Administration Guide*.

- Mit Framework Manager können Sie bestimmen, wie viele Cubes in einem Paket verfügbar gemacht werden sollen. Standardmäßig erhalten Sie einen Cube in jedem Paket. Dies kann jedoch zu einer großen Anzahl von Paketen führen, die schwierig zu verwalten sein könnten. Weitere Informationen finden Sie im *IBM Cognos Framework Manager-Benutzerhandbuch*.

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern. Weitere Informationen finden Sie unter „Datenquellenverbindungen" auf Seite 130.

Tabelle 23. Verbindungsparameter für die Datenquelle für die Planung von Kontributoren

Parameter	**Beschreibung**
Externer Namensbereich	Wählen Sie den externen Namespace aus.

IBM Cognos PowerCubes

IBM Cognos Analytics unterstützt PowerCubes, die von Transformer 7.3 und höheren Versionen generiert werden.

Sie stellen einen PowerCube für Endbenutzer bereit, indem Sie ein Paket erstellen und es von Transformer oder Framework Manager veröffentlichen. Sie können auch PowerCube-Pakete in IBM Cognos Analytics erstellen (siehe Kapitel 20, „Pakete", auf Seite 327. Sie erstellen eine Datenquellenverbindung zu einem PowerCube in Transformer oder in Framework Manager, während Sie den Cube veröffentlichen, oder in IBM Cognos Administration, nachdem der Cube veröffentlicht wurde.

PowerCubes können unter Verwendung von Transformer in Linux -Betriebssystemen und in HPUX-Umgebungen von Itanium erstellt werden. Sie können die Sicherheit von IBM Cognos mit diesen Typen von Cubes verwenden, aber nicht die Series 7-Sicherheit. Sie können jedoch gesicherte Series 7-PowerCubes auf Linux -und HPUX- Itanium -Computern implementieren, die als Berichtsserver in der IBM Cognos -Umgebung ausgeführt werden, wenn der Content-Store von Cognos auf einem Series 7-konformen Server ausgeführt wird.

Sie können keine Würfel auf Linux oder HPUX Itanium erstellen, wenn Sie Improvisiert -Abfragedefinitionsdateien (.iqd) als Datenquellen verwenden, da die IQD-Bridge Series 7 auf diesen Plattformen nicht unterstützt wird.

Nachdem Sie eine Verbindung zu einem PowerCube hergestellt haben, können Sie Folgendes ausführen:

- Erstellen Sie ein Paket für einen PowerCube, siehe „Erstellen eines Pakets für einen PowerCube" auf Seite 327
- aktualisierte PowerCubes implementieren, siehe „Aktualisierte PowerCubes implementieren" auf Seite 156

Weitere Informationen zu PowerCubes finden Sie im *IBM Cognos Transformer-Benutzerhandbuch*.

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern. Weitere Informationen finden Sie unter „Datenquellenverbindungen" auf Seite 130.

Tabelle 24. Verbindungsparameter für PowerCubes-Datenquelle	
Parameter	**Beschreibung**
Cachegröße lesen	**Anmerkung:** Der Standardwert für diesen Parameter ist 80 MB. Sie können diesen Parameter auf einen Wert zwischen 1 MB und 1 GB setzen, wie dies für eine optimale Abfrageleistung erforderlich ist. Die optimale Lesecachegröße kann höher oder niedriger als der Standardwert von 80 MB sein. Dies ist zu erwarten, da PowerCubes in der Produktion weithin in den Typ-und Abfrageeigenschaften variieren. Beachten Sie, dass die Lese-Cache-Größe keine Auswirkung auf die Anfangszeit hat, die zum Öffnen eines Würfels erforderlich ist. Das typische Profil für die Abfrageleistung oder die Verarbeitungszeit folgt einem Muster, bei dem die Leistung mit der Größe des Lesecache steigt und dann über die optimale Einstellung hinaus absteigt. Um die optimale Einstellung zu ermitteln, empfehlen wir Ihnen, den Standardwert um 10 MB (oder 5 MB oder 1 MB, abhängig von der gewünschten Feinabstimmung) zu senken und die Ergebnisse der Abfrageergebnisse als Leitfaden für die Feststellung zu verwenden, ob weitere Reduzierungen oder Erhöhungen erforderlich sind. Die optimale Lesecachegröße wird sich ändern, wenn der Cube wächst und sich die Produktionsumgebung ändert. Daher sollten Sie die optimale Lesecachegröße überprüfen, wenn Änderungen am Abfrageleistungsmuster des Benutzers oder Änderungen in den PowerCube-Merkmalen auftreten.
Position	Wenn alle Berichtsserver auf Microsoft Fenster -Betriebssystemcomputern installiert sind, geben Sie die **Windows-Position**an. Wenn alle Berichtsserver auf UNIX -Betriebssystemcomputern installiert sind, geben Sie die **UNIX-oder Linux-Position**an. Geben Sie den vollständigen Pfad und Dateinamen für den Cube ein. Beispiel: Für einen lokalen Würfeltyp C:\cubes\sales_and_marketing.mdc. Für einen Netzwürfeltyp *Servername*\cubes\sales_and_marketing.mdc **Anmerkung:** Für Cubes, die sich auf UNIX -Computern befinden, geben Sie die korrekte UNIX -Position an und geben Sie alle Zeichen in der Fenster -Position ein, da die Fenster -Position nicht leer sein kann. **Anmerkung:** Wenn die Berichtsserver auf Fenster -und UNIX -Computern installiert sind und der Berichtsserver eine Anforderung zum Zugriff auf den PowerCube in beiden Umgebungen ausführen soll, geben Sie die Positionen Fenster und UNIX an. Um sicherzustellen, dass unabhängig von der Umgebung, in der der Berichtsserver auf den Cube zugreift, dieselben Daten zurückgegeben werden, muss die gleiche Cube-Datei an beiden Positionen gespeichert werden.

Tabelle 24. Verbindungsparameter für PowerCubes-Datenquelle (Forts.)	
Parameter	**Beschreibung**
Anmeldung	Wenn Sie die IBM Cognos -Sicherheit verwenden, klicken Sie auf **PowerCube-Authentifizierung auf einen einzelnen Namensbereich beschränken**, und wählen Sie einen Namensbereich aus der Liste aus. Wenn Sie eine Verbindung zu einem kennwortgeschützten PowerCube herstellen, klicken Sie auf **Cube-Kennwort**, und geben Sie das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein. **Anmerkung:** Wählen Sie **Alle gültigen Namensbereiche (einschließlich nicht gesicherter PowerCubes)** nur aus, wenn Sie Series 7 PowerCubes auf IBM Cognos Analytics in Ihrer Entwicklungs-oder Testumgebung migrieren. Diese Einstellung kann auch für nicht gesicherte PowerCubes in einer Produktionsumgebung verwendet werden. Wenn ein Würfelkennwort erforderlich ist, klicken Sie auf **Cube-Kennwort**, und geben Sie das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein. Um eine Benutzer-ID und ein Kennwort zu erstellen, die automatisch mit der Datenquelle verbunden werden, klicken Sie auf **Signon erstellen, die die Gruppe "Jeder" verwenden kann**. Weitere Informationen finden Sie unter „Datenquellen sichern" auf Seite 157.

Empfehlung-Verwendung von PowerCubes in IBM Cognos Software

Es gibt Empfehlungen, wenn Sie PowerCubes in IBM Cognos Software verwenden.

Konkret:

- Wenn Sie die Migration von PowerCubes der Serie 7 testen, können Sie die Anmeldeoption für die Authentifizierung bei **Alle gültigen Namensbereiche**auswählen.

  Diese Option wird nur für die Migration von Namespaces in Transformer-Modellen verwendet. Sie ändert nicht die Tatsache, dass mehrere Namespaces in einer Produktionsumgebung nicht unterstützt werden.
- Wenn Sie Series 7 PowerCubes als Datenquellen verwenden, empfehlen wir Ihnen, diese für IBM Cognos Analyticszu optimieren.

  Optimierte PowerCubes sorgen für einen schnelleren Datenabruf zur Laufzeit. Sie optimieren PowerCubes mithilfe eines Befehlszeilendienstprogramms mit dem Namen pcoptimizer, das mit der IBM Cognos -Software bereitgestellt wird.

  Weitere Informationen zur Optimierung von PowerCubes finden Sie im *Handbuch zur Fehlerbehebung für IBM Cognos Analytics*.
- Wenn Sie einen PowerCube veröffentlichen und der Cube angepasste Ansichten enthält, müssen Sie in IBM Cognos -Software unter Verwendung einer gültigen Benutzer-ID und eines Kennworts authentifiziert werden.

  Der anonyme Zugriff wird in dieser Situation nicht unterstützt.

Sichern von PowerCubes

PowerCubes, die von IBM Cognos -Software unterstützt werden, können unter Verwendung von IBM Cognos -Sicherheitsnamensbereichen gesichert werden. Die Sicherheit kann auf einen gesamten Cube

oder auf seine angepassten Ansichten angewendet werden. Bevor Sie auf einen Cube zugreifen können, der gegen einen IBM Cognos -Namespace gesichert ist, müssen Sie sich an dem entsprechenden Namespace anmelden.

In production environments, IBM Cognos software supports only PowerCubes secured against a single namespace. Wenn Sie PowerCubes für die Verwendung in einer Produktionsumgebung implementieren, müssen Sie daher die Anmeldeoption **PowerCube-Authentifizierung auf einen einzelnen Namensbereich beschränken**auswählen.

Anmerkung: Anstatt die Sicherheit von IBM Cognos zu verwenden, können Sie einem PowerCube einen Kennwortschutz hinzufügen oder nicht die Sicherheit verwenden.

Oracle Essbase-Datenquelle

Bevor eine Verbindung zu einer Oracle Essbase-Datenquelle hergestellt wird, sind einige Konfigurationsschritte erforderlich, wenn die Datenquelle Szenariodimensionen, Hierarchien oder Kennzahlen verwendet.

Wenn eine Oracle Essbase System 9-Datenquelle mit einem LDAP-Namespace konfiguriert ist, wird die Einzelanmeldung unterstützt. Die Benutzer-ID und das Kennwort, die für die Anmeldung am LDAP-Namespace verwendet werden, werden automatisch mit der Datenquelle verbunden. Weitere Informationen zum Konfigurieren eines LDAP-Namespace finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern. Weitere Informationen finden Sie unter „Datenquellenverbindungen” auf Seite 130.

Tabelle 25. Oracle Essbase-Datenquellenparameter

Parameter	**Beschreibung**
Servername	Geben Sie den Namen des Servers ein, auf dem sich die Datenbank befindet. Für das Betriebssystem UNIX kann dies die TCP/IP-Adresse des Servers sein.

Tabelle 25. Oracle Essbase-Datenquellenparameter (Forts.)	
Parameter	**Beschreibung**
Anmeldung	Weitere Informationen zu Anmeldedaten finden Sie unter „Datenquellen sichern" auf Seite 157. Wenn keine Authentifizierung erforderlich ist, klicken Sie auf **Keine Authentifizierung**. Für Essbase Server System 9 und IBM Cognos 8.4 wird die Einzelanmeldung unterstützt, wenn Ihr Essbase-Server für einen LDAP-Namespace konfiguriert ist. · Wählen Sie **Externer Namensbereich** aus und wählen Sie **LDAP** in der Liste aus. · Die Benutzer-ID und das Kennwort, die für die Anmeldung am LDAP-Namespace verwendet werden, werden automatisch mit der Datenquelle verbunden. Wenn in der Verbindungszeichenfolge eine Benutzer-ID und ein Kennwort erforderlich sind, klicken Sie auf **Anmeldungen**. · Wenn ein Kennwort erforderlich ist, wählen Sie das Kontrollkästchen **Kennwort** aus, und geben Sie das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein. · Um eine Benutzer-ID und ein Kennwort zu erstellen, die automatisch mit der Datenquelle verbunden werden, klicken Sie auf **Signon erstellen, die die Gruppe "Jeder" verwenden kann**. Geben Sie die **Benutzer-ID** ein, und geben Sie anschließend das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein.

Szenario-Dimensionen konfigurieren

Wenn Sie eine Verbindung zu einer Oracle Essbase-Datenquelle herstellen und eine Szenariodimension enthält, müssen Sie die Szenariodimension manuell so konfigurieren, dass IBM Cognos Analytics sie erkennt. Andernfalls behandelt IBM Cognos Analytics die Szenariodimension als reguläre Dimension.

Vorgehensweise

Ordnen Sie in der Oracle Essbase ein benutzerdefiniertes Attribut (User Defined Attribute, UDA) mit dem Namen COGNOS_SCENARIO_DIMENSION der Szenariodimension zu.

Ausgeglichene Hierarchien angeben

Oracle Essbase Provider bestimmt nicht, ob eine Hierarchie ausgeglichen oder unausgewogen ist. Sie berücksichtigt, dass alle Hierarchien standardmäßig unausgewogen sind.

In einer ausgeglichenen Hierarchie wird jeder Pfad in die gleiche Tiefe herunterfahren, während die Verzweigungen in einer unausgeglichenen Hierarchie auf unterschiedliche Ebenen absteigen.

Vorgehensweise

1. Erstellen Sie im Tool 'Hyperion Solutions Essbase Administration Services' ein spezielles benutzerdefiniertes Attribut (User Defined Attribute, UDA) mit dem Namen COGNOS_HIERARCHY_BALANCED in der Gliederung der Essbase-Datenbank. Die UDA wird für das Stammelement der entsprechenden Dimension erstellt, die eine ausgewogene Hierarchie enthält.
2. Setzen Sie das Attribut auf 1.

Maßformate angeben

Um die Lesbarkeit der gemeldeten Werte zu verbessern, können Sie eine alternative Formatierzeichenfolge für jede Kennzahl angeben.

Definieren Sie eine UDA für die entsprechenden Mitglieder in der Dimension 'Account':

```
COGNOS_FORMAT=format_string
```

Der Wert *format_string* kann eines der vordefinierten Zahlenformate sein, die in der folgenden Tabelle aufgelistet sind. Sie können ein voreingestelltes numerisches Format verwenden, um Werte als Millionen (M) oder Tausende (K) anzuzeigen. Zum Beispiel kann 1.801.791 als 1.8M oder 1.801.8K angezeigt werden.

Die vordefinierten Formatierzeichenfolgen lauten wie folgt:

Tabelle 26. Vordefinierte Zeichenfolgen für Oracle Essbase-Datenquellen

Formatoption	**Beispielwert**	**Beispiel**
Allgemein	1000000	1000000
0	1000000	1000000
#,##0	1000000	1,000,000
$0	1000000	$1000000
$#,##0	1000000	$1,000,000
0%	1000000	100000000%
%0	1000000	%100000000
0E + 000	1000000	1E + 006
0K	1000000	1000K
#,##0K	1000000	1.000K
K0	1000000	K1000
K#,##0	1000000	K1, 000
$0K	1000000	1000K
$#,##0K	1000000	1.000K
0M	1000000000	1000M

Tabelle 26. Vordefinierte Zeichenfolgen für Oracle Essbase-Datenquellen (Forts.)		
Formatoption	**Beispielwert**	**Beispiel**
#,##0M	1000000000	1.000M
M0	1000000000	M1000
M#,##0	1000000000	M1, 000
$0M	1000000000	1000M
$#,##0M	1000000000	1.000M

Mit Ausnahme der Zeichenfolge für den allgemeinen Format können Sie auch die Anzahl der Dezimalstellen vorgeben, die angezeigt werden sollen. Dabei wird die Formatzeichenfolge ~ n verwendet, wobei n die Anzahl der Dezimalstellen ist. Zum Beispiel kann 1.801.791 mit der Formatzeichenfolge $#,##0~ 2 als $1.801.791.00 angezeigt werden. Wenn Sie keine Dezimalstellen haben wollen, beenden Sie die Formatierzeichenfolge mit ~0.

Wenn Ihre Clientanwendung eine andere Ländereinstellung verwendet, müssen Sie die Symbole "Währung ($)", "Tausend (,)" und "Dezimalzahl (.)" im Wert "format_string" für das COGNOS_FORMAT UDA durch die entsprechenden Ländereinstellungssymbole ersetzen, die für die Clientanwendung in Kraft sind.

Wenn Sie die Anzahl der anzuzeigenden Dezimalstellen nicht angeben oder wenn die Formatierzeichenfolge nicht mit einem der vordefinierten Werte (einschließlich der Ländereinstellungssymbole) übereinstimmt, wird standardmäßig die Zeichenfolge für den allgemeinen Format verwendet.

Sie können für jede Kennzahl ein anderes Format anwenden. Im Folgenden werden einige Beispiele erläutert, wie Sie verschiedene Formatierungen auf verschiedene Kennzahlen anwenden können:

Tabelle 27. Oracle Essbase-Datenquellenformate für Kennzahlen	
Maßnahme	**Anwendungsformat**
Maßnahmen (Kontodimension)	COGNOS_FORMAT = #,##0
Einheiten	COGNOS_FORMAT = #,##K
Kosten	COGNOS_FORMAT = $#,###
Gewinne	COGNOS_FORMAT= 0%

IBM InfoSphere Warehouse Cubing Services

IBM Cognos software provides support for accessing the cubing services technology of IBM InfoSphere Warehouse for version 9.5.2 and greater. Es müssen keine IBM Cognos -Komponenten auf dem Cubing-Services-Server installiert werden.

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern. Weitere Informationen finden Sie unter „Datenquellenverbindungen" auf Seite 130.

Tabelle 28. InfoSphere Warehouse-Cubing-Services-Datenquellenverbindungsparameter	
Parameter	**Beschreibung**
Server-URL	Geben Sie die URL des Servers in das Format http:// < Hostname>: < Würfelserver xmla port> / IBMXmlAnalysis/ oder https:// < Hostname>: < Würfelserver xmla port> /IBMXmlAnalysis/ ein. Ein Beispiel für den < Hostname>: < Würfelserver xmla port > ist wottcub1:80.
SSL-Verbindung öffnen	Wenn Sie sichere Sockets verwenden möchten, wählen Sie dieses Kontrollkästchen aus. Wenn Sie unsichere Sockets verwenden möchten, wählen Sie sie nicht aus. Die Einstellung muss mit der Einstellung auf dem Server identisch sein.
Anmeldung	Wenn in der Verbindungszeichenfolge eine Benutzer-ID und ein Kennwort erforderlich sind, wählen Sie das Kontrollkästchen **Benutzer-ID** aus. Wenn ein Kennwort erforderlich ist, wählen Sie das Kontrollkästchen **Kennwort** aus und geben Sie das Kennwort in den **Kennwort und Bestätigung** -Kennwortfeldern ein.

Informix -Datenquellen

IBM Cognos software provides support for Informix data sources.

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern. Weitere Informationen finden Sie unter „Datenquellenverbindungen” auf Seite 130.

Tabelle 29. Verbindungsparameter für Informix-Datenquellen	
Parameter	**Beschreibung**
Informix-Datenbankname	Geben Sie den Datenbanknamen ein.
Hostname	Geben Sie den Hostnamen ein.
Servername	Geben Sie den Servernamen ein.
Sortierfolge	Geben Sie die Sortierfolge ein, die in die Datenbankverbindungszeichenfolge eingeschlossen werden soll. Sortierfolge sind nur in seltenen Fällen erforderlich, in denen möglicherweise Diskrepanzen zwischen der IBM Cognos -Software und einer Datenbank sortiert werden.
Service	Wählen Sie den Servicenamen aus, den der ferne Datenbankserver für eingehende Anforderungen verwendet, oder geben Sie ihn ein.

Tabelle 29. Verbindungsparameter für Informix-Datenquellen (Forts.)	
Parameter	**Beschreibung**
Anmeldung	Weitere Informationen zu Anmeldedaten finden Sie unter „Datenquellen sichern" auf Seite 157. Wenn in der Verbindungszeichenfolge eine Benutzer-ID oder ein Kennwort erforderlich ist, wählen Sie das Kontrollkästchen **Benutzer-ID** aus. Wenn ein Kennwort erforderlich ist, wählen Sie das Kontrollkästchen **Kennwort** aus, und geben Sie das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein. Wenn Sie eine Benutzer-ID und ein Kennwort erstellen möchten, die automatisch eine Verbindung zur Datenquelle herstellen, wählen Sie **Signon erstellen, die die Gruppe "Jeder" verwenden kann**aus. Geben Sie die **Benutzer-ID** ein, und geben Sie anschließend das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein.

Datenquellen für Microsoft Analysis Services

IBM Cognos software supports connectivity to Microsoft Analysis Services from a Microsoft Fenster operating system platform.

Wenn Sie Microsoft SQL Server installieren, können Sie Analysis Services hinzufügen. Für die Konnektivität sind die Microsoft Pivot Table-Clientbibliotheken erforderlich, die mit Microsoft SQL Server-Clientkomponenten installiert werden.

Sie müssen eine passende Version der SQL Server-Client-Software auf jedem Computer installieren, auf dem Application-Tier-Komponenten für den IBM Cognos Analytics Server oder IBM Cognos Framework Manager ausgeführt werden.

Sie müssen das TCP-Protokoll für Microsoft SQL Server-und Microsoft SQL Server-Clientkomponenten aktivieren.

Der IBM Cognos Analytics -Server unterstützt drei verschiedene Typen von Authentifizierungsdaten für Analysis Services-Datenquellen:

- „Authentifizierung unter Verwendung von Signons" auf Seite 113
- „Authentifizierung mit Serviceberechtigungsnachweisen" auf Seite 114
- „Authentifizierung unter Verwendung eines externen Namespace" auf Seite 114

Wenn Sie Framework Manager verwenden (siehe „Überlegungen zum Framework Manager" auf Seite 115) und MDX-Abfragen (MDX = Multidimensional expression), finden Sie besondere Hinweise. Weitere Informationen finden Sie unter „MDX-Abfragen (MDX = Multidimensional Expression)" auf Seite 116.

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern. Sie können aus den folgenden Datenquellentypen auswählen:

- Microsoft Analysis Services 2012 (ODBO)
- Microsoft Analysis Services 2014 (ODBO)
- Microsoft Analysis Services 2016 (ODBO)
- Microsoft Analysis Services (HTTP XMLA)

Weitere Informationen finden Sie unter „Datenquellenverbindungen" auf Seite 130.

Tabelle 30. Daten der Datenquellenverbindungsparameter für Microsoft -Analyseservices	
Parameter	**Beschreibung**
Servername	**Anmerkung:** Geben Sie den Servernamen ein, in dem sich die Datenbanken befinden.
Benannte Instanz	Geben Sie die benannte Instanz ein, wenn eine während der Installation angegeben wurde. **Anmerkung:** Dieser Parameter gilt nur für Microsoft Analysis Services 2005 und 2008.
Sprache	Wählen Sie die Sprache aus. Bei den Microsoft Analysis Services 2005 und 2008 wird dies als Ländereinstellung für das Design verwendet, die der Berichtsersteller zum Abrufen von Metadaten aus dem Cube zum Anzeigen in Berichten verwendet. Sobald die Berichte erstellt wurden, können sie in einer beliebigen Ländereinstellung ausgeführt werden.

Tabelle 30. Daten der Datenquellenverbindungsparameter für Microsoft -Analyseservices (Forts.)	
Parameter	**Beschreibung**
Anmeldung	Weitere Informationen zu Anmeldedaten finden Sie unter „Datenquellen sichern" auf Seite 157. Wählen Sie **Berechtigungsnachweise für IBM Cognos-Software-Service**aus, um die Authentifizierung unter Verwendung der Berechtigungsnachweise des Fenster -Domänenaccounts, auf dem der IBM Cognos -Service ausgeführt wird, zu verwenden. Weitere Informationen finden Sie unter „Authentifizierung mit Serviceberechtigungsnachweisen" auf Seite 114 . Wenn Sie einen externen Namespace verwenden möchten, wählen Sie **Externer Namensbereich** aus, und wählen Sie einen Namespace aus. Weitere Informationen finden Sie unter „Authentifizierung unter Verwendung eines externen Namespace" auf Seite 114. Wenn Sie eine vorhandene Datenquelle ändern, die zuvor signons verwendet wurde, löschen Sie die Anmeldungen, nachdem Sie in einen externen Namespace gewechselt haben. Andernfalls haben die Anmeldungen Vorrang. Wenn Sie eine statische Anmeldung erstellen möchten, die jeder verwenden kann, wählen Sie **Anmeldungen** und **Signon erstellen, die die Gruppe "Jeder" verwenden kann**aus. Wählen Sie das Kontrollkästchen **Kennwort** aus und geben Sie eine gültige Fenster -Domäne **Benutzer-ID**ein, und geben Sie anschließend das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein. Weitere Informationen finden Sie unter „Authentifizierung unter Verwendung von Signons" auf Seite 113.

Authentifizierung unter Verwendung von Signons

Wenn Sie Berechtigungsnachweise für die Authentifizierung bei Microsoft Analysis Services-Datenquellen in IBM Cognos speichern und verwalten möchten, verwenden Sie bei der Erstellung der Datenquelle eine Anmeldung. Sie können eine Anmeldung definieren, die von allen verwendet wird (Standardeinstellung), oder Sie können Zugriff auf bestimmte Benutzer erteilen. Sie können auch mehrere Anmeldungen erstellen und Berechtigungen zum Erteilen von Zugriff für angegebene Benutzer, Gruppen oder Rollen verwenden.

Die Anmeldung speichert gültige Fenster -Domänenberechtigungsnachweise, die für die Authentifizierung bei Analysis Services verwendet werden. Sie müssen in der folgenden Syntax angegeben werden:

< DOMAIN> \ < BENUTZER-NAME>

Für Microsoft Analysis Services 2005 und 2008 sollten Benutzer mit Berechtigungsnachweisen ein Teil der lokalen OLAP-Benutzergruppe sein, die auf dem Computer vorhanden ist, auf dem Analysis Services ausgeführt werden. Diese Gruppe, die erstellt wird, wenn Analysis Services installiert ist, wird als SQLServerMSASUser$ < SERVERNAME> $MSSQLSERVER bezeichnet.

Stellen Sie bei jeder Installation einer IBM Cognos Application-Tier-Komponente sicher, dass die IBM Cognos -Software als ein eingebautes LocalSystem-Konto ausgeführt wird oder dass IBM Cognos -Software als gültiges Domänenkonto ausgeführt wird, dem das **Als Teil des Betriebssystems handeln** -Zugriffsrecht in der lokalen Sicherheitsrichtlinie erteilt wurde.

IBM Cognos -Benutzern muss die Lese-und Ausführungsberechtigung für diese Anmeldung erteilt werden.

Authentifizierung mit Serviceberechtigungsnachweisen

Wenn Sie die Berechtigungsnachweise des Accounts verwenden möchten, der den IBM Cognos -Service ausführt, um sich bei Microsoft Analysis Services zu authentifizieren, verwenden Sie Serviceberechtigungsnachweise. Bei jeder Verbindung zu Microsoft Analysis Services-Datenquellen werden die Serviceberechtigungsnachweise verwendet, unabhängig davon, welcher Benutzer die Anforderung ausführt.

Um Serviceberechtigungsnachweise zu verwenden, muss IBM Cognos -Software als Fenster -Service gestartet werden. Der Service muss als gültiger Fenster -Domänenbenutzer ausgeführt werden. Die integrierten Accounts von LocalSystem oder NetworkService sind nicht anwendbar. Informationen zum Starten des IBM Cognos -Service unter einem Account finden Sie in den Informationen zum Konfigurieren eines Benutzerkontos oder eines Netzservicekontos in der *IBM Cognos Analytics Installation und Konfiguration*.

Der Account, auf dem der IBM Cognos -Service ausgeführt wird, muss die folgenden Voraussetzungen erfüllen:

- Das Konto muss entweder ein Mitglied desselben Active Directory Forest sein, da Analysis Services oder Forest Trust für Cross-Forest-Setups eingerichtet werden müssen.
- Dem Konto muss das Zugriffsrecht **Als Service anmelden** in der lokalen Sicherheitsrichtlinie von allen Fenster -Computern, auf denen IBM Cognos Application-Tier-Komponenten ausgeführt werden, erteilt werden.
- Bei Konfigurationen mit mehreren Knoten muss auf allen Computern, auf denen IBM Cognos Application-Tier-Komponenten ausgeführt werden, dasselbe Konto verwendet werden.
- Für die Microsoft Analysis Services 2005 und 2008 muss dem Service-Account ausreichende Berechtigungen für die SSAS-Sicherheit erteilt werden, um die gewünschten Cubes zuzuordnen und Daten abzurufen.
- Bei den Microsoft Analysis Services 2005 und 2008 sollte das Konto ein Teil der lokalen OLAP-Benutzergruppe sein, die auf dem Computer vorhanden ist, auf dem Analysis Services ausgeführt werden. Diese Gruppe, die erstellt wird, wenn Analysis Services installiert ist, wird als SQLServerMSASUser$ < SERVERNAME> $MSSQLSERVER bezeichnet.

Authentifizierung unter Verwendung eines externen Namespace

Wenn IBM Cognos -Benutzer mit ihren eigenen Berechtigungsnachweisen (Benutzerdurchgriffsauthentifizierung, Anmeldung) auf Microsoft Analysis Services-Datenquellen zugreifen möchten, verwenden Sie einen externen Namespace. Die Berechtigungsnachweise, die für die Authentifizierung bei Analysis Services verwendet werden, werden dem angegebenen Namespace entnommen, für den der Benutzer zuvor authentifiziert wurde.

Die Berechtigungsnachweise, die von einem Benutzer bereitgestellt werden, der am Namespace angemeldet ist, werden an Analysis Services übergeben. Aufgrund der Authentifizierungsmethoden, die von Analysis Services unterstützt werden, können Sie nur einen Namespace des Typs Microsoft Active Directory auswählen.

Je nachdem, wie der Benutzer für den Active Directory-Namespace authentifiziert wird, der für die Authentifizierung mit externem Namespace angegeben wurde, können Sie die folgenden Anmeldekonfigurationen haben, die ein nahtloses Benutzererlebnis bieten:

- Wenn ein Benutzer explizit authentifiziert wird, indem er einen Domänenbenutzernamen und ein Kennwort bereitstellt, ist eine Durchgriffsauthentifizierung möglich. Die bereitgestellten Domänenberechtigungsnachweise werden an Analysis Services übergeben.
- Wenn ein Benutzer, der durch eine Anmeldung, die nicht auf Kerberos basiert, für den Active Directory-Namespace authentifiziert wurde, ist eine Durchgriffsauthentifizierung des Benutzers nicht möglich. Dies gilt für Setups, bei denen der Active Directory-Namespace für den Identitätszuordnungsmodus konfiguriert ist.

Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind, um die Benutzerdurchgriffsauthentifizierung für Analysis Services zu konfigurieren:

- Alle Computer, auf denen IBM Cognos Application-Tier-Komponenten ausgeführt werden, müssen IBM Cognos Analytics als Fenster -Service unter einem gültigen Domänenaccount oder LocalSystem ausführen.
- Alle Computer, auf denen IBM Cognos -Software ausgeführt wird, müssen über ein Serverbetriebssystem von Microsoft Fenster verfügen. (Pass-through-Authentifizierung wird für Fenster XP nicht unterstützt.)
- Die Computer, auf denen Analysis Services und IBM Cognos -Software ausgeführt werden, müssen Teil desselben Active Directory Forest sein.
- Für die Delegierung muss das Domänenkonto (Benutzerkonto) oder das Computerkonto (LocalSystem) anerkannt werden.
- Für alle Benutzer- Fenster -Accounts, für die der Zugriff auf Analysis Services über IBM Cognos erforderlich ist, darf die Eigenschaft **Konto ist sensitiv und kann nicht delegiert werden** nicht definiert sein.

Analyseservices sind für die Kerberos-Authentifizierung konfiguriert. Weitere Informationen erhalten Sie von Ihrem Analysis Services Administrator.

Für SSAS 2005 und SSAS 2008 müssen Fenster Accounts für alle Benutzer Teil der lokalen OLAP-Benutzergruppe auf dem Computer sein, auf dem Analysis Services ausgeführt werden. Diese Gruppe, die erstellt wird, wenn Analysis Services installiert ist, wird als SQLServerMSASUser$ < SERVERNAME> $MSSQLSERVER bezeichnet.

Beachten Sie, dass es ein Microsoft -Problem gibt, das die Durchgriffsauthentifizierung des Benutzers behindert, wenn Analysis Services und die Clients, die auf diese Services zugreifen, beide auf AES-Betriebssystemen ausgeführt werden (Fenster 2008, Microsoft Vista, Fenster 7). Ausführliche Informationen hierzu finden Sie in der Dokumentation zu Microsoft .

Beachten Sie, dass Sie keine Datenquelle testen können, die für die Authentifizierung mit externen Namensbereichen konfiguriert ist. Um zu überprüfen, ob es funktioniert, greifen Sie in einer Abfrage auf die Datenquelle zu.

Überlegungen zum Framework Manager

IBM Cognos Framework Manager greift direkt ohne die Verwendung des Berichts oder der Metadaten-Services auf die Datenquellen der Analysis Services zu. Dies hat wichtige Auswirkungen, insbesondere für Konfigurationen mit Benutzerdurchgriffsauthentifizierung für Analysis Services.

Wenn die Kerberos-basierte Anmeldung für den konfigurierten Active Directory-Namespace aktiviert ist, stellen Sie sicher, dass die Benutzer, die Framework Manager ausführen, als Authentifizierungsquelle für den externen Namespace für die Analysis Services-Datenquelle das folgende Kriterium erfüllen:

- verfügt über das Zugriffsrecht **Als Teil des Betriebssystems handeln** in der lokalen Sicherheitsrichtlinie auf dem Computer, auf dem Framework Manager ausgeführt wird, oder ist ein Mitglied der Gruppe 'Lokale Administratoren' auf dem Framework Manager-Computer mit der Berechtigung ' **Anmelden lokal** '.
- Für die Delegierung

MDX-Abfragen (MDX = Multidimensional Expression)

Sie müssen die folgenden Microsoft Office-Komponenten für Microsoft Excel Visual Basic for Applications-Funktionen (VBA) installieren, wie z. B. ROUNDDOWN für MDX-Abfragen:

- Office Excel
- Microsoft Visual Basic for Applications (eine gemeinsam genutzte Funktion im Office)

Installieren Sie diese Komponenten auf dem IBM Cognos Server für MSAS und auf dem Analysis Services-Server-Computer für SSAS 2005 oder SSAS 2008, und starten Sie anschließend die Servermaschine erneut.

Microsoft -SQL-Serverdatenquellen

IBM Cognos software supports the following types of Microsoft SQL Server data sources: ODBC, SQL 2012 Native Client, and SQL 2014 Native Client.

Abhängig von den Typen der Microsoft -SQL-Server-Datenquellen, die Sie verwenden, sollten Sie bei der Definition einiger Authentifizierungstypen Überlegungen berücksichtigen.

Authentifizierung mit IBM Cognos Service-Berechtigungsnachweisen

Sie sollten kein lokales Microsoft Fenster -Systemkonto für die IBM Cognos -Serveranmeldung mit einer OLE DB-Datenquelle von Microsoft SQL Server verwenden.

Authentifizierung mit externem Namensbereich

You can configure IBM Cognos software to use a Microsoft Active Directory namespace, where users are prompted for credentials as part of the IBM Cognos logon process. Sie können IBM Cognos -Software so konfigurieren, dass dieselben Berechtigungsnachweise automatisch verwendet werden, wenn auf die Datenquelle von Microsoft SQL Server zugegriffen wird. Die Datenquellenverbindung für Microsoft SQL Server muss für **Externer Namensbereich** konfiguriert werden, und dieser Namespace muss der Active Directory-Namespace sein.

You can configure IBM Cognos software to use a Microsoft Active Directory namespace and to authenticate users for IBM Cognos software using Kerberos authentication and delegation. Sie können die IBM Cognos -Software so konfigurieren, dass der Benutzer beim Zugriff auf die Microsoft SQL Server-Datenquelle automatisch authentifiziert wird. Die folgende Konfiguration ist erforderlich:

- Das IBM Cognos -Gateway muss auf einem IIS-Web-Server installiert sein, der für die integrierte Fenster -Authentifizierung konfiguriert ist.
- Content Manager, der Berichtsserver (Komponenten der Anwendungsebene), der IIS-Web-Server und der Datenquellenserver (Microsoft SQL Server) müssen zu derselben Active Directory-Domäne gehören.
- Die Datenquellenverbindung für Microsoft SQL Server muss für **Externer Namensbereich** konfiguriert werden, und dieser Namespace muss der Active Directory-Namespace sein.
- Die Berichtsserver werden der Delegierung als vertrauenswürdig angesehen.

Einschränkung: Wenn Sie die Kerberos-Authentifizierung für Single Sign-on verwenden, kann jede Datenquelle nur eine Verbindung haben. Für mehrere Verbindungen zu SQL Server mit aktivierter Einzelanmeldung müssen Sie mehrere Datenquellen erstellen oder eine Verbindung für jede Datenquelle erstellen.

Weitere Informationen zu den Installationsoptionen für Gateway und Content Manager sowie zur Konfiguration des Namespace und zum Delegieren von Vertrauen finden Sie im *Installations-und Konfigurationshandbuch*.

Microsoft SQL Server-Verbindungsparameter

Die folgenden Parameter werden von Microsoft SQL Server-Datenquellen verwendet.

Tabelle 31. Microsoft SQL Server-Verbindungsparameter	
Parameter	**Beschreibung**
Servername	Geben Sie den Servernamen ein. Wenn mehrere Instanzen von Microsoft SQL Server vorhanden sind, geben Sie *Servername**Instanzname*an.
Datenbankname	Geben Sie den Datenbanknamen ein.
Anwendungsname	Geben Sie den Anwendungsnamen ein.
Sortierfolge	Geben Sie die Sortierfolge ein, die in die Datenbankverbindungszeichenfolge eingeschlossen werden soll. Sortierfolge sind nur in seltenen Fällen erforderlich, in denen möglicherweise Diskrepanzen zwischen der IBM Cognos -Software und einer Datenbank sortiert werden.
MARS-Verbindung	Wählen Sie die Verbindung mit mehreren aktiven Ergebnissen (MARS = Active Results Set) aus. Dieser Parameter wird nur von Microsoft SQL Server (SQL 2005 Native Client oder höher) verwendet. Klicken Sie auf **Ja** , um zuzulassen, dass Anwendungen mehr als eine anstehende Anforderung pro Verbindung und mehr als eine aktive Standardergebnismenge pro Verbindung haben.
Optionale Verbindungsparameter	Geben Sie einen optionalen, einen Schlüssel-Wert-Typ eines Parameters ein. Verwenden Sie dazu die folgende Syntax: *Param1=Wert1*. Mehrere Parameter müssen durch ein Semikolon begrenzt werden, wie im folgenden Beispiel gezeigt: *Param1=Wert1;Param2=Wert2* Alles, was Sie für diesen Parameter eingeben, wird an den Datenbankteil der Verbindungszeichenfolge angehängt. **Tipp:** Das erste Vorkommen des @-Zeichens trennt den Datenbankteil der Verbindungszeichenfolge vom IBM Cognos -Abschnitt der Verbindungszeichenfolge, außer wenn das Zeichen @ ein Teil der Benutzer-ID oder des Kennworts ist. Dies gilt nicht für den dynamischen Abfragemodus.

Tabelle 31. Microsoft SQL Server-Verbindungsparameter (Forts.)	
Parameter	**Beschreibung**
Anmeldung	Weitere Informationen zu Anmeldedaten finden Sie unter „Datenquellen sichern" auf Seite 157. Wenn keine Authentifizierung erforderlich ist, wählen Sie **Keine Authentifizierung**aus. Weitere Informationen zu **IBM Cognos Analytics**finden Sie unter „Authentifizierung mit IBM Cognos Service-Berechtigungsnachweisen" auf Seite 116. Wenn Sie einen Active Directory-Namespace von Microsoft verwenden und Sie die Einzelanmeldung unterstützen möchten, wählen Sie **Externer Namensbereich**aus, und wählen Sie den Active Directory-Namespace aus. Weitere Informationen finden Sie unter „Authentifizierung mit externem Namensbereich" auf Seite 116. Wenn die Authentifizierung erforderlich ist, wählen Sie **Anmeldungen**aus. Wenn in der Verbindungszeichenfolge eine Benutzer-ID und ein Kennwort erforderlich sind, wählen Sie das Kontrollkästchen **Benutzer-ID** aus. Wenn ein Kennwort erforderlich ist, wählen Sie das Kontrollkästchen **Kennwort** aus, und geben Sie das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein.

Sie können Datenbankbefehle in die Verbindungsinformationen für diesen Typ von Datenquelle einschließen. Weitere Informationen finden Sie unter „IBM Cognos-Kontext an eine Datenbank übergeben" auf Seite 145.

Informationen zu den Verbindungsparametern von Microsoft SQL Server (ODBC) finden Sie unter „ODBC-Datenquellenverbindungen" auf Seite 118.

ODBC-Datenquellenverbindungen

IBM Cognos software supports ODBC data sources.

IBM Cognos software divides ODBC connections into two categories: vendor-specific ODBC data sources connections, which use driver-specific capabilities for query creation, and generic ODBC data source connections, which use general capabilities.

IBM Cognos software supports the ODBC data sources listed in the following table. Der Datenbankcode wird in der Verbindungszeichenfolge angezeigt, kann jedoch nicht bearbeitet werden.

Tabelle 32. ODBC-Datenquellen und Datenbankcode	
ODBC-Datenquelle	**Datenbankcode**
ODBC	OD
Microsoft SQL Server (ODBC)	SS
Netezza (ODBC)	NZ
Sybase-IQ (ODBC)	IQ

Tabelle 32. ODBC-Datenquellen und Datenbankcode (Forts.)	
ODBC-Datenquelle	**Datenbankcode**
Teradata (ODBC)	TD

Jede ODBC-Datenquellenverbindung, die nicht aufgelistet ist, sollte mit der generischen ODBC-Datenquelle, dem Datenbankcode OD, erstellt werden.

ODBC-Verbindungsparameter

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern.

Weitere Informationen finden Sie unter „Datenquellenverbindungen" auf Seite 130.

Tabelle 33. ODBC-Verbindungsparameter	
Parameter	**Beschreibung**
ODBC-Datenquelle	Geben Sie den Datenquellennamen (DSN) gemäß der Definition in der Datei ODBC.ini ein. For more information about the ODBC.ini file, see the IBM Cognos Analytics *Installations-und Konfigurationshandbuch*.
ODBC-Verbindungszeichenfolge	Geben Sie einen beliebigen Text ein, der an die Verbindungszeichenfolge angehängt werden muss. Dieser Parameter bleibt in der Regel leer.
Sortierfolge	Geben Sie die Sortierfolge ein, die in die Datenbankverbindungszeichenfolge eingeschlossen werden soll. Sortierfolge sind nur in seltenen Fällen erforderlich, in denen möglicherweise Diskrepanzen zwischen der IBM Cognos -Software und einer Datenbank sortiert werden.
Asynchron öffnen	Wählen Sie aus, ob die Verbindung Anforderungen unabhängig voneinander verarbeiten soll. Wählen Sie nicht aus, ob die Verbindung zur Ausführung der aktuellen Anforderung ausgeführt werden soll, bevor Sie eine andere starten.
Unicode-ODBC	Wenn die Option UNICODE aktiviert ist, wird die ODBC-API für Unicode aufgerufen, andernfalls wird die Nicht-Unicode-ODBC-API aufgerufen. Wenn die Nicht-UNICODE-API aufgerufen wird, werden SQL-Anweisungen und -parameter in dem Zeichensatz der Maschine codiert, auf der die Abfrageengine ausgeführt wird. Weitere Informationen zur ODBC-API und zur UNICODE-Unterstützung finden Sie in der Microsoft-ODBC-API-Referenz.

Tabelle 33. ODBC-Verbindungsparameter (Forts.)	
Parameter	**Beschreibung**
Zeitlimitüberschreitungen	Geben Sie die Zeit in Sekunden an, in der die Datenbank eine Verbindung herstellen oder auf Ihre Antwort warten soll, bevor Sie das Zeitlimit überschritten haben. Gültige Einträge sind null bis 32.767. Damit die Datenbank auf unbestimmte Zeit warten kann, geben Sie null ein. Dies ist der Standardwert.
Anmeldung	Weitere Informationen zu Anmeldedaten finden Sie unter „Datenquellen sichern" auf Seite 157. Für Teradata, Microsoft SQL und generisches ODBC: · Wenn keine Authentifizierung erforderlich ist, wählen Sie **Keine Authentifizierung**aus. · Wenn die Berechtigungsnachweise für die Datenbank mit den Berechtigungsnachweisen übereinstimmen, die für die Anmeldung bei der IBM Cognos -Umgebung verwendet werden, wählen Sie **Externer Namensbereich** aus, und wählen Sie den entsprechenden Namespace aus. · Wenn die Authentifizierung erforderlich ist, wählen Sie **Anmeldungen**aus. Wenn ein Kennwort erforderlich ist, wählen Sie das Kontrollkästchen **Kennwort** aus, und geben Sie das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein. Wenn Sie eine Benutzer-ID und ein Kennwort erstellen möchten, die automatisch eine Verbindung zur Datenquelle herstellen, wählen Sie **Signon erstellen, die die Gruppe "Jeder" verwenden kann**aus. Geben Sie die **Benutzer-ID** ein, und geben Sie anschließend das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein.

Oracle-Datenquellen

IBM Cognos software supports Oracle data sources.

Oracle-Verbindungsparameter

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern.

Weitere Informationen finden Sie unter „Datenquellenverbindungen" auf Seite 130.

Tabelle 34. Oracle-Verbindungsparameter	
Parameter	**Beschreibung**
SQL* Net-Verbindungszeichenfolge	Geben Sie den Instanznamen der Oracle-Datenbank ein, wie er in der Datei tnsnames.ora eingegeben wird.
Sortierfolge	Geben Sie die Sortierfolge ein, die in die Datenbankverbindungszeichenfolge eingeschlossen werden soll. Sortierfolge sind nur in seltenen Fällen erforderlich, in denen möglicherweise Diskrepanzen zwischen der IBM Cognos -Software und einer Datenbank sortiert werden.
Anmeldung	Weitere Informationen zu Anmeldedaten finden Sie unter „Datenquellen sichern" auf Seite 157. Wenn in der Verbindungszeichenfolge eine Benutzer-ID erforderlich ist, geben Sie die Benutzer-ID in das Feld **Benutzer-ID** ein. Wenn ein Kennwort erforderlich ist, wählen Sie das Kontrollkästchen **Kennwort** aus, und geben Sie das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein. Wenn Sie eine Benutzer-ID und ein Kennwort erstellen möchten, die automatisch eine Verbindung zur Datenquelle herstellen, wählen Sie **Signon erstellen, die die Gruppe "Jeder" verwenden kann**aus. Geben Sie die **Benutzer-ID** ein, und geben Sie anschließend das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein.

Datenquellenverbindungen für externe Repositorys

IBM Cognos software supports data source connections to external report repositories. Sie verwenden die Berichtsrepositoryverbindung, um eine Verbindung zu einem Dateisystem oder einem IBM FileNet Content Manager-Repository herzustellen.

Sie müssen Ihr IBM FileNet Content Manager-Repository installieren, konfigurieren und konfigurieren, bevor Sie eine Datenquellenverbindung für externe Repositorys erstellen.

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern. Weitere Informationen finden Sie unter „Datenquellenverbindungen" auf Seite 130.

IBM FileNet Content Manager connections

Verwenden Sie die Informationen in der folgenden Tabelle, um die Parameter anzugeben, die für die Erstellung einer Verbindung zu Ihrem IBM FileNet Content Manager-Repository erforderlich sind.

Weitere Informationen zum Erstellen von Datenquellen finden Sie unter „Datenquellenverbindung erstellen" auf Seite 131.

Tabelle 35. Verbindungsparameter für die Verbindung zu einem FileNet -Repository	
Parameter	**Beschreibung**
Repository-Typ	Wählen Sie **IBM FileNet Content Manager** aus, um eine Verbindung zu Ihrem externen FileNet -Repository herzustellen.
Repository-CMIS-URL	Geben Sie die URL für die Position Filenet mit dem folgenden Format ein: http:// < Servername> :Portnummer/ < FileNet CMIS_name> /resources/ < FileNet_object store_name>/ Beispiel: http://server1:9080/fncmis/resources/archive/
Rootpfad	Geben Sie die Position des Ordners ein, in dem der archivierte Inhalt in FileNetgespeichert werden soll. Diese Position muss bereits in FileNetvorhanden sein. Beispiel: Sie können einen Ordner in Filenet mit dem Namen report_repository haben.
Repository-Verbindungsparameter	Geben Sie optional Parameter ein, die an die URL für den Treiberklassennamen angehängt werden sollen.
Anmeldung	Wählen Sie das Markierungsfeld **Benutzer-ID** aus. Wählen Sie das Markierungsfeld **Kennwort** aus. Wenn Sie eine Benutzer-ID und ein Kennwort erstellen möchten, die automatisch eine Verbindung zur Datenquelle herstellen, klicken Sie auf "Anmeldedaten erstellen", die die Gruppe "Jeder" verwenden kann. Geben Sie die Benutzer-ID ein, und geben Sie anschließend das Kennwort in die Felder Kennwort und Kennwort bestätigen ein.

Dateisystemverbindungen

Sie können eine Datenquellenverbindung zu einem Dateisystem erstellen, nachdem Sie das Aliasstammverzeichnis in IBM Cognos Configuration konfiguriert haben. Der Alias-Root verweist auf eine Dateiposition auf einem lokalen Laufwerk oder auf einem lokalen Netzwerk-Share.

Verwenden Sie die Informationen in der folgenden Tabelle, um die Parameter einzugeben, die erforderlich sind, wenn Sie eine Datenquellenverbindung zu Ihrem Dateisystem-Repository erstellen.

Tabelle 36. Verbindungsparameter, die zum Herstellen einer Verbindung zu einem Dateisystemrepository verwendet werden	
Parameter	**Beschreibung**
Repository-Dateisystemstammverzeichnis	Wählen Sie das Aliasstammverzeichnis aus.
Rootpfad	Dies ist ein optionaler Parameter, der ein Unterordner des Aliasnamens ist. Wenn Sie den Stammverzeichnispfad angeben möchten, geben Sie die Position des Unterordners ein, um den archivierten Inhalt in der Position des Dateisystems zu speichern. Diese Position muss bereits vorhanden sein. Beispiel: /sales.
Repository-Verbindungsparameter	Geben Sie optional Parameter ein, die an die URL für den Treiberklassennamen angehängt werden sollen.

SAP Business Information Warehouse (SAP BW)-Datenquellen

IBM Cognos software supports access to SAP BW data sources.

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern. Weitere Informationen finden Sie unter „Datenquellenverbindungen" auf Seite 130. Die Parametertypen, die Sie angeben, unterscheiden sich abhängig vom Typ der SAP BW-Anmeldung, die Sie auswählen:

· Anmeldetyp des Anwendungsservers

· Anmeldeart des Ziels

· Anmeldetyp des Nachrichtenservers

Verbindungsparameter für Anmeldetyp des Anwendungsservers

Wenn Sie **Anwendungsserver** als **SAP-Anmeldetyp**auswählen, geben Sie die Parameter in der folgenden Tabelle an.

Tabelle 37. Verbindungsparameter für den Anmeldetyp des Anwendungsservers

Parameter	Beschreibung
Anwendungsserver	Geben Sie den Namen des SAP-Anwendungsservers ein. Wenden Sie sich an Ihren SAP-Systemadministrator, um weitere Informationen zu erhalten.
Systemnummer	Geben Sie die Systemnummer ein. Wenden Sie sich an Ihren SAP-Systemadministrator, um weitere Informationen zu erhalten.
Clientnummer	Geben Sie die Clientnummer ein. Wenden Sie sich an Ihren SAP-Systemadministrator, um weitere Informationen zu erhalten.
SAP-Servercodepage	Wählen Sie die Codepage des SAP-Servers aus. IBM Cognos software follows the SAP internationalization rules, providing a compatible application that supports multiple scripts and languages without modifying SAP BW in IBM Cognos software. Wenden Sie sich an Ihren SAP-Systemadministrator, um weitere Informationen zu erhalten.
SAP-Router-Zeichenfolge	Geben Sie die SAP-Routerzeichenfolge ein. Die Routerzeichenfolge beschreibt die Stationen einer Verbindung, die zwischen zwei Hosts erforderlich ist. Wenden Sie sich an Ihren SAP-Systemadministrator, um weitere Informationen zu erhalten.

Tabelle 37. Verbindungsparameter für den Anmeldetyp des Anwendungsservers (Forts.)	
Parameter	**Beschreibung**
Anmeldung	Weitere Informationen zu Anmeldedaten finden Sie unter „Datenquellen sichern" auf Seite 157. Wenn ein vertrauenswürdiger signon-Namespace mit IBM Cognos Configuration konfiguriert wird, können Sie **Externer Namensbereich** auswählen und den Namespace auswählen, den Sie verwenden möchten. Wenn Sie eine Benutzer-ID und ein Kennwort erstellen möchten, die automatisch eine Verbindung zur Datenquelle herstellen, wählen Sie **Signon erstellen, die die Gruppe "Jeder" verwenden kann**aus. Geben Sie die **Benutzer-ID** ein, und geben Sie anschließend das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein.

Verbindungsparameter für Zielanmeldungstyp

Wenn Sie **Ziel** als **SAP BW-Anmeldetyp**auswählen, geben Sie die Parameter in der folgenden Tabelle an.

Tabelle 38. Verbindungsparameter für Zielanmeldungsart	
Parameter	**Beschreibung**
Clientnummer	Geben Sie die Clientnummer ein. Wenden Sie sich an Ihren SAP-Systemadministrator, um weitere Informationen zu erhalten.
SAP-Servercodepage	Wählen Sie die Codepage des SAP-Servers aus. IBM Cognos software follows the SAP internationalization rules, providing a compatible application that supports multiple scripts and languages without modifying SAP BW in IBM Cognos software. Wenden Sie sich an Ihren SAP-Systemadministrator, um weitere Informationen zu erhalten.

Tabelle 38. Verbindungsparameter für Zielanmeldungsart (Forts.)	
Parameter	**Beschreibung**
Anmeldung	Weitere Informationen zu Anmeldedaten finden Sie unter „Datenquellen sichern" auf Seite 157. Wenn ein vertrauenswürdiger signon-Namespace mit IBM Cognos Configuration konfiguriert wird, können Sie **Externer Namensbereich** auswählen und den Namespace auswählen, den Sie verwenden möchten. Wenn Sie eine Benutzer-ID und ein Kennwort erstellen möchten, die automatisch eine Verbindung zur Datenquelle herstellen, wählen Sie **Signon erstellen, die die Gruppe "Jeder" verwenden kann**aus. Geben Sie die **Benutzer-ID** ein, und geben Sie anschließend das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein.

Verbindungsparameter für den Anmeldetyp des Nachrichtenservers

Wenn Sie **Nachrichtenserver** als **SAP BW-Anmeldetyp**auswählen, geben Sie die Parameter in der folgenden Tabelle an.

Tabelle 39. Verbindungsparameter für den Anmeldetyp des Nachrichtenservers	
Parameter	**Beschreibung**
System-ID	Geben Sie die System-ID des SAP-Systems ein, zu dem eine Verbindung hergestellt werden soll. Wenden Sie sich an Ihren SAP-Systemadministrator, um weitere Informationen zu erhalten.
Anmeldegruppe	Geben Sie die SAP-Gruppe ein. Wenden Sie sich an Ihren SAP-Systemadministrator, um weitere Informationen zu erhalten.
Clientnummer	Geben Sie die Clientnummer ein. Wenden Sie sich an Ihren SAP-Systemadministrator, um weitere Informationen zu erhalten.

Tabelle 39. Verbindungsparameter für den Anmeldetyp des Nachrichtenservers (Forts.)	
Parameter	**Beschreibung**
Anmeldung	Weitere Informationen zu Anmeldedaten finden Sie unter „Datenquellen sichern" auf Seite 157. Wenn ein vertrauenswürdiger signon-Namespace mit IBM Cognos Configuration konfiguriert wird, können Sie **Externer Namensbereich** auswählen und den Namespace auswählen, den Sie verwenden möchten. Wenn Sie eine Benutzer-ID und ein Kennwort erstellen möchten, die automatisch eine Verbindung zur Datenquelle herstellen, wählen Sie **Signon erstellen, die die Gruppe "Jeder" verwenden kann**aus. Geben Sie die **Benutzer-ID** ein, und geben Sie anschließend das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein.

Sybase Adaptive Server Enterprise Data Sources

IBM Cognos software supports Sybase Adaptive Server Enterprise CT-15.

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern.

Tabelle 40. Sybase Adaptive Server Enterprise-Datenquellenparameter	
Parameter	**Beschreibung**
Servername	Geben Sie den Namen des Servers ein.
Datenbankname	Geben Sie den Datenbanknamen ein. Wählen Sie **Master** aus, wenn der Sybase-Server die Standarddatenbank bestimmen soll. Um den Standardwert zu überschreiben, geben Sie einen gültigen Datenbanknamen ein.
Anwendungsname	Geben Sie den Anwendungsnamen ein. Wenn Sie dieses Feld leer lassen, ist der Standardwert der Name der ausführbaren Datei von Cognos , z. B. BiBustkservermain oder DataBuild.
Sortierfolge	Geben Sie die Sortierfolge ein, die in die Datenbankverbindungszeichenfolge eingeschlossen werden soll. Sortierfolge sind nur in seltenen Fällen erforderlich, in denen möglicherweise Diskrepanzen zwischen der IBM Cognos -Software und einer Datenbank sortiert werden.

Tabelle 40. Sybase Adaptive Server Enterprise-Datenquellenparameter (Forts.)	
Parameter	**Beschreibung**
Paketgröße	Geben Sie die Paketgröße ein. Der Standardwert ist 2048. Erhöhen Sie die Paketgröße, um die Anzahl der Pakete zu reduzieren, die gesendet werden müssen. Verringern Sie die Paketgröße, wenn eine größere Paketgröße ein Problem ist. Die Größe, die Sie anfordern können, kann nicht größer sein, als der Sybase-Server zulässt. Weitere Informationen erhalten Sie von Ihrem Datenbankadministrator.
Asynchrone Ebenen	Wählen Sie die asynchrone Ebene aus.
Sendeaufruf-Zeitscheibe	Geben Sie die Sendeaufrufzeitscheibe ein. Der Standardwert ist 100.
Zeitlimitüberschreitungen	Geben Sie die Zeit in Sekunden an, in der die Datenbank eine Verbindung herstellen oder auf Ihre Antwort warten soll, bevor Sie das Zeitlimit überschritten haben. Gültige Einträge sind null bis 32.767. Um die Datenbank auf unbestimmte Zeit warten zu lassen, geben Sie null ein. Dies ist der Standardwert.
Anmeldung	Weitere Informationen zu Anmeldedaten finden Sie unter „Datenquellensignonen" auf Seite 141 . Wenn in der Verbindungszeichenfolge eine Benutzer-ID oder ein Kennwort erforderlich ist, wählen Sie das Kontrollkästchen **Benutzer-ID** aus. Wenn ein Kennwort erforderlich ist, wählen Sie das Kontrollkästchen **Kennwort** aus, und geben Sie das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein. Wenn Sie eine Benutzer-ID und ein Kennwort erstellen möchten, die automatisch eine Verbindung zur Datenquelle herstellen, wählen Sie **Signon erstellen, die die Gruppe "Jeder" verwenden kann**aus. Geben Sie die **Benutzer-ID** ein, und geben Sie anschließend das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein.

TM1 -Datenquellen

IBM Cognos software provides support for accessing TM1 servers and cubes.

Sie müssen den TM1 -Client auf dem gleichen Computer wie die IBM Cognos Business Intelligence-Installation installieren. Wenn Sie eine TM1 -Datenquellenverbindung erstellen, sollten Sie sich überlegen, wie Sie die Authentifizierung einrichten möchten.

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern. Weitere Informationen finden Sie unter „Datenquellenverbindungen" auf Seite 130.

Tabelle 41. TM1 -Datenquellenparameter	
Parameter	**Beschreibung**
Administrationshost	Geben Sie den Namen einer Maschine ein, die durch das Netz identifiziert werden kann.
Servername	Geben Sie den Servernamen so ein, wie er in der Datei TM1S.cfg konfiguriert ist. Weitere Informationen finden Sie in der Dokumentation zu TM1 .
Anmeldung	Weitere Informationen zu Anmeldedaten finden Sie unter „Datenquellen sichern" auf Seite 157. Wenn keine Authentifizierung erforderlich ist, wählen Sie **Keine Authentifizierung**aus. Wenn ein externer Namespace verwendet wird, wählen Sie **Externer Namensbereich** aus, und wählen Sie dann den Namespace aus. Wenn die Authentifizierung erforderlich ist, wählen Sie **Anmeldungen**aus. Wenn in der Verbindungszeichenfolge eine Benutzer-ID erforderlich ist, wählen Sie das Kontrollkästchen **Benutzer-ID** aus. Wenn ein Kennwort erforderlich ist, wählen Sie das Kontrollkästchen **Kennwort** aus, und geben Sie das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein. Wenn Sie eine Benutzer-ID und ein Kennwort erstellen möchten, die automatisch eine Verbindung zur Datenquelle herstellen, wählen Sie **Signon erstellen, die die Gruppe "Jeder" verwenden kann**aus. Geben Sie die **Benutzer-ID** ein, und geben Sie anschließend das Kennwort in den Feldern **Kennwort** und **Kennwort bestätigen** ein.

Authentifizierung

Ihre Auswahl muss die Authentifizierungsanforderung für den TM1 -Server erfüllen. Wenn Sie beispielsweise keine Benutzer-ID und kein Kennwort erstellen, der TM1 -Server jedoch ein Protokoll erfordert, wird der Benutzer aufgefordert, sich anzumelden.

Sie können einen externen Namespace (Third-Party-Verzeichnisservice-Provider) als Authentifizierungsmethode verwenden. Der TM1 -Server muss für die Authentifizierung bei IBM Cognos BI konfiguriert sein. Weitere Informationen finden Sie in der Dokumentation zu TM1 unter Cognos Access Manager Authentication.

Unerwartete Ergebnisse bei Verwendung von Aggregation mit TM1 -Datenquellen

TM1 -Datenquellen können regelabgeleitete Zellen enthalten. IBM Cognos BI kann diese von der Regel abgeleiteten Zellen nicht vor der Zeit identifizieren, sodass eine Aggregation auf diesen Zellen zu unerwarteten Ergebnissen führen kann. Wenn Sie beispielsweise eine Gruppe zusammenfassen, die einen regelabgeleiteten Wert enthält, können unerwartete Ergebnisse in Report Studio und Analysis Studio generiert werden.

Anmerkung: Explizite Aggregationsoperationen wie Summe, Durchschnitt, Zähler, Minimum und Maximum sind nicht betroffen.

Wenn Sie TM1 -Datenwürfel mit regelabgeleiteten Zellen in IBM Cognos BI verwenden, empfehlen wir Ihnen, TM1 Buildnummer 9.4.00001.576 zu installieren, die Aggregationsfehler identifiziert, indem Sie die Fehlerzellen mit Gedankenstrichen (--) markieren.

Der Verwaltungshost muss vollständig qualifiziert sein, um TM1 -Datenquellen zu unterstützen.

Zu Ihrer Installation gehören IBM Cognos 8 Business Intelligence Server-und TM1 -Datenquellen. Nach dem Upgrade oder beim Erstellen oder Ändern einer TM1 -Datenquellenverbindung können Sie die folgende Fehlernachricht erhalten:

COGCQ00223094-TM1-ERR-0060 Der TM1 -Server ist mit einem nicht unterstützten Sicherheitsmodus konfiguriert.

Um das Problem zu beheben, ändern Sie den Namen des Verwaltungshosts in einen vollständig qualifizierten Domänennamen im Assistenten für die Datenquellenverbindungen.

XML-Datenquellen

Wenn Sie eine XML-Datenquelle erstellen, müssen Sie XML als Typ der Verbindung verwenden und die Position des XML-Dokuments in der Verbindungszeichenfolge angeben.

Sie können die Verbindungszeichenfolge für eine XML-Datenquelle wie folgt angeben:

- Eine HTTP-URL, die den Content-Store angibt, der für die Herstellung einer Verbindung zum XML-Dokument erforderlich ist.

  Beispiel: HTTP://xmltestserver.cognos.com/XML/countryregion.xml.

  Stellen Sie sicher, dass Sie einen Webaliasnamen für das Verzeichnis erstellen, das die XML-Datei enthält, und dass Sie das Durchsuchen des Verzeichnisses aktivieren.
- Dateipfad

  Ein Microsoft Fenster -Beispielpfadbeispiel für das Betriebssystem lautet *Servername*\XML \countryregion.xml.

  Ein Beispiel für ein UNIX -Betriebssystem für das Dateisystem ist/*Mountname*/XML/countryregion.xml.
- eine lokale Datei

  Ein Beispiel hierfür ist C:\XML \countryregion.xml;VALIDATE=ON.

Um auf eine lokale Datei zuzugreifen, verwenden Sie einen Dateipfad, der plattformspezifische Syntax verwendet.

Um eine XML-Verbindungszeichenfolge zu testen, müssen Sie den folgenden Code am Ende der Zeichenfolge eingeben:

```
;VALIDATE=ON
```

Bei dem Text dieses Codes muss die Groß-/Kleinschreibung nicht beachtet werden.

Sie geben Verbindungsparameter an, wenn Sie eine Datenquelle erstellen oder eine Datenquellenverbindung ändern. Weitere Informationen finden Sie unter „Datenquellenverbindungen" auf Seite 130.

Tabelle 42. XML-Datenquellenparameter

Parameter	Beschreibung
Verbindungszeichenfolge	Geben Sie die Verbindungszeichenfolge ein.

Parametrisierte XML-Verbindungsstrings

In einer HTTP-URL-Verbindungszeichenfolge für eine XML-Datenquelle können Sie Parameter verwenden, um zusätzliche Informationen zu senden. Sie können eine Eingabeaufforderungsdefinitionszeichenfolge in die Parameterkomponente einbetten.

Wenn die Eingabeaufforderungsdefinition in dem Bericht angegeben ist, wird dieser Wert verwendet. Andernfalls wird der Benutzer aufgefordert, einen Wert anzugeben. Die Bedienerführung wird für andere Arten von Verbindungszeichenfolgen nicht unterstützt.

Ein Beispiel für eine URL-Komponente ist 'addressing_scheme://*network_location*/path; parameters? query#fragment_identifier '.

Codieren Sie die Parameterkomponente mit der Definitionszeichenfolge in zwei Gruppen von Fragezeichen. Eine Eingabeaufforderung kann eine Komponentengrenze nicht überschreiten.

Ein Beispiel für eine parametrisierte XML-Zeichenfolge ist http://*My_Network_Location*/*My_Pfad*/ myxml.asp?countryregionsid =??CanadaPrompt?

Parametrisierte XML-Verbindungszeichenfolgen haben diese Einschränkungen:

- Wenn eine URL-Komponente eine Eingabeaufforderung ist, kann sie keine weiteren Daten enthalten.
- Eingabeaufforderungen, die in XML-Verbindungszeichenfolgen eingebettet sind, funktionieren nicht in Framework Manager. Sie können keine Daten aus einer parametrisierten XML-Verbindungszeichenfolge importieren.
- Wenn Sie eine parametrisierte XML-Verbindungszeichenfolge einrichten, funktioniert die Schaltfläche "Test" nicht.
- Die Validierung der Abfragespezifikation in Reporting funktioniert nicht, wenn Sie mit einer parametrisierten XML-Verbindungszeichenfolge verbunden sind.

Datenquellenverbindungen

Eine Datenquellenverbindung gibt die Parameter an, die zum Herstellen einer Verbindung zu einer Datenbank erforderlich sind, wie z. B. die Position der Datenbank und die Zeitlimitdauer. Diese Parameter bilden eine Verbindungszeichenfolge für die Datenquelle.

Wenn Sie ein Administrator sind, können Sie alle erforderlichen Datenquellen einrichten, bevor Modelle in Framework Manager erstellt werden, so dass alle Verbindungen im Assistenten für den Metadaten-Framework-Manager verfügbar sind.

Datenquellen werden im Namespace von **Cognos** gespeichert und müssen eindeutige Namen haben. Sie können zum Beispiel nicht denselben Namen für eine Datenquelle und eine Gruppe verwenden.

JDBC-Verbindungen für Datenquellen verwenden

Für einige Datenquellenverbindungen können Sie zusätzliche JDBC-Datenquellenverbindungsinformationen (Java -Database Connectivity) bereitstellen. Die Verbindungsinformationen für die JDBC-Datenquelle sind optional. JDBC-Datenquellenverbindungen sind erforderlich, wenn Ihre Pakete über Framework Manager mit aktivierter Option **Dynamischen Abfragemodus verwenden** veröffentlicht werden.

Die JDBC-Verbindungszeichenfolgen für relationale Datenquellen haben das folgende Format:

```
^User ID:^?Password:;LOCAL;JD;URL=<urlspec>;
DRIVER_NAME=<driver class name spec>[;CognosProperty=value[;...]]
```

Die JDBC-Verbindungszeichenfolge für eine Microsoft -SQL-Server-Datenquelle sieht beispielsweise wie folgt aus:

```
^UserID:^?Password:;LOCAL;JD-SS;URL=jdbc:sqlserver://sotaimpqc05:1433;
databaseName=dmsqc1;DRIVER_NAME=com.microsoft.sqlserver.jdbc.SQLServerDriver;
LOCALSORT=us_us_ASCII;LEVEL=PRIMARY
```

Für relationale Datenbanken müssen die JDBC-Treiber in das Cognos Analytics-Verzeichnis *Installationsposition*\drivers kopiert werden. Weitere Informationen finden Sie im Artikel zum Festlegen der Datenbankkonnektivität für Berichtsdatenbanken in der *IBM Cognos Analytics-Installations- und Konfigurationshandbuch*.

Informationen zu den Einstellungen für Abfrageservice finden Sie im Kapitel 7, „Service 'Query Service'", auf Seite 159.

Beachten Sie, dass die Isolationsstufen für JDBC-Verbindungen nicht implementiert sind. Möglicherweise sehen Sie ein anderes Verhalten, wenn die Isolationsstufe, die Sie für die native Clientverbindung auswählen, von der Standardverbindung abweicht, die vom JDBC-Treiber verwendet wird. Weitere Informationen zur Standardeinstellung des Treibers finden Sie in der Dokumentation zu Ihrem JDBC-Treiber.

Weitere Informationen zu Isolationsstufen finden Sie unter „Isolationsstufen" auf Seite 143 .

Netzpfade für dateibasierte Datenquellen verwenden

Wenn Sie über eine verteilte Installation mit mehreren Servern verfügen, empfehlen wir, dass Sie Netzpfade für alle dateibasierten Datenquellen und nicht für lokale Pfade verwenden. Auf diese Weise wird sichergestellt, dass auf die Datenquellen von den Services zugegriffen werden kann, für die sie erforderlich sind, unabhängig davon, welcher Server die Daten benötigt.

Wenn Sie eine Verbindung zu einer dateibasierten Datenquelle erstellen, wie z. B. einen PowerCube, geben Sie einen Pfad und einen Dateinamen ein. Um auf die Datei zu verweisen, verwenden Sie einen lokalen Pfad, wie z. B. C: \cubes \ Great Outdoors Company.mdc, oder einen Netzpfad, wie z. B. \ *Servername*\cubes \ Great Outdoors Company.mdc.

In einer verteilten Installation, in der Berichtsserver auf verschiedenen Computern ausgeführt werden, ist es erforderlich, dass die Datei und der Pfad auf jedem Computer, auf dem ein Berichtsserver ausgeführt wird, gültig sein müssen. Wenn Sie einen Netzpfad verwenden, um auf eine Datei zu verweisen, verweist jeder Berichtsserver alternativ auf dieselbe Datei im Netz, ohne die Datei lokal verfügbar zu haben. Um sicherzustellen, dass die Datei immer verfügbar ist, wird empfohlen, diese Datei in einem gemeinsam genutzten Verzeichnis zu speichern, auf das in Ihrem Netz zugegriffen werden kann.

Wenn Sie IBM Cognos Analytics -Komponenten auf UNIX -Betriebssystemservern installiert haben, empfehlen wir Ihnen, auch die dateibasierte Datenquelle auf einem UNIX -Server zu finden. Anschließend sollten Sie einen UNIX -Pfad verwenden, z. B./Servername/Würfel/Große Außentüren Company.mdc , um auf die Datei zuzugreifen.

Wenn Sie alle Komponenten auf einem einzelnen Computer installiert haben, können Sie lokale Pfade verwenden, aber Sie müssen sicherstellen, dass die Services, die die Daten anfordern, den entsprechenden Zugriff auf die Datendateien auf dem Computer haben.

Bei verteilten Installationen von Microsoft Fenster wird empfohlen, UNC-Pfade für gemeinsam genutzte Verzeichnisse für dateibasierte Datenquellen, wie z. B. PowerCubes oder XML-Dateien, zu verwenden.

Datenquellenverbindung erstellen

Eine Datenquellenverbindung gibt die Parameter an, die zum Herstellen einer Verbindung zu einer Datenbank erforderlich sind, wie z. B. die Position der Datenbank und die Zeitlimitdauer. Diese Parameter bilden eine Verbindungszeichenfolge für die Datenquelle.

Sie können Authentifizierungsinformationen für die Datenbank in die Datenquellenverbindung aufnehmen, indem Sie einen Anmeldetext erstellen. Benutzer müssen bei jeder Verwendung der Verbindung keine Datenbankauthentifizierungsinformationen eingeben, weil die Authentifizierungsinformationen verschlüsselt und auf dem Server gespeichert werden. Die Anmeldung, die beim Erstellen einer Datenquelle erstellt wurde, ist für die Gruppe "Everyone" verfügbar. Später können Sie ändern, wer die Anmeldedaten verwenden oder mehr Anmeldungen erstellen kann.

Vorbereitende Schritte

Sie müssen über Schreibberechtigungen für den Ordner verfügen, in dem Sie die Datenquelle speichern möchten, und für den **Cognos** -Namespace. Sie müssen auch Ausführungsberechtigungen für das gesicherte Feature von **Datenquellenverbindungen** haben. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen”, auf Seite 207.

Informationen zu diesem Vorgang

Vorhandene Datenquellenverbindungen können nicht in Framework Manager bearbeitet werden.

Vorgehensweise

1. Wählen Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** die Option **Datenquellenverbindungen**aus.

   Tipp: Wenn Sie eine Datenquelle entfernen möchten, wählen Sie das Kontrollkästchen für die Datenquelle aus, und wählen Sie die Schaltfläche zum Löschen aus.
2. Wählen Sie die neue Schaltfläche für die Datenquelle aus.
3. Geben Sie auf der Seite 'Name und Beschreibung' einen eindeutigen Namen für die Datenquelle und optional eine Beschreibung und eine Anzeigenspitze ein und wählen Sie anschließend **Weiter**aus.
4. Wählen Sie auf der Verbindungsseite in der Dropdown-Liste **Typ** den Typ der Datenquelle aus, die Sie erstellen möchten.

   Wenn Ihre Datenquelle nicht aufgelistet ist, klicken Sie auf **Anderer Typ**.

   Tipp: Wenn Sie eine Verbindung zum The Weather Company -Service konfigurieren, wählen Sie **JDBC**aus.

   Wenn Sie eine relationale Datenquelle ausgewählt haben, wird das Kontrollkästchen **JDBC-Verbindung konfigurieren** ausgewählt. Wenn Sie keine JDBC-Verbindung erstellen möchten, wählen Sie das Kontrollkästchen ab. Weitere Informationen zu JDBC-Verbindungen finden Sie unter „JDBC-Verbindungen für Datenquellen verwenden” auf Seite 130.
5. Geben Sie die Isolationsstufe an:

   - Wenn **Isolationsstufe** nicht angezeigt wird, wählen Sie **Weiter**aus.
   - Wenn **Isolationsstufe** auch angezeigt wird, wählen Sie das Standardobjektgateway aus, oder geben Sie einen Wert an, und wählen Sie dann **Weiter**aus.
6. Geben Sie die Verbindungsparameter für die Datenquelle an.

   Klicken Sie in der folgenden Liste auf das zugehörige Element, um Informationen zu Verbindungsparametern für den Typ der Datenquelle zu erhalten, die Sie verwenden:

   - „IBM Cognos Planning Contributor” auf Seite 102
   - „IBM Cognos PowerCubes” auf Seite 103
   - „ODBC-Datenquellenverbindungen” auf Seite 118
   - „IBM Db2 -Datenquellen” auf Seite 100
   - „IBM InfoSphere Warehouse Cubing Services” auf Seite 109
   - „Informix -Datenquellen” auf Seite 110
   - „Microsoft -SQL-Serverdatenquellen” auf Seite 116
   - „Datenquellen für Microsoft Analysis Services” auf Seite 111
   - „Oracle-Datenquellen” auf Seite 120
   - „SAP Business Information Warehouse (SAP BW)-Datenquellen” auf Seite 123
   - „Sybase Adaptive Server Enterprise Data Sources” auf Seite 126
   - „TM1 -Datenquellen” auf Seite 127
   - „XML-Datenquellen” auf Seite 129

- „Datenquellenverbindungen für externe Repositorys“ auf Seite 121
- „Verbindungen von IBM Weather Company“ auf Seite 136

7. Wählen Sie **Verbindung testen**und anschließend **Test** aus, um zu testen, ob Parameter korrekt sind.

   In der Spalte **Status** können Sie feststellen, ob die Verbindung erfolgreich war. Wenn der Fehler nicht erfolgreich war, wählen Sie **Schließen**aus, kehren Sie zu den vorherigen Schritten zurück und überprüfen Sie die Verbindungsparameter. Wenn er erfolgreich war, fahren Sie mit dem nächsten Schritt fort.
8. Klicken Sie auf **Fertigstellen**.

   Wenn Sie eine andere Datenquelle als IBM Cognos PowerCube oder SAP BW ausgewählt haben, wird die neue Datenquelle in **Datenquellenverbindungen** auf der Registerkarte **Konfiguration** angezeigt und kann bei der Verwendung des Metadatenassistenten in Framework Manager ausgewählt werden.

   Wenn Sie IBM Cognos PowerCube oder SAP BW ausgewählt haben, fahren Sie mit dem nächsten Schritt fort.
9. Klicken Sie auf **OK** , um zu **Datenquellenverbindungen**zurückzukehren, oder klicken Sie für einige Datenquellen auf **Paket erstellen** und **OK**.

   Anmerkung: Sie können jetzt oder später ein Paket mit Ihrer neuen Datenquelle erstellen. Das Kontrollkästchen **Paket erstellen** ist nur verfügbar, wenn Sie über die erforderlichen Funktionen verfügen.
10. Wenn Sie die Datenquellenverbindung in der neuen Verwaltungsschnittstelle in **Verwalten** > **Datenserververbindungen**verfügbar machen möchten, klicken Sie für die Verbindung auf die Schaltfläche 'Eigenschaften festlegen'  , und aktivieren Sie auf der Registerkarte **Verbindung** das Kontrollkästchen **Webbasierte Modellierung zulassen** .

Nächste Schritte

Wenn Sie eine Anmeldung erstellt haben, können Sie sie jetzt ändern oder weitere Anmeldungen hinzufügen. Weitere Informationen finden Sie unter „Datenquellensignonen“ auf Seite 141.

Cognos-spezifische Verbindungsparameter

Sie können einige optionale, Cognos-spezifische Parameter für JDBC-Verbindungen angeben.

Sie können diese Parameter bei der Erstellung oder Aktualisierung von JDBC-Verbindungen für Datenquellen in IBM Cognos Administration oder IBM Cognos Framework Manager oder beim Erstellen oder Aktualisieren von Datenserververbindungen in der Verwaltungsschnittstelle von **Verwalten** > **Datenserververbindungen** angeben.

In verschiedenen Verbindungseditoren können diese Parameter als **Verbindungseigenschaften** oder **JDBC-Verbindungsparameter**angegeben werden.

ibmcognos.fetchBufferSize

Dieser Parameter wird verwendet, um die Abrufgröße des JDBC-Treibers für Datenquellenverbindungen in IBM Cognos Analyticsfestzulegen.

Wenn der Abfrageservice in IBM Cognos Analytics Abfragen mithilfe von JDBC ausführt, wird der Wert für die Abrufgröße, der an einen JDBC-Treiber übergeben wird, dynamisch berechnet. Die Unterstützung für Abrufgrößen hängt von den Datenbankanbietern ab. Die Anbieter entscheiden darüber hinaus, was die Abrufgröße bedeutet und was die Abrufgröße ist, wenn sie intern im Treiber und im Server verwendet wird. Weitere Informationen finden Sie in der JDBC-Dokumentation Ihres Anbieters.

Der Abfrageservice berechnet einen Wert für eine Abfrage unter Verwendung der folgenden Formel:
`maximum ((bufferSize/'row-size '), 10)`

Der Standardwert für die Puffergröße beträgt 100 Kilobyte (KB). Die Zeilengröße wird aus der Größe der Spalten berechnet, die von der Ergebnismenge in einer Abfrage projiziert werden. Abfragen, die Spalten mit großer Genauigkeit oder mit vielen Spalten projizieren, verwenden eine kleinere Abrufgröße als diejenigen, die weniger Spalten oder Spalten mit geringerer Genauigkeit projizieren.

Wenn der Abruf einer Ergebnismenge durch die Verwendung einer größeren Puffergröße erheblich verbessert werden kann, kann ein Cognos-Administrator die Verbindungseigenschaft **ibmcognos.fetchBufferSize**angeben. Der Abfrageservice passt den Wert automatisch an, wenn er kleiner als 10 Kilobyte oder größer als 10 Megabyte ist.

If ibmcognos.fetchBufferSize > 1024 * 10240 then bufferSize = 1024 * 10240

If ibmcognos.fetchBufferSize < 10240 then bufferSize = 10240

Größere Abrufgrößen werden nicht immer empfohlen, da sie möglicherweise den Speicherverbrauch des JDBC-Treibers erhöhen und nicht zu einer verbesserten Leistung führen können. Überprüfen Sie immer die Dokumentation des Datenbankanbieters und die empfohlenen Verfahren, bevor Sie große Werte für die Eigenschaft **ibmcognos.fetchBufferSize** verwenden.

ibmcognos.decfloat

Wenn dieser Parameter angegeben wird, wird der Abfrageservice angewiesen, einen Dezimalfloatentyp (DECFLOAT 128) zu verwenden, der genau Werte mit einer Genauigkeit von bis zu 34 Ziffern darstellt. Wenn eine Spalte mit großer Genauigkeit erkannt wird, wird sie intern in DECFLOAT geändert, und der Datentyp im Modell oder Bericht wird als DECIMAL (0, 0) beschrieben.

Um diese Funktion zu aktivieren, geben Sie den Verbindungsparameter **ibmcognos.decfloat=true** für die Datenbankverbindung an, die vom Abfrageservice verwendet wird. In vorhandenen Modellen müssen die Spalten in DECIMAL (0, 0) neu zugeordnet werden, statt doppelt vorhanden zu sein.

Damit der Abfrageservice die Zeilen liest, die von einer Abfrage zurückgegeben werden, muss der JDBC-Treiber die Spaltenwerte mithilfe eines bestimmten Java -Datentyps zurückgeben. In früheren Releases war es möglich, dass eine Datenbank wie ORACLE eine numerische Spalte zurückgibt, bei der die Genauigkeit den Abfrageservice für die Verwendung des Doppeldatentyps verursacht hat. Wenn die Werte, die von einer Abfrage zurückgegeben wurden, eine Genauigkeit von mehr als 16 Ziffern hatten, konnte die Konvertierung zu einem ungenauen Wert führen.

Beispiel: Wenn eine ORACLE-Spalte als NUMBER (ohne Angabe von Genauigkeit) definiert wurde oder ein Aggregat wie SUM berechnet wurde, dass ORACLE als NUMBER zurückgegeben wurde, kann der zurückgegebene Wert 1234567890123456789 in den Wert 1.23456789012345677E18 konvertiert werden. Die beiden Werte sind nicht identisch.

Wenn die Datenbank keine großen Werte zurückgibt, verwenden Sie diesen Parameter nicht und stellen Sie sicher, dass die Modelle Spalten mit dem Datentyp DECIMAL (0, 0) nicht enthalten. Auf diese Weise kann der Abfrageservice einen Datentyp verwenden, der weniger Speicher erfordert als der Typ DECFLOAT.

ibmcognos.qualifikationsliste

Dieser Parameter wird verwendet, um Metadaten zu disambiguieren, wenn dynamische Abfragen ausgeführt werden. Sie ordnet Datenquellen, die in IBM Cognos Analyticsdefiniert sind, eine Liste mit einer oder mehreren Qualifikationsmerkmalen zu.

Die folgenden Beispiele zeigen die Syntax, die bei der Angabe des Parameters **ibmcognos.qualifikationsliste** verwendet werden soll, und die Werte, die für sie zugeordnet werden können:

- ibmcognos.qualifi_list=CATALOG1.SCHEMA1, CATALOG2.SCHEMA2
- ibmcognos.qualifikationsliste = SCHEMA1, SCHEMA2
- ibmcognos.qualifikationsliste = CATALOG1.SCHEMA1, SCHEMA2
- ibmcognos.qualifier_list=CATALOG1, CATALOG2

Ein Punkt im Qualifikationsmerkmal wird verwendet, um die Katalog-und Schemakomponenten zu trennen. Wenn keine Periode vorhanden ist und die Datenbank Schemas unterstützt, wird der Wert als Schema behandelt. Andernfalls wird der Wert als Katalog behandelt, wenn die Datenbank Kataloge unterstützt.

Der Abfrageservice durchsucht die Liste in der angegebenen Reihenfolge und verwendet die Spaltenmetadaten, die für das erste Qualifikationsmerkmal gefunden werden, das mit diesem

übereinstimmt. Wenn keine Übereinstimmung gefunden wird, wird ein mehrdeutiger Metadatenfehler ausgelöst.

Der Administrator sollte bestätigen, dass die Liste der Qualifikationsmerkmale, die für diesen Parameter bereitgestellt werden, in der Reihenfolge und dem Inhalt der Suchliste identisch ist, die von der Datenbanksitzung des Benutzers definiert wurde. Die Liste der Qualifikationsmerkmale wird nur angewendet, wenn die Sitzung versucht, Metadaten, die von einem JDBC-Treiber zurückgegeben werden, zu disambiguieren. Qualifizierte Namen in dynamischen SQL-Anweisungen spiegeln die Werte wider, die den Katalog-oder Schemaeigenschaften zugeordnet sind, die die Paketdatenquelle während der Abfrageplanung verwendet hat.

ibmcognos.authentication

Dieser Parameter wird verwendet, um Datenquellenverbindungen bei der Verwendung der Kerberos-Authentifizierung zu konfigurieren.

Geben Sie für die verschiedenen Datenquellenverbindungstypen **ibmcognos.authentication=java_krb5**an und fügen Sie dann die Eigenschaften hinzu, die vom JDBC-Treiber für die Kerberos-Authentifizierung erforderlich sind, sofern diese erforderlich sind. In den folgenden Beispielen wird gezeigt, wie dieser Parameter für einige Datenquellenverbindungen angegeben wird:

- Geben Sie für Teradata-Verbindungen **ibmcognos.authentication=java_krb5; LOGMECH=KRB5;** an.
- Für SAP-HANA-Verbindungen geben Sie **ibmcognos.authentication=java_krb5;** an.
- Geben Sie für Microsoft SQL Server-Verbindungen **ibmcognos.authentication=java_krb5; authenticationScheme=JavaKerberos;** an.

ibmcognos.maxvarcharsize

Der Abfrageservice kann einen größeren Standard-VARCHAR-Genauigkeitswert verwenden als der Standardwert, der von der Datenbank unterstützt wird. Dieser Parameter wird verwendet, um den Datenbankstandardwert des Typs VARCHAR für den Abfrageservice außer Kraft zu setzen.

Wenn Sie diesen Parameter angeben möchten, verwenden Sie die folgende Syntax, wobei N für einen ganzzahligen Wert größer als null steht, der vom Datenbankanbieter unterstützt wird:

```
ibmcognos.maxvarcharsize=N
```

Der SQL-Standard verwendet den Datentyp CLOB und den großen Objekttyp (NCLOB) für den nationalen Charakter, um große Zeichenwerte zu speichern. Unterschiedliche Datenbanken unterstützen den Datentyp CLOB oder eigene Versionen dieses Typs mit ähnlichen Merkmalen. Der Datentyp CLOB legt mehrere Einschränkungen für die Typen von SQL-Konstrukten fest, die in Abfragen verwendet werden können. Außerdem können Datenbankanbieter zusätzliche Einschränkungen für die Handhabung von CLOB-Spalten in den Clientschnittstellen, wie z. B. JDBC, festlegen. Um CLOB-bezogene Einschränkungen zu vermeiden, konvertiert der Abfrageservice CLOB-Spalten automatisch in VARCHAR-Spalten, indem er die Funktion CAST verwendet. Daher werden die ersten N -Zeichen des CLOB-Typs als VARCHAR an den Abfrageservice zurückgegeben.

Tipp: Die Funktion für automatische CAST wird nicht ausgeführt, wenn ein JDBC-Treiber den Spaltendatentyp als VARCHAR (Feld für variable Zeichen) und nicht als Datentyp CLOB (Character Large Object) beschreibt und wenn der Spaltenverweis eine vom Benutzer angegebene CAST -Funktion umgibt.

Wenn die Länge einer CLOB in einer Zeile größer ist als die CAST -Präzisionsdaten, erfolgt das Abschneiden.

In einigen Fällen kann ein Datenbankanbieter eine größere Genauigkeit unterstützen, wenn bestimmte Einstellungen für die Datenbankkonfiguration, wie z. B. Seiten-und Zeilengröße oder Servereinstellungen, erfüllt sind. Wenn solche Vorbedingungen erfüllt sind, kann für eine Datenserververbindung ein größerer Wert angegeben werden. Wenn die Vorbedingungen nicht erfüllt sind und Sie einen Wert verwenden, der größer ist als der, der von der Datenbank unterstützt wird, werden die SQL-Anweisungen nicht ausgeführt.

Bevor Sie größere VARCHAR-Genauigkeitswerte verwenden, lesen Sie die Dokumentation zu den Datenbankanbietern und überprüfen Sie den Wert mit dem Datenbankadministrator.

Der Abfrageservice verwendet die folgenden standardmäßigen VARCHAR-Genauigkeitswerte für die verschiedenen Datenbanken:

Tabelle 43. Standardpräzisions-VARCHAR-Werte im Abfrageservice

Datenbank	**Standard-VARCHAR-Genauigkeit**
DB2-iSeries	32739
DB2-zSeries	4096
DB2-LUW	8168
Exasol	2000000
Informix Dynamic Server	255
MariaDB	21845
MemSQL	21845
MySQL	65535
Oracle	4000
Schwenkbares Greenplum	2000000
PostgreSQL	2000000
SAP Hana	5000
SQL Server	varchar (max)
Teradata	32000
Andere Anbieter	1024

Wenn der Wert für `ibmcognos.maxvarcharsize` höher ist als der Wert für "Java Integer max" (2147483647) oder nicht für eine ganze Zahl, wird der Wert ignoriert.

Wenn der `ibmcognos.maxvarcharsize` -Wert niedriger ist als der Standardwert von 1024 und der Größe des Anbieters VARCHAR, wird der niedrigste Wert dieser beiden Werte anstelle des Werts von `ibmcognos.maxvarcharsize` verwendet.

ibmcognos.typeinsqldisabled

Wenn diese Eigenschaft angegeben wird, sind Abfragen, die auf typisierten SQL basieren, von der Verbindung nicht zulässig. Diese Eigenschaft wird für Datenmodule mit Sicherheitsfiltern benötigt, um Sicherheitslücken zu verhindern, die in SQL eingegeben werden können.

Wenn Sie versuchen, eine SQL-basierte Tabelle zu erstellen, nachdem diese Eigenschaft angegeben wurde, wird die Tabelle nicht erstellt. Wenn Sie diese Eigenschaft angeben, nachdem eine SQL-basierte Tabelle erstellt wurde, wird die Abfrageausführung gestoppt.

Diese Einschränkungen gelten für alle Datenmodule, die auf Verbindungen basieren, für die diese Eigenschaft angegeben ist. Um diese Einschränkungen zu umgehen, erstellen Sie eine separate Datenserververbindung für Datenmodule mit Sicherheitsfiltern, und geben Sie diese Eigenschaft nur für diese Verbindung an. Andere Verbindungen zu demselben Datenserver, für die diese Eigenschaft nicht angegeben ist, können Abfragen auf der Basis von typisierten SQL verarbeiten.

Verbindungen von IBM Weather Company

Sie können einige optionale Parameter in der Verbindungs-URL oder in den Verbindungseigenschaften für die IBM Weather Company angeben.

Geben Sie die JDBC-URL im folgenden Format an:

```
jdbc:twc://[database][?properties]
```

Dabei ist *Datenbank* optional und gibt den Namen der Datenbank an, und *Eigenschaften* ist null oder mehr der Parameter, die in der folgenden Tabelle beschrieben sind. Trennen Sie die einzelnen Parameter durch ein Komma.

Anmerkung: Außerdem müssen Sie in der Datenquellenverbindung mindestens eine Anmeldung konfigurieren. Das Kennwort muss Ihr API-Schlüssel von Weather Company sein. Weitere Informationen finden Sie unter *Mustercode 'Weather Company' importieren* in der *Handbuch für Beispiele*.

Parameter	**Beschreibung**
UNITS	Maßeinheit. In der folgenden Liste sind die gültigen Werte aufgeführt: **e oder E** Imperial oder Englisch **m oder M** Messwert **s oder S** Internationales System der Einheiten Es wird eine Ausnahme ausgelöst, wenn ein nicht unterstützter Wert angegeben wird.
SPRACHE	Zeichenfolge im Format xx-XX. Momentan ist der einzige unterstützte Wert de-US. Es wird eine Ausnahme ausgelöst, wenn der Wert nicht im Format xx-XXangegeben ist.
MAX_STATEMENTS	Ganze Zahl Die maximale Anzahl gleichzeitiger Anforderungen, die über die Verbindung an The Weather Company gesendet werden. Der Wert muss größer oder gleich 1 sein. Der Standardwert ist 15. Es wird eine Ausnahme ausgelöst, wenn ein nicht unterstützter Wert angegeben wird.
CACHE_SIZE	Ganze Zahl Die Anzahl der Ergebnisse, die von der Verbindung zwischengespeichert wurden. Um sicherzustellen, dass aktuelle Informationen zurückgegeben werden, wird das Caching für eine Anforderung an die Prognose für den Bedarfsservice nicht ausgeführt. Der Wert muss größer als oder gleich 0 sein. 0 bedeutet kein Caching. Der Standardwert ist 100 (MB des Bereichs). Es wird eine Ausnahme ausgelöst, wenn ein nicht unterstützter Wert angegeben wird.
CACHE_TTL	Zeit zum Leben in Sekunden für eine Ergebnismenge im Cache. Ein Ergebnis wird entfernt, wenn es älter als dieser Wert ist. Der Wert muss größer oder gleich 1 sein. Der Standardwert ist 86400 (24 Stunden). Es wird eine Ausnahme ausgelöst, wenn ein nicht unterstützter Wert angegeben wird.

Parameter	Beschreibung
CACHE_DIR	Der Ordner, in den die Ergebnisse zwischengespeichert werden. Der Standardwert ist der Ordner, der von der Java Runtime Environment (`java.io.tmpdir`) verwendet wird. Die Cognos-Prozesse, die auf dem Computer ausgeführt werden, müssen über Schreib-/Lesezugriff auf den Ordner verfügen. Der Ordner wird erstellt, wenn er nicht vorhanden ist. Wenn die Position nicht zugänglich ist, schlagen die Verbindungen fehl.
QUERY_TIMEOUT	Die Anzahl der Sekunden, nach denen eine Abfrage das Zeitlimit überschreitet. Der Standardwert ist 60 Sekunden. Es wird eine Ausnahme ausgelöst, wenn ein nicht unterstützter Wert angegeben wird.
PROXY_HOST, PROXY_PORT	Der Hostname und der Port eines HTTP-Caching-Service. Bei Abfragen an den The Weather Company -Server handelt es sich um REST (HTTP). Sie legen diese Parameter fest, um Anforderungen an den HTTP-Caching-Service zu senden, der die Abfragen dann an den The Weather Company -Server sendet.
FILTER_METADATA	Boolesch Der Standardwert ist 'false'. Wenn ein neues Modell (Framework Manager oder Datenmodul) erstellt wird, enthält der Import Metadaten für alle Produkte, die über den The Weather Company -Server verfügbar sind. Wenn dieser Wert wahr ist, enthalten die Metadaten nur die Produkte, für die der API-Schlüssel berechtigt ist, abzufragen. Der API-Schlüssel wird in dem Kennwort in der Verbindungszeichenfolge angegeben.

Im folgenden Beispiel werden nur die Objekte importiert, die für den The Weather Company -API-Schlüssel verfügbar sind, der der Anmeldung zugeordnet ist. Eine Abfrage kann bis zu 250 MB Speicher verwenden.

```
jdbc:twc://?FILTER_METADATA=true,CACHE_SIZE=250
```

Neue Verbindung hinzufügen

Sie können eine neue Verbindung für eine vorhandene Datenquelle erstellen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Datenquellenverbindungen**.
2. Klicken Sie auf die Datenquelle, für die Sie eine neue Verbindung hinzufügen möchten.

   Tipp: Wenn Sie eine Datenquellenverbindung entfernen möchten, wählen Sie das entsprechende Kontrollkästchen aus, und klicken Sie auf die Schaltfläche zum Löschen.
3. Klicken Sie auf die neue Verbindungsschaltfläche  .
4. Geben Sie auf der Seite "Name und Beschreibung" einen eindeutigen Namen für die Verbindung und optional eine Beschreibung und einen Anzeigentipp ein, und klicken Sie anschließend auf **Weiter**.
5. Fahren Sie mit den Schritten 5 bis 10 in „Datenquellenverbindung erstellen” auf Seite 131fort.

Ergebnisse

Wenn Sie eine Anmeldung erstellt haben, können Sie sie jetzt ändern oder weitere Anmeldungen hinzufügen. Weitere Informationen finden Sie unter „Datenquellensignonen" auf Seite 141.

Vorhandene Verbindung ändern

Sie können neue Datenquellenverbindungen hinzufügen oder vorhandene Verbindungen bearbeiten.

Sie können mehrere Verbindungen zu einer vorhandenen Datenquelle hinzufügen. Beispiel: Sie möchten, dass eine Datenquelle über zwei oder mehr Verbindungen zu derselben Datenbank verfügt, die unterschiedliche Eigenschaften haben, wie z. B. unterschiedliche Zeitlimitwerte oder Zugriffsberechtigungen. Sie können auch Verbindungen zu einer Datenquelle hinzufügen, die auf verschiedene Datenbanken verweisen, aber die Datenbanken müssen dasselbe Schema enthalten.

Wenn Sie eine Datenquellenverbindung erstellen, können Sie eine Anmeldung erstellen, die von der Gruppe "Jeder" für den Zugriff auf die Datenbank verwendet werden kann. Später können Sie ändern, wer diese Anmeldedaten verwenden oder mehr Anmeldungen erstellen kann. Sie können zum Beispiel den Zugriff auf Daten steuern, indem Sie die Berechtigungen für jede Datenquellenverbindung festlegen. Weitere Informationen finden Sie unter „Zugriffsberechtigungen für einen Eintrag festlegen" auf Seite 200.

Wenn Sie eine Datenquellenverbindung hinzufügen oder ändern möchten, müssen Sie Zugriff auf die erforderlichen Funktionen für die Verwaltung von Datenquellen haben (siehe Kapitel 13, „Funktionen", auf Seite 207).

Wenn Sie eine Oracle-, IBM Db2-oder Microsoft SQL Server-Datenquelle erstellen, können Sie Datenbankbefehle in die Verbindungsinformationen einschließen. Weitere Informationen finden Sie unter „IBM Cognos-Kontext an eine Datenbank übergeben" auf Seite 145.

Informationen zum Festlegen der maximalen Anzahl von Datenquellenverbindungen, die für den Berichtsserver verfügbar sind, finden Sie unter „Verbindungseinstellungen ändern" auf Seite 139.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Datenquellenverbindungen**.
2. Klicken Sie auf die Datenquelle, für die Sie die Verbindung ändern möchten.
3. Klicken Sie auf die Schaltfläche 'Eigenschaften festlegen'  für die Verbindung, die Sie ändern möchten.
4. Klicken Sie auf die Registerkarte **Verbindung** .
5. Wenn Sie den Datenquellentyp ändern möchten, klicken Sie auf ein Element in der Dropdown-Liste **Typ** .
6. Klicken Sie auf das Bearbeitungssymbol  , um die Verbindungszeichenfolge zu ändern.
7. Fahren Sie mit den Schritten 5 bis 10 in „Datenquellenverbindung erstellen" auf Seite 131fort.

Verbindungseinstellungen ändern

Sie können die maximale Anzahl verfügbarer Datenquellenverbindungen, die Dauer für die Verbindung von Verbindungen und die Verwendung von Datenquellenverbindungen festlegen.

Jede Instanz des Berichtsservers verfügt über einen festgelegten Pool an Datenbankverbindungen. Die Verbindungen werden für neue Anforderungen, die mit der Datenbank, dem Benutzer und dem Kennwort übereinstimmen, wiederverwendet. Einträge bleiben im Pool, bis sie für eine Zeitlimitperiode inaktiv sind und dann geschlossen werden. Sobald ein Pool voll ist, werden keine weiteren Verbindungen hinzugefügt. Dies führt zu einem Anforderungsfehler.

Poolgröße

Gibt die maximale Anzahl der Datenquellverbindungen an, die für den Berichtsserver verfügbar sind.

Zeitlimit

Gibt die Zeitdauer für Halteverbindungen an. Verbindungen werden einmal pro Minute untersucht, und jede Verbindung, die länger inaktiv war als der Zeitlimitwert, wird entfernt.

Standardwert: 900 Sekunden

Wiederverwendbare Datenverbindungen

Datenquellenverbindungen sind nur dann wiederverwendbar, wenn die Datenbankberechtigungsnachweise der Verbindung mit denen der neuen Anforderung übereinstimmen. Inaktive Datenquellenverbindungen können durch eine neue Anforderung beansprucht werden. Dies tritt auf, wenn die maximale Anzahl an Verbindungen erreicht wurde und keine der inaktiven Verbindungen von der neuen Anforderung verwendet werden kann. In diesem Fall wird die älteste inaktive Verbindung beendet und es wird eine neue Verbindung erstellt.

Wenn die maximale Anzahl an Verbindungen erreicht ist und alle aktiv sind, schlagen weitere Anforderungen fehl. Der Server muss so konfiguriert sein, dass die gleichzeitigen Berichtsanforderungen die Größe des Anforderungspools nicht überschreiten.

Weitere Informationen zu Berichtsserviceanforderungen finden Sie im Artikel „Maximale Anzahl Prozesse und Verbindungen“ auf Seite 68.

Vorgehensweise

1. Öffnen Sie auf jedem Computer, auf dem IBM Cognos Analytics installiert ist, die *Installationsposition*/configuration/CQEConfig.xml.sample -Datei in einem Texteditor.

   Stellen Sie sicher, dass Ihr Editor das Speichern von Dateien im UTF-8-Format unterstützt.
2. Suchen Sie die Zeitlimit -und Poolgröße -Parameter, und bearbeiten Sie sie wie folgt:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration company="Cognos" version="#.#"
rendition="###">
  <component name="CQE">
    <section name="DBConnectionPool">
      <!-- Description: Database connection timeout.
       Default is 900 seconds (15minutes) -->
      <entry name="Timeout" value="number_of_seconds"/>
      <!-- -->
      <!-- Description: Database connection pool size. -->
      <!-- Maximum number of connections managed by the report
           server. Default=50 -->
      <entry name="PoolSize" value="number_of_connections"/>
    </section>
  </component>
</configuration>
```

3. Speichern Sie die Datei als CQEConfig.xml in dem Verzeichnis *Installationsposition*/configuration .
4. Stoppen Sie den IBM Cognos -Service, indem Sie IBM Cognos konfigurieren, stoppen und anschließend erneut starten.

   Informationen zum Stoppen von Services finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Dynamische Verbindungsparameter in JDBC-Verbindungen

Eine JDBC-Verbindung zu einer Datenquelle gibt eine statische Gruppe von Werten an, die von der Abfrageengine an den JDBC-Treiber übergeben werden.

Umgebungen wie Apache Hive oder Cloudera Impala können Funktionen unterstützen, wie z. B. Identitätsdelegierung, die dynamische Werte erfordern, die von der Abfrageengine übergeben werden müssen. Sie können Sitzungsvariablen in den Feldern **JDBC-URL** und **Verbindungseigenschaften** angeben. Das Feld **JDBC-URL** kann z. B. das folgende Name/Wert-Paar enthalten:

```
hive.server2.proxy.user=#$account.defaultName#
```

Wenn die Abfrageengine eine neue Datenbankverbindung erstellt, ersetzt sie die Sitzungsvariablen durch ihren entsprechenden Wert. Wenn eine Sitzungsvariable nicht vorhanden ist, wird der Variablenname ohne Wert an seiner Stelle entfernt, was dazu führen kann, dass der Treiber die Verbindung zurückweist.

Anmerkung: Makrofunktionen können nicht verwendet werden. Es werden nur Verweise auf Sitzungsvariablen unterstützt.

Datenquellensignonen

Sie fügen den Datenquellenverbindungen signons hinzu, damit Benutzer bei der Ausführung von Berichten keine Datenbankberechtigungsnachweise eingeben müssen.

Wenn Sie eine Anmeldung erstellen, geben Sie die Benutzer und Gruppen an, die auf den Anmeldebereich zugreifen können. Die Benutzer-ID und das Kennwort, die das Anmeldezeichen bilden, müssen bereits in der Datenbank definiert sein.

Sie können eine vorhandene Anmeldung ändern, wenn sich die für die Anmeldung bei der Datenbankänderung verwendeten Berechtigungsnachweise ändern oder wenn Sie Änderungen vornehmen möchten, die die Anmeldung verwenden können.

Bei Datenquellenkonfigurationen, bei denen jeder Benutzer über seine eigenen Anmeldedaten verfügt, kann es unhandlich sein, alle Benutzer zu verwalten. Informationen dazu, wie Benutzer ihre eigenen Datenquellen-Berechtigungsnachweise verwalten können, finden Sie unter „Eigene Datenquellen-Berechtigungsnachweise verwalten“ auf Seite 204.

Signon erstellen

Die Datenquellenverbindung signon muss definiert sein, damit der Abfrageservice automatisch auf die Datenzugreifen kann.

Informationen zu diesem Vorgang

Eine Datenquellenverbindung muss mindestens eine Anmeldung haben, die der Abfrageservice verwenden kann, um eine Verbindung zur Datenquelle herzustellen. Wenn die Datenquellenverbindung zwei oder mehr Anmeldungen hat, muss einer der Anmeldungen den Namen `Dynamische Cubes`haben. Diese Anmeldung wird vom Abfrageservice verwendet, um eine Verbindung zur Datenquelle herzustellen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Datenquellenverbindungen**.
2. Klicken Sie auf die Datenquelle, und klicken Sie dann auf die Verbindung, zu der Sie einen neuen Anmeldetext hinzufügen möchten.
3. Klicken Sie auf die neue Anmeldeschaltfläche  .
4. Geben Sie auf der Seite für den Namen und die Beschreibung einen eindeutigen Namen für die Datenquellenanmeldung und, wenn Sie möchten, eine Beschreibung und eine Anzeigenspitze ein und klicken Sie dann auf **Weiter**.
5. Geben Sie den **Benutzer-ID** und den **Kennwort** ein, um eine Verbindung zur Datenbank herzustellen, und klicken Sie auf **Weiter**.

   Die Seite **Benutzer auswählen** wird angezeigt.
6. Zum Hinzufügen von Benutzern und Gruppen, die die Anmeldung verwenden können, und klicken Sie auf **Hinzufügen**.

   · Wenn Sie aus aufgelisteten Einträgen auswählen möchten, klicken Sie auf den entsprechenden Namespace und wählen Sie anschließend die Kontrollkästchen neben den Benutzern, Gruppen oder Rollen aus.

- Um nach Einträgen zu suchen, klicken Sie auf **Suchen** und geben Sie in das Feld **Suchbegriff** den Ausdruck ein, nach dem gesucht werden soll. Klicken Sie für Suchoptionen auf **Bearbeiten**. Suchen und klicken Sie auf den gewünschten Eintrag.
- Wenn Sie den Namen der Einträge eingeben möchten, die hinzugefügt werden sollen, klicken Sie auf **Typ** , und geben Sie die Namen von Gruppen, Rollen oder Benutzern ein. Verwenden Sie dabei das folgende Format, wobei ein Semikolon (;) jeden Eintrag trennt:

  Namensbereich/group_name; -Namespace/role_name; -Namensbereich/Benutzername;

  Im Folgenden sehen Sie ein Beispiel:

  Cognos/Authors; LDAP/scarter;

7. Klicken Sie auf die Schaltfläche mit der Rechtspfeiltaste, und klicken Sie auf **OK**, wenn die gewünschten Einträge im Feld **Ausgewählte Einträge** angezeigt werden.

   Tipp: Wenn Sie Einträge aus der Liste **Ausgewählte Einträge** entfernen möchten, wählen Sie sie aus und klicken Sie auf **Entfernen**. Um alle Einträge in einer Liste auszuwählen, wählen Sie in der Titelleiste für die **Name** -Liste das Kontrollkästchen aus. Um die Benutzereinträge sichtbar zu machen, klicken Sie auf **Benutzer in der Liste anzeigen**.
8. Klicken Sie auf **Fertigstellen**.

   Die neue Datenquellenanmeldung wird unter der Verbindung angezeigt.

Signon ändern

Sie können eine vorhandene Anmeldung ändern.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Datenquellenverbindungen**.
2. Klicken Sie auf die Datenquelle, und klicken Sie dann auf die Verbindung, für die Sie die Anmeldung ändern möchten.

   Tipp: Wenn Sie eine Anmeldung entfernen möchten, wählen Sie das entsprechende Kontrollkästchen aus, und klicken Sie auf die Schaltfläche zum Löschen.
3. Klicken Sie auf die Schaltfläche 'Eigenschaften festlegen'  für die Anmeldung, die Sie ändern möchten.
4. Klicken Sie auf die Registerkarte **Anmeldung** .

   Eine Liste der Benutzer und Gruppen, die die Anmeldung verwenden können, wird angezeigt.
5. Wenn Sie die Benutzer-ID und das Kennwort ändern möchten, die die Anmeldung durchführen, klicken Sie auf **Signon bearbeiten**, geben Sie die neuen Berechtigungsnachweise ein, und klicken Sie auf **OK**.
6. Wenn Sie Benutzer oder Gruppen zur Anmeldeliste hinzufügen möchten, klicken Sie auf **Hinzufügen**, und wählen Sie aus, wie Benutzer und Gruppen ausgewählt werden sollen:
   - Wenn Sie aus aufgelisteten Einträgen auswählen möchten, klicken Sie auf den entsprechenden Namespace und wählen Sie anschließend die Kontrollkästchen neben den Benutzern, Gruppen oder Rollen aus.
   - Um nach Einträgen zu suchen, klicken Sie auf **Suchen** und geben Sie in das Feld **Suchbegriff** den Ausdruck ein, nach dem gesucht werden soll. Klicken Sie für Suchoptionen auf **Bearbeiten**. Suchen und klicken Sie auf den gewünschten Eintrag.
   - Wenn Sie den Namen der Einträge eingeben möchten, die hinzugefügt werden sollen, klicken Sie auf **Typ** , und geben Sie die Namen von Gruppen, Rollen oder Benutzern ein. Verwenden Sie dabei das folgende Format, wobei ein Semikolon (;) jeden Eintrag trennt:

     namespace/group_name;*namespace/role_name*;*namespace/user_name*;

     Im Folgenden sehen Sie ein Beispiel:

Cognos/Authors; LDAP/scarter;

7. Klicken Sie auf die Schaltfläche mit der Rechtspfeiltaste, und klicken Sie auf **OK**, wenn die gewünschten Einträge im Feld **Ausgewählte Einträge** angezeigt werden.

   Tipp: Wenn Sie Einträge aus der Liste **Ausgewählte Einträge** entfernen möchten, wählen Sie sie aus und klicken Sie auf **Entfernen**. Wenn Sie alle Einträge in der Liste auswählen möchten, wählen Sie das Kontrollkästchen für die Liste aus. Um die Benutzereinträge sichtbar zu machen, klicken Sie auf **Benutzer in der Liste anzeigen**.
8. Klicken Sie auf **OK**.

Isolationsstufen

Sie können Isolationsstufen für Datenquellen angeben.

Die Isolationsstufe gibt an, wie Transaktionen, die die Datenbank modifizieren, verarbeitet werden. Standardmäßig wird das Standardobjektgateway verwendet. Nicht alle Typen von Datenbanken unterstützen jede Isolationsstufe. Einige Datenbankanbieter verwenden unterschiedliche Namen für die Isolationsstufen.

Abfragen, die von Berichten und Analysen ausgeführt werden, sollen schreibgeschützte Operationen sein. Die Abfragen werden mit einer UOW (Unit of Work) an der Datenquelle ausgeführt, die als Transaktion mit einer Standardisolationsstufe oder einer vom Administrator definierten Isolationsstufe bezeichnet wird. Berichtsersteller sollten nicht davon ausgehen, dass Abfragen, die gespeicherte Prozeduren ausführen, alle Daten festschreiben, die von der Prozedur geschrieben wurden. In einigen Umgebungen können Änderungen, die von einer Prozedur vorgenommen werden, aufgrund von Features der Datenbank festgeschrieben werden. Eine gespeicherte Prozedur, die für den Schreibvorgang in Framework Manager markiert ist, schreibt Änderungen fest, kann aber nur von Event Studio verwendet werden.

Wenn Sie bestimmte Abfragen für die Ausführung mit unterschiedlichen Isolationsstufen benötigen, müssen Sie unterschiedliche Datenbankverbindungen definieren.

Für OLAP-Datenquellen, einschließlich SAP BW, ist die Transaktionseinheit der Arbeit schreibgeschützt.

Die folgenden Isolationsstufen sind in der Reihenfolge der Isolation zu finden:

· Nicht festgeschriebenes Lesen

  Änderungen, die von anderen Transaktionen vorgenommen werden, sind sofort für eine Transaktion verfügbar.

Tabelle 44. Nicht festgeschriebene Datenbanktypen und gleichwertige Isolationsstufen lesen

Datenbanktyp	**Gleichwertige Isolationsstufe**
Oracle	Nicht zutreffend
Db2	Nicht festgeschriebenes Lesen
Microsoft SQL Server	Nicht festgeschriebenes Lesen
Sybase Adaptive Server Enterprise	Nicht festgeschriebenes Lesen
Informix	Verschmutztes Lesen

· Festgeschriebenes Lesen

  Eine Transaktion kann nur auf Zeilen zugreifen, die von anderen Transaktionen festgeschrieben wurden.

Tabelle 45. Festgeschriebene Datenbanktypen und äquivalente Isolationsstufen lesen	
Datenbanktyp	**Gleichwertige Isolationsstufe**
Oracle	Lesevorgang
Db2	Cursorstabilität
Microsoft SQL Server	Lesevorgang
Sybase Adaptive Server Enterprise	Lesevorgang
Informix	Engagiertes Lesen

· Cursorstabilität

Andere Transaktionen können die Zeile, in der eine Transaktion positioniert ist, nicht aktualisieren.

Tabelle 46. Datenbanktypen für Cursorstabilität und gleichwertige Isolationsstufen	
Datenbanktyp	**Gleichwertige Isolationsstufe**
Oracle	Nicht zutreffend
Db2	Nicht zutreffend
Microsoft SQL Server	Nicht zutreffend
Sybase Adaptive Server Enterprise	Nicht zutreffend
Informix	Cursorstabilität

· Reproduzierbare Lesevorgänge

Zeilen, die von einer Transaktion ausgewählt oder aktualisiert wurden, können erst durch eine andere Transaktion geändert werden, wenn die Transaktion abgeschlossen ist.

Tabelle 47. Reproduzierbare Lesedatenbanktypen und gleichwertige Isolationsstufen	
Datenbanktyp	**Gleichwertige Isolationsstufe**
Oracle	Nicht zutreffend
Db2	Lesestabilität
Microsoft SQL Server	Wiederholbares Lesen
Sybase Adaptive Server Enterprise	Wiederholbares Lesen
Informix	Wiederholbares Lesen

· Phantom-Schutz

Eine Transaktion kann nicht auf Zeilen zugreifen, die seit dem Start der Transaktion eingefügt oder gelöscht wurden.

Tabelle 48. Phantomschutzdatenbanktypen und gleichwertige Isolationsstufen	
Datenbanktyp	**Gleichwertige Isolationsstufe**
Oracle	Nicht zutreffend
Db2	Nicht zutreffend
Microsoft SQL Server	Nicht zutreffend
Sybase Adaptive Server Enterprise	Nicht zutreffend
Informix	Nicht zutreffend

- Serialisierbar

  Eine Gruppe von Transaktionen, die gleichzeitig ausgeführt werden, erzeugt dasselbe Ergebnis, als wenn sie nacheinander ausgeführt wurden.

Tabelle 49. Serialisierbare Datenbanktypen und äquivalente Isolationsstufen	
Datenbanktyp	**Gleichwertige Isolationsstufe**
Oracle	Serialisierbar
Db2	Wiederholtes Lesen
Microsoft SQL Server	Serialisierbar
Sybase Adaptive Server Enterprise	Serialisierbar
Informix	Nicht zutreffend

IBM Cognos-Kontext an eine Datenbank übergeben

Datenbankadministratoren möchten Details zu Anwendungen kennen, die eine Verbindung zu ihren Datenbanksystemen herstellen. Diese Informationen können für die Prüfung, das Workload-Management und die Fehlerbehebung verwendet werden.

Die Informationen zu IBM Cognos -Anwendungen können über die Befehlsblöcke für die Datenquellenverbindung an die Datenbanken übergeben werden.

Abhängig vom Abfragemodus unterstützen Befehlsblöcke diese Datenquellverbindungen:

- Im Kompatiblen Abfragemodus (CQM), ORACLE (OR), IBM Db2 (D2), Teradata (TD), SQL Server (SS) und Netezza (NZ).
- Im dynamischen Abfragemodus (DQM) alle Datenquellverbindungen, die über JDBC unterstützt werden.

Weitere Informationen finden Sie unter „Befehlsblöcke“ auf Seite 146.

Für Db2können Verbindungsattribute auch als ein Mittel zum Übergeben von Informationen zu den Cognos -Anwendungen verwendet werden. Weitere Informationen finden Sie unter „Verwenden von IBM Db2 CLI-Verbindungsattributen für Db2“ auf Seite 152.

IBM Cognos software can provide information about its reporting applications and users who access the applications, including the default set of information about authenticated users that is retrieved from authentication providers. Die Informationen können erweitert werden, indem Sie angepasste Namensbereichszuordnungen in IBM Cognos -Konfiguration angeben. Weitere Informationen zu den Zuordnungen finden Sie im *IBM Cognos Analytics-Installations-und Konfigurationshandbuch*.

Befehlsblöcke

Verbindungsbefehlsblöcke sollen den Sitzungsstatus in einer Verbindung ändern, die in einer Datenquelle geöffnet wird. Die Anweisungen, die in den Befehlsblöcken verwendet werden können, hängen von den Anweisungen ab, die von Datenbankanbietern unterstützt werden, sowie von den Berechtigungen des Benutzers für diese Anweisungen. Anweisungen in Befehlsblöcken können mithilfe von IBM Cognos -Sitzungsvariablen und Makrofunktionen parametrisiert werden.

Befehlsblöcke werden als IBM Cognos -Software ausgeführt, und schließen Datenbankverbindungen oder -sitzungen für Verbindungen. Sie können Befehlsblöcke verwenden, um native SQL-Befehle auszuführen, z. B., um eine gespeicherte Prozedur auszuführen, wenn eine Sitzung geöffnet wird.

Die folgenden Typen von Befehlsblöcken sind verfügbar:

- **Verbindungsbefehle öffnen**
- **Sitzungsbefehle öffnen**
- **Sitzungsbefehle schließen**
- **Verbindungsbefehle schließen**

Als Administrator müssen Sie wissen, wann ein Befehlsblock für eine Datenbankverbindung ausgeführt wird. Häufig ist es am besten, die Datenbankanweisungen in einem offenen Sitzungsbefehlsblock zu definieren. Offene Datenbankverbindungen werden weniger häufig ausgeführt, weil IBM Cognos Datenbankverbindungen erstellt und erneut verwendet. Verwenden Sie offene Sitzungsbefehlsblöcke, wenn sich der Anwendungskontext einer Datenbankverbindung häufig ändert.

Befehlsblöcke sollten keine Cognos -Sitzungsvariablen oder Makros enthalten, die die Werte häufig ändern. Diese Typen von Sitzungsvariablen oder -makros erhöhen die Befehlsblockausführungshäufigkeit und die Anzahl der Datenquellencaches und reduzieren die Wiederverwendung des Ergebnissetcache.

Beachten Sie bei der Erstellung der Befehlsblöcke die folgenden Einstellungen für die Datenbankverbindung:

- Was sind die Einstellungen für den Datenbankverbindungspool, die für die Berichtsserver in der Datei `CQEConfig.xml` angegeben wurden?
- Verfügt die Datenbank über aggressive Einstellungen für das Zeitlimit für inaktive Verbindungen?
- Hat die Abfrageengine eine aggressive Einstellung für das Zeitlimit für inaktive Verbindungen?
- Ist der Zeitraum zwischen Anforderungen länger als die Zeitlimiteinstellungen?
- Gibt es Anforderungen, die an verschiedene Berichtsserver weitergeleitet werden, die neue Verbindungen erstellen müssen?

Das folgende Diagramm zeigt ein Beispiel für die Interaktion zwischen den vier Typen von Befehlsblöcken. Die Interaktion wird gestartet, wenn eine Abfrage für den Benutzer eintrifft. Es wird davon ausgegangen, dass eine Verbindung zur Datenbank nicht vorhanden ist.

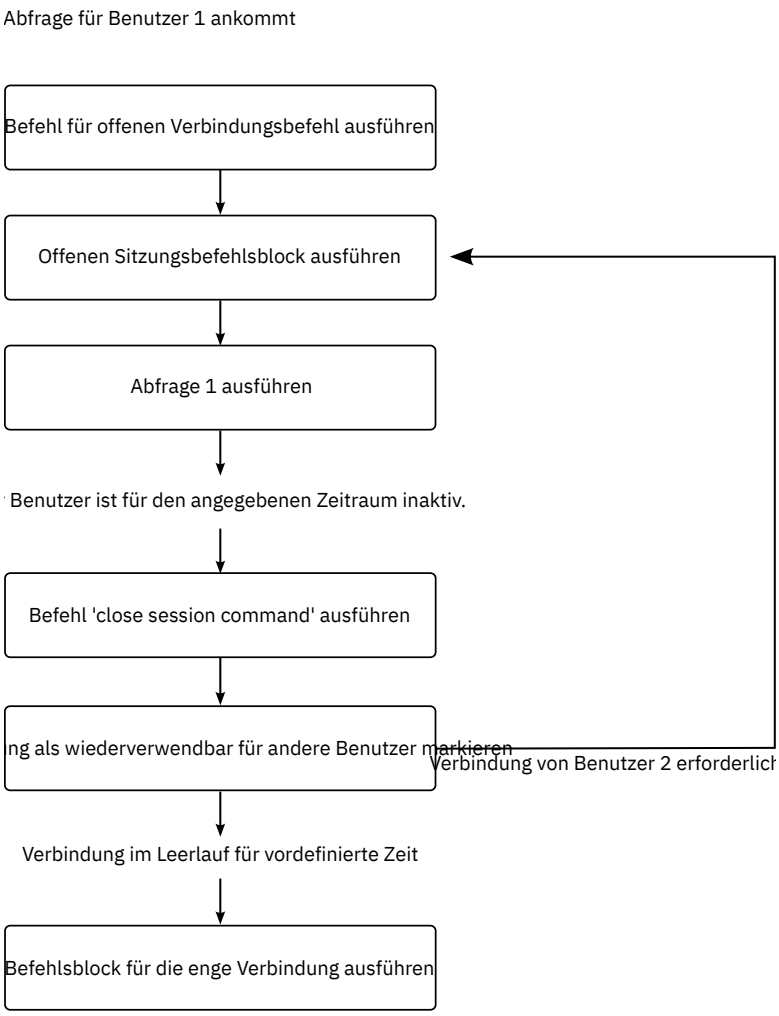


Abbildung 3. Beispiel für die Interaktion zwischen Befehlsblöcken

Makrofunktionen

Die Makrofunktionen, die in der IBM Cognos -Software verfügbar sind, können Informationen in einem Befehlsblock über Benutzer bereitstellen und Anwendungsobjekte, wie z. B. Pakete, Berichte oder Abfragen, melden. Alle Makrofunktionen können Werte zurückgeben, wenn sie von einem Befehlsblock referenziert werden, wodurch der Anwendungskontext von einem Befehlsblock an die Datenbank übergeben werden kann. Makrofunktionen, die auf Parameterzuordnungen in einem Modell verweisen, können ebenfalls verwendet werden.

Hinweise

- Sie können die Befehlsblöcke für Verbindungen, die den Link **Verbindung testen** auf der Seite mit den Verbindungseigenschaften verwenden, nicht testen. Wenn das Software Development Kit installiert ist, können Sie sicherstellen, dass Ihr XML-Code anhand der Schemadatei *c10_location*/webapps/p2pd/WEB-INF/classes/ DataSource.xsdvalidiert wird.
- Die Befehlsstruktur ist für alle Datenquellen identisch. Die spezifischen Datenbankbefehle können jedoch abhängig von der verwendeten Datenbank variieren. In diesem Abschnitt werden die Befehle Oracle und IBM Db2 verwendet.
- Die Befehle in den Blöcken sind herstellerspezifisch und müssen in den Tag < sqlCommand> eingeschlossen werden.
- Abhängig von Ihren Einstellungen kann die Abfrageengine neue Verbindungen schneller öffnen als in einer normalerweise geladenen Anwendung. Dies kann einen falschen Eindruck erzeugen, dass

Informationen für jede ausgeführte Anforderung zurückgesetzt werden. Sie können dieses Verhalten steuern, indem Sie den Governor von **(DQM) Cache ist für Verbindungsbefehlsblöcke sensitiv** verwenden. Weitere Informationen finden Sie im Artikel zu den Framework Manager-Governors für den dynamischen Abfragemodus in *IBM Cognos Framework Manager-Benutzerhandbuch*.

Beispiel-Verbindungsbefehlsblock öffnen

Im Folgenden sehen Sie ein Beispiel für die Verwendung eines Befehlsblocks für die offene Verbindung, um Französisch als Sprache für eine Oracle-Verbindung festzulegen.

```
<commandBlock>
  <commands>
   <sqlCommand>
    <sql>ALTER SESSION SET NLS_LANGUAGE = FRENCH</sql>
   </sqlCommand>
  </commands>
</commandBlock>
```

Beispiel-Verbindungsbefehlsblock schließen

Im Folgenden sehen Sie ein Beispiel für die Verwendung eines Befehlsblocks für die enge Verbindung zum Zurücksetzen der Sprache auf Englisch, bevor eine Verbindung zu einer Oracle-Datenbank getrennt wird.

```
<commandBlock>
  <commands>
   <sqlCommand>
    <sql>ALTER SESSION SET NLS_LANGUAGE = ENGLISH</sql>
   </sqlCommand>
  </commands>
</commandBlock>
```

Beispiel-Informationen zum Kennenlassen von Anforderungen

Im Folgenden sehen Sie ein Beispiel für einen IBM Db2 -Befehlsblock für geöffnete Sitzungen, der bei der Ausführung eine Gruppe von Parametern generiert, die an eine benutzerdefinierte Prozedur übergeben werden sollen.

Das Beispiel kombiniert Makrofunktionen, um sicherzustellen, dass die Werte als gültige Zeichenfolgeliterale und Zeichenfolgeliterationen mit einigen Literalen generiert werden. Die Variable "modelPath" ist ein Beispiel dafür, wie auf die Eigenschaften einer Anforderung zugegriffen werden kann, die beim Ausführen des Blocks verarbeitet wurde.

```
<commandBlock>
    <commands>
        <sqlCommand>
            <sql> CALL myproc(#sq($current_timestamp) + ',' +
            sq($machine) + ',' +
            sq(#$modelPath}#) + 'Constant1'''#)
            </sql>
        </sqlCommand>
    </commands>
</commandBlock>
```

Nachdem das Makro erweitert wurde, ruft der Datenbankadministrator die folgenden Informationen zu der Abfrage ab:

CALL myproc ('2009-05-27 08 :13:33.425-05:00', 'USERCOMPUTERNAME' ,'/content/package [@name= ''EAPPS ''] /model [@name= '' model' ']', 'Constant1', '')

Beispiel-Parameterzuordnungen verwenden

Dieses IBM Db2 -Beispiel zeigt, wie ein Datenbankadministrator Modellinformationen abrufen kann.

Ein Anwendungsstandard kann darin bestehen, eine Parameterzuordnung zu definieren, die in allen Modellen angezeigt wird. Die Parameterzuordnung definiert Kontextinformationen zu der Anwendung IBM

Cognos . Dieser Ansatz erfordert, dass jede Anwendung, die die Verbindung verwendet, diese Informationen zur Verfügung stellt, um Fehler zu vermeiden.

```
<commandBlock>
    <commands>
        <sqlCommand>
            <sql> CALL myproc(#sq($APP_INFO{APPNAME}) + ',' +
             sq($APP_INFO{'APPMAJOR'}) + ',' +
             sq($APP_INFO{'APPMINOR'}) + ',' +
             sq($APP_INFO{'APPCONTACT'}) + ', ''Constant1'' '#))
            </sql>
        </sqlCommand>
    </commands>
</commandBlock>
```

Nachdem das Makro erweitert wurde, ruft der Datenbankadministrator die folgenden Informationen zu der Abfrage ab:

```
CALL myproc('ApplicationName','10','1','TradingApp@email.com',
'Constant' )
```

Beispiel-Passing-Authentifizierungsprovider-Details

Dieses IBM Db2 -Beispiel zeigt, wie Sitzungsdaten, die von einem Authentifizierungsprovider stammen, in die Informationen eingeschlossen werden, die an die Datenbank übergeben werden.

Der Befehlsblock ruft die Db2 -Prozedur SYSPROC.WLM_SET_CLIENT auf und übergibt Werte, die von den verfügbaren Sitzungsvariablen abgeleitet wurden. Diese Informationen können von Datenbankadministratoren bei der Definition von Workload-Management-Regeln in der Datenbank verwendet werden, die bestimmten Benutzergruppen höhere Priorität einräumen, wenn eine Datenbankverbindung von mehreren Benutzergruppen gemeinsam genutzt wird.

```
<commandBlock>
    <commands>
        <sqlCommand>
            <sql> CALL SYSPROC.WLM_SET_CLIENT_INFO
            (#$account.personalInfo.userName#,
             'UserComputerName',
#$account.parameters.var1#, 'ApplicationName', 'AUTOMATIC')
            </sql>
        </sqlCommand>
    </commands>
</commandBlock>
```

Beispiel-Befehlsblöcke für Proxy-Verbindungen verwenden

Wenn Sie Proxy-Verbindungen verwenden, können Sie eine vorhandene inaktive Verbindung mit Anmeldungen für Proxy-Verbindungen verwenden.

Die physische Verbindung kann von mehr als einem Benutzer verwendet werden. Da die Proxyverbindungen auf der vorhandenen physischen Verbindung ausgeführt werden, sind weniger physische Verbindungen erforderlich.

Um eine Proxy-Verbindung zu erstellen, erstellen Sie offene Sitzungsbefehlsblöcke in XML.

Im Folgenden sehen Sie ein einfaches Beispiel für einen offenen Sitzungsbefehlsblock, der eine Proxy-Verbindung für User1 (Oracle) erstellt oder zu User1 (Db2) wechselt. Beachten Sie, dass der Befehl sessionStartCommand nur mit Oracle und Db2verwendet werden kann.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
```

```
  </commands>
</commandBlock>
```

Ein weiteres Beispiel ist ein Makro, das ersetzt werden kann, wenn die Authentifizierung userNames der Proxy-Benutzer-ID oder dem Benutzer mit dem gesicherten Kontext entspricht.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>#$account.personalInfo.userName#
          </value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

Im Folgenden sehen Sie ein einfaches Beispiel für einen Blockierungsbefehlsblock für eine Proxy-Sitzung. Die aktuelle Proxy-Verbindung wird beendet. Beachten Sie, dass sessionEndCommand eine OCI_session in Oracle beendet und den Benutzer zurück an den Eigner des gesicherten Kontexts für Db2schaltet.

```
<commandBlock>
  <commands>
    <sessionEndCommand>
      <arguments/>
    </sessionEndCommand>
  </commands>
</commandBlock>
```

Beispiel-Befehlsblöcke für virtuelle private Datenbanken für Oracle verwenden

In der Regel verwendet Oracle signons, um die Datenbankinformationen zu ermitteln, auf die Benutzer zugreifen können. Eine virtuelle private Datenbank legt fest, welche Benutzer auf welche Informationen zugreifen können, ohne dass weitere Anmeldedaten erforderlich sind.

Sie erstellen einen Befehlsblock für die Verbindung mithilfe von Makros, die während der Ausführung für den angemeldeten Benutzer ersetzt werden. Die Makros identifizieren den Benutzer, so dass der Benutzer keine Informationen zum erneuten Eingeben von Informationen eingeben muss.

Wenn alle Benutzer, die auf die Datenbank zugreifen, als Datenbankbenutzer definiert sind und Benutzerkonten für Verbindungen verwendet werden, können Sie den Kontext automatisch einrichten, wenn die Verbindung hergestellt wird. Zum Beispiel kann das Makro für den Benutzernamen ersetzt werden.

Der XML-Befehlsblock speichert eine Reihe von Befehlen, die in der angegebenen Reihenfolge ausgeführt werden. Dazu können die Befehle gehören, die in Anhang E, „Schema für Datenquellenbefehle”, auf Seite 485beschrieben werden.

Das folgende Beispiel zeigt einen XML-Befehlsblock für eine virtuelle private Datenbank.

Dieser Befehlsblock definiert einen Kontext (virtuelle private Datenbank) innerhalb der Verbindung, der auf dem übergebenen Parameter basiert. Der übergebene Parameter wird aus der Umgebung abgerufen, die sich auf die Anmeldung des Benutzers auf der Portalebene bezieht. Diese Variablen können in dem Konfigurationstool geändert werden. Ihre Werte sind benutzerspezifisch und werden mit Hilfe des Sicherheitssteuermechanismus (CAM) abgerufen.

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql>BEGIN PKG_COUNTRY_CONTEXT.SP_SET_COUNTRY1
       (#$account.parameters.var1#);
END;</sql>
    </sqlCommand>
```

```
  </commands>
</commandBlock>
```

In diesem Beispiel wird die Accountparametersubstitution angezeigt. Sie müssen Kontoinformationen als angepasste Eigenschaften angeben. Informationen zu Sitzungseigenschaften finden Sie im Framework Manager *Benutzerhandbuch*.

Hinweis: -Befehlsblöcke für Oracle-Proxy-Verbindungen und virtuelle private Datenbanken auf der Datenquellenebene gelten für alle Verbindungen zu dieser Datenquelle.

Hinzufügen von Befehlsblöcken beim Erstellen einer Datenquelle

Sie können Befehlsblöcke hinzufügen, wenn Sie Datenquellen erstellen.

Standardmäßig erfassen Verbindungen Eigenschaften aus der übergeordneten Datenquelle. Sie können einzelne Verbindungen zu einem späteren Zeitpunkt ändern.

Vorgehensweise

1. Starten Sie auf der Registerkarte **Konfiguration** in Cognos Administration die Erstellung einer Datenquelle für eine Datenbank, die Befehlsblöcke unterstützt.
2. Klicken Sie auf der Seite mit den Befehlsbefehlen auf **Festlegen** neben dem Befehl, den Sie angeben möchten.
3. Fügen Sie auf der Seite mit dem Befehl set den XML-Code für den Befehlsblock hinzu, und klicken Sie auf **OK**.

   Tipp: Für IBM Db2 oder Microsoft SQL Server können Sie einen Befehlsblock nur zum Öffnen einer Sitzung hinzufügen.
4. Fügen Sie nach Bedarf weitere Befehlsblöcke hinzu und klicken Sie dann auf **Fertigstellen**.

Hinzufügen oder Ändern von Befehlsblöcken für eine Verbindung

Sie können Befehlsblöcke für bestimmte Datenquellenverbindungen hinzufügen, ändern oder entfernen.

Verbindungen erfassen Eigenschaften aus ihrer übergeordneten Datenquelle. Wenn Sie einen Befehlsblock für eine Datenquelle hinzufügen, steht dieser Befehlsblock für alle Verbindungen für diese Datenquelle zur Verfügung.

Vorgehensweise

1. Wählen Sie auf der Registerkarte **Konfiguration** in Cognos Administration eine der folgenden Optionen aus:
   - Greifen Sie auf die Datenquelleneigenschaften zu, wenn Sie die Befehlsblöcke für alle Verbindungen ändern möchten, die diese Datenquelle hat.
   - Greifen Sie auf die Eigenschaften für die Datenquellenverbindung zu, wenn Sie die Befehlsblöcke für eine Verbindung ändern möchten.
2. Klicken Sie auf die Registerkarte **Verbindung** und führen Sie im Abschnitt **Befehle** eine der folgenden Tasks aus:
   - Wenn Sie den Befehlsblock hinzufügen möchten, klicken Sie auf **Festlegen** für einen der verfügbaren Befehlstypen und fügen Sie den XML-Code für den Befehlsblock in das Feld **XML-Datenbankbefehle** ein.
   - Wenn Sie einen Befehlsblock ändern möchten, klicken Sie auf **Bearbeiten** für den ausgewählten Befehl und ändern oder entfernen Sie den XML-Code für den Befehlsblock aus dem Feld **XML-Datenbankbefehle** .

   Sie können Befehlsblöcke zurücksetzen, indem Sie die Markierungsfelder **Auf übergeordneter Wert zurücksetzen** oder **Löschen** auswählen.

Tipp: Für IBM Db2 oder Microsoft SQL Server können Sie Befehlsblöcke nur zum Öffnen einer Sitzung hinzufügen.

3. Fahren Sie nach Bedarf mit dem Hinzufügen oder Ändern von Befehlsblöcken fort, und klicken Sie anschließend auf **Fertigstellen**.

Verwenden von IBM Db2 CLI-Verbindungsattributen für Db2

Db2 Call Level Interface (Db2 CLI) ist eine aufrufbare SQL-Schnittstelle zu Db2 LUW, Db2 für z/OS und Db2for I). IBM Cognos Analytics kann einige der Db2 -CLI-Verbindungsattribute ändern, um den Anwendungskontext an Db2 in einem Format zu übergeben, das für die Komponenten von IBM Optim Integrated Data Management akzeptabel ist.

Diese Informationen können später über SQL-Anweisungen aus Db2 -Sonderregistern abgerufen werden.

Um diese Funktionalität zu aktivieren, müssen Sie eine Konfigurationsdatei auf jedem IBM Cognos -Berichtsservercomputer ändern, der in Ihrer IBM Cognos -Umgebung konfiguriert ist. Da diese Funktionalität auf der Abfrageebene eingerichtet ist, werden die Informationen, die den Verbindungsattributen zugeordnet sind, bei jeder Ausführung des Berichts automatisch aktualisiert.

In der folgenden Liste sind die Db2 -CLI-Verbindungsattribute aufgeführt, die von IBM Cognos Analyticsgeändert werden können, sowie die Art der Informationen, die diese Attribute an Db2übergeben können:

· SQL_ATTR_INFO_USERID

Gibt den Namen des Benutzers an, der einen Bericht ausführt.

· SQL_ATTR_INFO_WRKSTNNAME

Gibt die Adresse des Systems an, auf dem der Browser des Benutzers installiert ist.

· SQL_ATTR_INFO_APPLNAME

Gibt den Paketnamen an, der der Abfrage zugeordnet ist. Wenn die Zeichenfolge länger als 32 Zeichen ist, wird sie in der Abrechnungszeichenfolge zu $SLOT2 überfließen.

· SQL_ATTR_INFO_ACCTSTR

Gibt das Präfix oder die Zeichenfolge an, das bzw. die die Anforderung mit IBM Cognos Analyticsverknüpft. Die Werte lauten wie folgt:

Tabelle 50. Verwenden von Db2 CLI-Verbindungsattributen für Db2

Wert	**Beschreibung**
COG	Ordnet die Anforderung mit IBM Cognos -Produkten in IBM Optim Integrated Data Management zu.
ccc	Ordnet die Anforderung einer IBM Cognos -Lösung zu.
Vr	Gibt die Version des Produkts IBM Cognos an.

Tabelle 50. Verwenden von Db2 CLI-Verbindungsattributen für Db2 (Forts.)	
Wert	**Beschreibung**
Zusätzliche Abrechnungsdaten	Diese Informationen sind in die folgenden Felder (Slots) unterteilt: – $SLOT2-$packageName (Überlaufabschnitt für $SLOT1) – $SLOT3-$reportName – $SLOT4-$queryName – $SLOT5-$reportPath Jeder Steckplatz verfügt über eine feste Länge, die Zeichenfolgen akzeptiert, die nicht mehr als 46 Byte enthalten, und bei Bedarf mit Leerzeichen aufgefüllt werden. Da Berichtspfade, Modellpfade und so weiter oft lang sind, können die Zeichenfolgen verkürzt werden, um sich an die Speicherplatzbeschränkungen anzupassen. **Anmerkung:** In Db2dürfen Werte, die an die API übergeben werden, keine einzelnen Anführungszeichen enthalten, die in Leerzeichen konvertiert werden. Wenn die Zeichensatzcodierung mehrere Byte pro Zeichen verwendet, wird das Zeichen in "?" konvertiert, um einen Überlauf zu vermeiden. Dies ist wichtig, wenn Unicode verwendet wird und ein Zeichen möglicherweise mehr als 2 Byte benötigt.

Vorgehensweise

1. Wenn Sie eine Verbindung zu Ihrer Datenbank mit dem kompatiblen Abfragemodus herstellen, führen Sie die folgenden Schritte aus:
   a) Erstellen Sie im Verzeichnis *Installationsposition*/configuration eine Kopie der CQEConfig.xml.sample -Datei und benennen Sie sie in CQEConfig.xmlum.

      Tipp: Wenn die Datei CQEConfig.xml für andere Zwecke verwendet wurde, z. B. zum Inaktivieren des Sitzungscaching, ist sie möglicherweise im Verzeichnis *Installationsposition*/configuration vorhanden. In dieser Situation verwenden Sie die vorhandene CQEConfig.xml -Datei, um die verbleibenden Schritte auszuführen.

   b) Öffnen Sie die *Installationsposition*/configuration/CQEConfig.xml -Datei in einem Editor.

      Stellen Sie sicher, dass Ihr Editor das Speichern von Dateien im UTF-8-Format unterstützt.

   c) Suchen Sie das < section name="QueryEngine"> -Element, und fügen Sie den Eintrag DB2WFM mit dem Wert 1 hinzu, wie im folgenden Beispiel gezeigt:

      ```
      <section name="QueryEngine">
            <entry name=" DB2WFM" value="1"/>
      </section>
      ```

      Wenn Sie diese Funktion inaktivieren möchten, setzen Sie den Wert auf null.
2. Wenn Sie eine Verbindung zu Ihrer Datenbank mit dem dynamischen Abfragemodus herstellen, führen Sie die folgenden Schritte aus:
   a) Erstellen Sie im Verzeichnis *Installationsposition*/configuration eine Kopie der xqe.config.xml -Datei und benennen Sie sie in xqe.config.xml.backupum.
   b) Öffnen Sie die *Installationsposition*/configuration/xqe.config.xml -Datei in einem Editor.

      Stellen Sie sicher, dass Ihr Editor das Speichern von Dateien im UTF-8-Format unterstützt.

c) Suchen Sie das Element < setConnectionAttributes enabled="false"> und ändern Sie seinen Wert in "true", wie im folgenden Beispiel gezeigt:

```
<setConnectionAttributes enabled="true">
```

Wenn Sie diese Funktionalität inaktivieren möchten, setzen Sie den Wert auf "false".

3. Speichern Sie die Datei.
4. Wiederholen Sie die Schritte für jeden Berichtsservercomputer, der in Ihrer IBM Cognos -Umgebung konfiguriert ist.
5. Starten Sie den IBM Cognos -Service erneut.

Anwendungskontext in Dynamic SQL verwenden

Datenbankserveradministratoren können die dynamische SQL-Workload, die von IBM Cognos-Software generiert wird, protokollieren und analysieren.

Als IBM Cognos -Administrator können Sie eine angepasste Zeichenfolge definieren, die den Anwendungskontext enthält, der als Kommentarmarkierung in SQL hinzugefügt wird, die von der Anwendung generiert wird. Sie können Literale, Makros und Sitzungsvariablen, wie z. B. einen Benutzernamen, einen Servernamen, einen qualifizierten Berichtspfad usw. verwenden, um den von der Cognos -Software generierten Kommentar anzupassen.

Der Datenbankadministrator sollte prüfen, ob der Datenbankclient Kommentare von Anweisungen vor dem Senden an den Server entfernt. Diese Option ist wahrscheinlich konfigurierbar, prüfen Sie mit Ihrem Datenbankclient-Provider.

Durch die Verwendung der anwendbaren Sitzungsvariablen können Sie das Format der Zeichenfolge für bestimmte Tools und Produkte konfigurieren, die Kommentare aus dynamischem SQL extrahieren können. IBM Cognos software includes the comments within any dynamic SQL it generates to a Relational Database Management System (RDBMS) if the vendor supports this functionality.

Verwenden Sie die Datei CQEConfig.xml.sample, die im Lieferumfang des Produkts enthalten ist, um die Zeichenfolgespezifikationen anzupassen. Das Makro in dieser Datei zeigt die Standardeinträge an, die von IBM Cognos für die Generierung der Kommentare verwendet werden. Sie können jedoch auch andere Einträge hinzufügen.

Das folgende Beispiel zeigt Arten von Sitzungsvariablen, die Sie in dem Makro in der Datei CQEConfig.xml.sample angeben können:

```
<configuration company="Cognos" version="0.1" rendition="cer2">
    <component name="CQE">
        <section name="QueryEngine">
            <entry name="GenerateCommentInNativeSQL" value="1"/>
            <!-- ( default(off)=0, on=1) -->
            <entry name="GenerateCommentInCognosSQL" value="1"/>
            <!-- ( default(off)=0, on=1) -->
            <!-- The content of the comments is controlled with two entries, their
defaults are specified in the value attribute -->
            <entry name="NativeCommentMacro" value="# 'NC user=' + $account.defaultName
+ 'report=' + $report + 'start=' + $startTime + 'modelPath='  +
$modelPath + 'reportPath=' + $reportPath + ' queryName=' + $queryName
+ ' REMOTE_ADDR=' + $REMOTE_ADDR + 'HTTP_HOST=' + $HTTP_HOST + 'SERVER_NAME='
+ $SERVER_NAME +' requestID=' + $requestID + 'sessionID=' + $sessionID
#"/>
            <entry name="CognosCommentMacro" value="# 'CC user=' + $account.defaultName
+ 'report=' + $report + 'start=' + $startTime + 'modelPath='  +
$modelPath + 'reportPath=' + $reportPath + ' queryName=' + $queryName
+ ' REMOTE_ADDR=' + $REMOTE_ADDR + 'HTTP_HOST=' + $HTTP_HOST + 'SERVER_NAME='
+ $SERVER_NAME +' requestID=' + $requestID + 'sessionID=' + $sessionID
#"/>
        </section>
    </component>
</configuration>
```

Während der Laufzeit würde das im vorherigen Beispiel verwendete Makro den folgenden Kommentar zum automatisch generierten SQL-oder nativen SQL hinzufügen:

```
/* CC user=Anonymous report=REPORT1
start=2008-08-28T01:59:35.403Z modelPath=/content/package
[@name='New Package']/model[@name='model']
reportPath=/content/package[@name='New Package']/report[@name='REPORT1']
queryName=Query1 REMOTE_ADDR=127.0.0.1 HTTP_HOST=localhost
SERVER_NAME=localhost
requestID=wq2lshM9jGhqdMj9h92MqlqvdMlhyMlGq9lyG9sq
sessionID=010:0d159165-745a-11dd-ac9f-b741aeca4631:2789499633
*/
select distinct
       ALL_TIME.CALENDAR_WEEKDAY  as  CALENDAR_WEEKDAY
 from
       EAPPS..EAPPS.ALL_TIME ALL_TIME
```

Nicht alle Informationen in dem generierten Kommentar sind in allen Situationen aussagekräftig. Die Informationen zu Anforderungs-und Sitzungs-IDs stellen einen Link zur Prüfeinrichtung, zur Leistung von perfQFS-Leistungsinformationen und zu anderen Traces in IBM Cognos bereit. Der Name einer Abfrage in einem Bericht und der Bericht selbst können jedoch bedeutungslos sein, z. B. wenn ein Benutzer eine Ad-hoc-Abfrage oder -Analyse im Gegensatz zum Ausführen einer gespeicherten Abfrage, Analyse oder Bericht ausführt.

Ein anonymer Benutzer kann in den generierten Kommentaren standardmäßig nicht alle Sitzungsvariablen anzeigen.

Anwendungskontext für dynamischen Abfragemodus hinzufügen

Wenn Sie Kommentare in SQL für den dynamischen Abfragemodus verwenden möchten, können Sie die Datei "xqe.config.xml" konfigurieren, die sich in der Konfiguration "install_location/configuration" befindet.

Sie bearbeiten die folgenden Elemente im Element < queryPlanning>.

```
<generateCommentsInNativeSQL enabled="true"/>
<NativeCommentMacro value="#'user=' + $account.defaultName + ' reportPath='
 + $reportPath +' queryName=' + $queryName + ' REMOTE_ADDR=' + $REMOTE_ADDR
 + ' SERVER_NAME=' + $SERVER_NAME + ' requestID=' + $requestID#"/>
```

Anwendungskontext zu dynamischem SQL hinzufügen

Datenbankserveradministratoren können die Datei "CQEConfig.xml.sample" für die Protokollierung und Analyse der dynamischen SQL-Workload konfigurieren, die von IBM Cognos -Software generiert wird. Für den dynamischen Abfragemodus konfigurieren Administratoren die Datei 'xqe.config.xml'.

Vorgehensweise

1. Erstellen Sie im Verzeichnis *Installationsposition*/configuration eine Kopie der CQEConfig.xml.sample -Datei und benennen Sie sie in CQEConfig.xmlum.

   Tipp: Wenn die CQEConfig.xml -Datei für andere Zwecke verwendet wurde, z. B. zum Inaktivieren des Sitzungscaching, ist sie möglicherweise bereits im Verzeichnis *Installationsposition*/configuration vorhanden. In dieser Situation verwenden Sie die vorhandene CQEConfig.xml -Datei, um die verbleibenden Schritte auszuführen.
2. Öffnen Sie die *Installationsposition*/configuration/CQEConfig.xml -Datei in einem Editor.

   Stellen Sie sicher, dass Ihr Editor das Speichern von Dateien im UTF-8-Format unterstützt.
3. Suchen Sie die Codezeilen, die mit den folgenden Codezeilen beginnen:

   ```
   entry name="GenerateCommentInNativeSQL " ...
   ```

   ```
   entry name="GenerateCommentInCognosSQL " ...
   ```

```
entry name="NativeCommentMacro " ...
entry name="CognosCommentMacro " ...
```

4. Wenn Sie möchten, können Sie `NativeCommentMacro` und `CognosCommentMacro` ändern, indem Sie die erforderlichen Parameterwerte angeben und die Parameter löschen, die Sie nicht benötigen.

   Wenn Sie einen Parameterwert leer lassen, wird der Parameter in dem generierten Kommentar nicht angezeigt.
5. Speichern Sie die Datei `CQEConfig.xml` .
6. Starten Sie den IBM Cognos -Service erneut.

Aktualisierte PowerCubes implementieren

Nachdem Sie einen PowerCube erneut erstellt oder aktualisiert haben, können Sie verschiedene Methoden verwenden, um den Cube in der Produktionsumgebung zu implementieren.

Wenn Sie einen aktualisierten IBM Cognos Transformer-PowerCube implementieren möchten, verwenden Sie die Methode "Copy and Activate" in IBM Cognos Transformer (die empfohlene Methode) oder kopieren Sie den PowerCube selbst und verwenden Sie das Befehlszeilendienstprogramm von `pcactivate` .

Um einen aktualisierten Series 7 Transformer PowerCube zu implementieren, müssen Sie den PowerCube zuerst kopieren. Verwenden Sie anschließend das Befehlszeilendienstprogramm `pcactivate` , um den Cube zu aktivieren.

For more information, see the section Copy and Activate a Newer Version of a Published PowerCube in the IBM Cognos Analytics Transformer *Benutzerhandbuch*.

Vorgehensweise

1. Kopieren Sie den Transformer PowerCube in die Produktionsumgebung.

   - Der Name des Zielverzeichnisses in der Produktionsumgebung muss mit dem Namen des PowerCubes identisch sein. Wenn der Cube beispielsweise den Namen `Produkt.mdc`hat, muss das Zielverzeichnis als Produktion bezeichnet werden.
   - Das Zielverzeichnis muss sich im selben Verzeichnis wie der PowerCube befinden. Wenn die Datenquellenverbindung beispielsweise angibt, dass der PowerCube-Standort `D: \Cubes\production.mdc`ist, muss das Zielverzeichnis mit dem Namen 'production' `D: \Cubes\production`sein.

   Kopieren Sie zum Beispiel den PowerCube in `D: \Cubes\production\production.mdc`.
2. Geben Sie an der Eingabeaufforderung den Befehl `Pcativate` mit der folgenden Syntax ein:

   ```
   pcactivate cube_name.mdc
   destination_location destination_location
   ```

   Sie können mehr als eine Zielposition eingeben.

   Geben Sie beispielsweise Folgendes ein:

   - `pcactivate TheCube.mdc d: \deploy\cubes`
   - `pcactivate production.mdc D: \Cubes`
   - `pcactivate sales.mdc \\Server 1\cubes \\Server_2\cubes`
   - `pcactivate "Produktion Cube.mdc" "install_location\webcontent\cubes"`

   Anmerkung: Wenn Sie einen Pfad in den Parameter `cube_name` einschließen, wird der Pfad entfernt und ignoriert.

Datenquellen sichern

You can secure data sources using IBM Cognos security or data source-specific security.

Die Sicherheit von IBM Cognos für eine Datenquelle überschreibt keine Sicherheitsrichtlinien, die bereits für die Datenquelle vorhanden sind. Für IBM Cognos -Würfel kann die Sicherheit beispielsweise auf Würfelebene festgelegt werden. Für Datenquellen von Microsoft Analysis Server kann die Sicherheit mithilfe von Cube-Rollen festgelegt werden.

Abhängig von der Datenquelle stehen eine oder mehrere der folgenden Authentifizierungsmethoden zur Verfügung:

- Keine Authentifizierung

  IBM Cognos software logs on to the data source without providing any signon credentials.

- Berechtigungsnachweise für IBM Cognos

  IBM Cognos software logs on to the data source using the logon specified for the IBM Cognos service. Für Benutzer sind keine einzelnen Datenbanksignonen erforderlich. Für Produktionsumgebungen sind jedoch die einzelnen Datenbanksignonen in der Regel besser geeignet.

- Externer Namensbereich

  IBM Cognos software logs on to the data source with the credentials used to authenticate to the specified authentication namespace. Der Namespace muss aktiv sein, Benutzer müssen vor dem Zugriff auf die Datenquelle angemeldet sein, und die Authentifizierungsnachweise, die für den Namespace verwendet werden, müssen für die Datenquellenauthentifizierung relevant sein.

  Wenn Sie das Kontrollkästchen **Benutzer-ID umsetzen** auswählen, entfernt der Cognos Analytics -Server den Domänennamen aus der Benutzer-ID, die vom externen Namespace zurückgegeben wird, bevor die Datenbankverbindung hergestellt wird. Die aktuelle Implementierung unterstützt die Benutzer-ID-Transformation nur für die folgenden Formate:

  – *Domänenname**Benutzer-ID* -Nach der Umsetzung wäre die Benutzer-ID *Benutzer-ID*

  – `user_id@domain-Name` -Nach der Umsetzung wäre die Benutzer-ID `Benutzer-ID`

  Verbindungen, die Kerberos-Delegierungsdelegierte verwenden, können diese Option verwenden, um den Domänennamen zu entfernen.

  Sie konfigurieren beispielsweise eine SQL-Server-Datenquellenverbindung, die einen externen Active Directory-Namespace verwendet. Die SQL Server-Datenbank ist für die Kerberos-Delegierte-Delegierung konfiguriert. Wenn Sie das Kontrollkästchen **Benutzer-ID umsetzen** auswählen, wird die *Domänenname* -Kennung entfernt und nur *Benutzer-ID* wird vom externen Namespace zurückgegeben.

  Wenn Sie den Domänennamen als Teil der Benutzer-ID beibehalten möchten, stellen Sie sicher, dass dieses Kontrollkästchen eindeutig ist.

Alle Datenquellen unterstützen auch Datenquellensignonen, die für die Gruppe "Jeder" oder für einzelne Benutzer, Gruppen oder Rollen definiert sind, siehe Kapitel 11, „Benutzer, Gruppen und Rollen”, auf Seite 187. Wenn für die Datenquelle eine Anmeldung erforderlich ist, Sie aber keinen Zugriff auf eine Anmeldung für diese Datenquelle haben, werden Sie bei jedem Zugriff auf die Datenquelle zur Authentifizierung aufgefordert.

Kapitel 7. Service 'Query Service'

Der Abfrageservice unterstützt den dynamischen Abfragemodus von IBM Cognos Analytics .

Weitere Informationen finden Sie unter Kapitel 6, „Datenquellen und Verbindungen”, auf Seite 99.

Mit der Verwaltung von Cognos können Sie die folgenden Verwaltungstasks für Abfrageservice ausführen:

- Eigenschaften für Abfrageservices festlegen
- Abfrageservice-Caching

Darüber hinaus können Sie die Prüfprotokollierungsstufe für den Abfrageservice festlegen. Weitere Informationen finden Sie unter „Prüfberichterstellung einrichten” auf Seite 19.

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf **IBM Cognos Administration**verfügen. Weitere Informationen finden Sie unter Kapitel 12, „Zugriffsberechtigungen und Berechtigungsnachweise”, auf Seite 193. Außerdem müssen Sie über die Verwaltungsfunktion für die Abfrageservice verfügen. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen”, auf Seite 207.

Eigenschaften des Abfrageservice festlegen

Der Abfrageservice verwendet eine Reihe von Umgebungs-, Protokollierungs-und Optimierungskonfigurationseinstellungen.

Vorgehensweise

1. Wählen Sie in **IBM Cognos Administration**auf der Registerkarte **Status** die Option **System**aus.
2. Wählen Sie im Abschnitt **Scorecard** die Ansicht **Alle Servergruppen** aus.

   Tipp: Wenn Sie eine andere Ansicht auswählen möchten, klicken Sie im Abschnitt **Scorecard** auf das Dropdown-Menü für die aktuelle Ansicht.
3. Klicken Sie unter **System**auf die Servergruppe.
4. Klicken Sie im **Aktionen** -Menü für die **QueryService-** ***Dispatchername***auf **Eigenschaften festlegen** .
5. Klicken Sie auf die Registerkarte **Einstellungen** .
6. Geben Sie in der Spalte **Wert** die Werte für die Eigenschaften ein oder wählen Sie sie aus, die Sie ändern möchten. In der folgenden Liste werden die Eigenschaften beschrieben, die Sie für den Abfrageservice festlegen können.

   Erweiterte Einstellungen
   Klicken Sie auf **Bearbeiten** , um erweiterte Konfigurationseinstellungen anzugeben. Da ein Eintrag erweiterte Einstellungen von einem übergeordneten Element erwirbt, überschreibt die Bearbeitung dieser Einstellungen die erworbenen erweiterten Einstellungen. Informationen zu den Typen der erweiterten Einstellungen finden Sie im *IBM Cognos Analytics Administration and Security Guide*.

   Dynamische Cube-Konfigurationen
   Klicken Sie auf **Bearbeiten** , um dem Abfrageservice dynamische Cubes hinzuzufügen.

   Prüfprotokollebene für Abfrageservice
   Wählen Sie die Protokollierungsstufe aus, die für den Abfrageservice verwendet werden soll.

   Traceausführungstrace aktivieren
   Ein Trace-Ausführungstrace (Baum-Trace ausführen) zeigt Abfragen an, die für eine Datenquelle ausgeführt werden. Sie verwenden den Trace, um Probleme im Zusammenhang mit der Abfrage zu beheben.

   Sie können Ausführungstrace-Protokolle an der folgenden Position finden:
   Installationsposition/logs/XQE/*Berichtsname*/runtreeLog.xml

Sie können diese Protokolldateien mit IBM Cognos Dynamic Query Analyzer anzeigen und analysieren. Weitere Informationen finden Sie im *IBM Cognos Dynamic Query Analyzer-Benutzerhandbuch*.

Trace-Planungstrace aktivieren
Die Traceerstellung für Abfragepläne (Planbaum) erfasst den Transformationsprozess einer Abfrage. Sie können diese Informationen verwenden, um ein erweitertes Verständnis für die Entscheidungen und Regeln zu erhalten, die ausgeführt werden, um einen Ausführungsbaum zu erstellen.

Der Trace für die Abfrageplanung wird für jede Abfrage protokolliert, die mit dem dynamischen Abfragemodus ausgeführt wird. Sie können Planungstraceprotokolle an der folgenden Position finden: *Installationsposition*/logs/XQE/*Berichtsname*/plantreeLog.xml

Da die Planung von Protokollen groß ist, wirkt sich die Auswirkung auf die Abfrageleistung aus, wenn diese Einstellung aktiviert ist.

Kommentare in nativem SQL generieren
Gibt an, welche Berichte die SQL-Abfragen in der Datenbank generieren.

Modell in Datei schreiben
Gibt an, ob der Abfrageservice das Modell in eine Datei schreiben wird, wenn eine Abfrage ausgeführt wird. Die Datei wird nur zu Fehlerbehebungszwecken verwendet. Ändern Sie diese Eigenschaft nur mit der Anleitung von IBM Software Support.

Sie finden die Datei an der folgenden Position: *Installationsposition*\logs\XQE\model*Paketname*.txt

Zeitlimit für inaktive Verbindungen
Gibt die Anzahl der Sekunden an, in denen eine inaktive Datenquellenverbindung für die Wiederverwendung verwaltet werden soll.

Die Standardeinstellung ist 300. Gültige Einträge sind 0 bis 65535.

Niedrigere Einstellungen reduzieren die Anzahl der Verbindungen auf Kosten der Leistung. Höhere Einstellungen verbessern möglicherweise die Leistung, heben jedoch die Anzahl der Verbindungen zur Datenquelle auf.

Dynamische Würfel beim Starten des Service nicht starten
Verhindert, dass die dynamischen Würfel beim Starten des Abfrageservice gestartet werden.

Zeitlimit für Verwaltungsbefehl für dynamischen Cube
Geben Sie den Zeitraum an, in dem gewartet werden soll, bis eine Ressource für eine Verwaltungsaktion für dynamische Cubes verfügbar ist. Diese Aktion wird abgebrochen, wenn die Zeitperiode überschritten wird.

Tipp: Wenn Sie diesen Wert auf null setzen, wird der Befehl auf unbestimmte Zeit gewartet.

Minimale Abfrageausführungszeit, bevor eine Ergebnismenge für das Caching berücksichtigt wird
Geben Sie die minimale Zeit an, die auf eine Abfrage gewartet werden soll, bevor die Ergebnisse zwischengespeichert werden.

Diese Einstellung gilt nur für dynamische Cubes.

Anfangsgröße des JVM-Heapspeichers für den Abfrageservice
Gibt die Anfangsgröße (in MB) des JVM-Heapspeichers (JVM Java Virtual Machine) an.

Größe der JVM-Heapspeichergröße für den Abfrageservice
Gibt die maximale Größe (in MB) des JVM-Heapspeichers an.

Anfangsgröße für JVM-Nursery
Gibt die Anfangsgröße (in MB) an, die die JVM neuen Objekten zuordnet. Die Gärtnergröße wird automatisch berechnet. Sie müssen die Einstellung nicht ändern, es sei denn, die Kundenunterstützung von IBM Cognos empfiehlt eine Änderung.

Größe der JVM-Nursery-Größe
Gibt die maximale Größe (in MB) an, die die JVM neuen Objekten zuordnet. Die Gärtnergröße wird automatisch berechnet. Sie müssen die Einstellung nicht ändern, es sei denn, die Kundenunterstützung von IBM Cognos empfiehlt eine Änderung.

JVM-Garbage-Collection-
Gibt die von der JVM verwendete Garbage-Collection-Richtlinie an. Sie müssen die Einstellung nicht ändern, es sei denn, die Kundenunterstützung von IBM Cognos empfiehlt eine Änderung.

Zusätzliche JVM-Argumente für den Abfrageservice
Gibt weitere Argumente an, die die Java Virtual Machine (JVM) steuern. Die Argumente können abhängig von der JVM variieren.

Anzahl der Garbage-Collection-Zyklen, die in das ausführliche Protokoll ausgegeben werden
Gibt die Anzahl der Garbage-Collection-Zyklen an, die in die ausführliche Garbage-Collection eingeschlossen werden sollen. Damit wird die maximale Größe der Protokolldatei gesteuert. Wenden Sie sich an die Kundenunterstützung von IBM Cognos , um die Einstellung zu erhöhen und weitere Protokolle zu erfassen.

Ausführliche Garbage-Collection-Protokollierung für JVM inaktivieren
Steuert die ausführliche JVM-Garbage-Collection-Protokollierung. Sie müssen die Einstellung nicht ändern, es sei denn, die Kundenunterstützung von IBM Cognos empfiehlt eine spezielle Änderung.

7. Starten oder starten Sie den Abfrageservice erneut.

Ergebnisse

Eine Zusammenfassung der Eigenschaften des Abfrageservice wird im Teilfenster **Einstellungen-Abfrageservice** angezeigt.

Service-Caching-Verwaltung abfragen

Das Caching verwendet zuvor ausgeführte Ergebnisse und vermeidet, wenn möglich, neue Abfragen für die Datenbank.

Das Caching kann die Leistung verbessern, wenn Berichte mit kleinen Änderungen erneut ausgeführt werden, Analysen innerhalb desselben Cubes durchgeführt werden und wiederholte Master-Detail-Anforderungen für große Berichte ausgeführt werden. Der Cache verwaltet die Sicherheitsberechtigungen des Benutzers, der die Anforderung ausführt.

Weitere Informationen dazu, wie der Cache funktioniert, finden Sie unter Dynamic Query Cookbook für Cognos BI 10.1.1 (https: //developer.ibm.com/tutorials/the-cognos-bi-1011-dynamic-query-cookbook/).

Alles im Cache löschen

Um zu vermeiden, dass veraltete Daten verwendet werden, die im Cache gespeichert werden können, können Sie den Cache löschen.

Möglicherweise möchten Sie den Cache manuell löschen, wenn sich die Metadaten Ihrer Datenquelle selten ändern oder wenn Sie den Cache zwischen automatisch geplanter Cacheberichtung löschen möchten. Wenn Sie den Cache mit den folgenden Schritten löschen, löscht er alles im Cache.

Wenn Sie den Cache für eine bestimmte Datenquelle, einen bestimmten Katalog oder einen bestimmten Cube löschen möchten, erstellen Sie eine Task zur Verwaltung des Abfrageservice. Sie können auch eine Task zur Verwaltung von Abfrageservices erstellen, wenn sich die Metadaten Ihrer Datenquelle regelmäßig ändern. Sie können z. B. einen Zeitplan festlegen, um den Cache stündlich, täglich oder wöchentlich zu löschen. Weitere Informationen finden Sie unter „Administrationsaufgaben für Abfrageservices erstellen und planen“ auf Seite 162.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Abfrageservice-Caching**.
2. Wählen Sie die Servergruppen für die Cacheberichtung aus.
3. Klicken Sie auf **Cache löschen**.

   Der Status des Befehls **Cache löschen** wird angezeigt.

Wenn ein Cache von einem oder mehreren anstehenden Berichten oder Abfragen verwendet wird, wird er von diesem Befehl intern als "veraltet" markiert und wird automatisch gelöscht, sobald diese Verwendung abgeschlossen ist.

4. Klicken Sie auf **Schließen**.

Cacheverwendung analysieren

Sie können die Cachenutzung analysieren, indem Sie eine Zeitstempel-XML-Datei erstellen, die den Status der angegebenen Cube-Caches (Anzahl der Cachetreffer und Cachefehler für verschiedene Ebenen eines Würfels) anzeigt.

Dies ist nützlich, um zu ermitteln, welche Cubes zu einem beliebigen Zeitpunkt im Cache gespeichert sind. Die Datei enthält eine Liste mit dem Datenquellennamen, dem Katalognamen und dem Cube-Namen für Würfel, die derzeit im Cache gespeichert sind. Dies kann Ihnen helfen, zu entscheiden, wann der Cache gelöscht werden soll.

Der Bericht wird im Verzeichnis *c8_location*/logs gespeichert. Der Dateiname hat das Format SALDump_*Präfix_Quellenname_Kategoriename_Würfelname_Zeitmarke*.xml.

Sie können auch festlegen, dass der Cache-Status-Schreiben automatisch ausgeführt werden soll. Weitere Informationen finden Sie unter „Administrationsaufgaben für Abfrageservices erstellen und planen“ auf Seite 162.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Abfrageservice-Caching**.
2. Wählen Sie die Servergruppen für die Cacheberichtung aus.
3. Klicken Sie auf **Schreiben des Cachestatus**.

   Der Status des Befehls **Schreiben des Cachestatus** wird angezeigt.
4. Klicken Sie auf **Schließen**.

Administrationsaufgaben für Abfrageservices erstellen und planen

Administratoren können Abfrageservicetasks für Datenquellen erstellen und planen. Abfrageservice-Tasks steuern einen oder mehrere Würfel, indem sie den zugehörigen Cache löschen, schreiben oder aktualisieren. Für dynamische Cubes können Sie auch planen, wann Cubes gestartet, gestoppt oder neu gestartet und die Sicherheit aktualisiert werden sollen.

- Cacheberichtung planen und den Cache löschen, um die Speicherbelegung durch eine bestimmte Datenquelle oder einen bestimmten Cube zu steuern
- Planen der Generierung eines Zeitstempelberichts (Schreibcachestatus)

Sie können den gesamten Cache auch manuell löschen und den Cachestatus manuell in einen Bericht schreiben.

Weitere Informationen finden Sie unter „Alles im Cache löschen“ auf Seite 161 und „Cacheverwendung analysieren“ auf Seite 162.

Sie können Verwaltungstasks für Abfrageservices erstellen und diese auf Anforderung ausführen. Sie können sie zu einem geplanten Zeitpunkt oder auf der Basis eines Auslösers, wie z. B. einer Datenbankaktualisierung oder einer E-Mail „Trigger-basierte Eintragsplanung“ auf Seite 272, ausführen. Sie können diese als Teil eines Jobs planen „Job zum Planen mehrerer Einträge erstellen“ auf Seite 269. Sie können auch den Ausführungsverlauf der Tasks für die Verwaltung von Abfrageservices „Anzeigen des Ausführungsprotokolls von Einträgen“ auf Seite 266anzeigen.

Vorbereitende Schritte

Wenn Sie Tasks für dynamische Cubes erstellen und planen, müssen Sie die Start-und Stopptasks für Quellencubes und virtuelle Cubes separat terminieren. Bei der Planung von Start-und Stoppaufgaben für dynamische Cubes sind weitere Faktoren zu beachten:

- Quellencubes, die Teil eines virtuellen Cubes sind, müssen zunächst gestartet werden.
- Wenn Quellencubes Teil eines virtuellen Würfels sind, muss der virtuelle Würfel so geplant werden, dass er vor den Quellencubes gestoppt wird.
- Sie müssen genügend Zeit für den Start von Quellencubes bereitstellen, bevor Sie einen virtuellen Cube planen, der gestartet werden soll. Die gleiche Überlegung muss gemacht werden, wenn Sie virtuelle und Quellwürfel zum Stoppen planen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
2. Klicken Sie auf die Schaltfläche 'Neue Abfrageservice-Task'  .
3. Geben Sie einen Namen, eine Beschreibung, eine Bildschirmspitze und einen Standort an. Klicken Sie auf **Weiter**.
4. Wählen Sie eine Operation aus, entweder **Cache löschen** oder **Schreibcache-Status**.
5. Geben Sie für Oracle Essbase-und SAP BW-Datenquellen die Datenquelle, den Katalog und den Cube ein. Klicken Sie auf **Weiter**.

   Geben Sie einen Stern (*) als Platzhalterzeichen ein, um alle anzugeben.
6. Bei Dimensional Modellierten Relationalen (DMR) -Datenquellen geben Sie entweder den Namen eines Paketnamens oder den Namen einer Datenquelle ein. Wenn Sie einen Datenquellennamen angeben und die Operation **Cache löschen** auswählen, wird der Cache für alle Pakete gelöscht, die diese Datenquelle betreffen.
7. Wählen Sie für dynamische Cube-Tasks die **Servergruppe**-, **Dispatcher**-und **Würfel**aus und klicken Sie dann auf **Weiter**.
8. Wählen Sie die Aktion aus, die Sie ausführen möchten:
   - Wenn Sie die Task jetzt oder später ausführen möchten, klicken Sie auf **Speichern und einmal ausführen** und dann auf **Fertigstellen**. Geben Sie eine Uhrzeit und ein Datum für die Ausführung an, und klicken Sie anschließend auf **Ausführen**. Überprüfen Sie die Laufzeit und klicken Sie auf **OK**.
   - Wenn Sie die Task zu einem wiederkehrenden Zeitpunkt planen möchten, klicken Sie auf **Speichern und planen** und dann auf **Fertigstellen**. Wählen Sie dann Frequenz und Start-und Enddatum aus. Klicken Sie auf **OK**.

     Tipp: Wenn Sie den Zeitplan vorübergehend inaktivieren möchten, wählen Sie das Kontrollkästchen **Zeitplan inaktivieren** aus.
   - Klicken Sie auf **Nur speichern** , und klicken Sie auf **Fertigstellen**, um die Task ohne Planung oder Ausführung zu speichern.

Nächste Schritte

Sie müssen sich daran erinnern, eine geplante Task zu löschen, wenn Sie den zugeordneten Cube aus dem Abfrageservice löschen. Andernfalls weisen Ihre geplanten Tasks auf nicht vorhandene Cubes hin.

Befehlszeilen-API für Abfrageservice

Sie können den Cache zusätzlich zur Verwendung von IBM Cognos Administration manuell oder automatisch mit einer Befehlszeilen-API verwalten.

Das Befehlszeilendienstprogramm befindet sich in dem Verzeichnis *Installationsposition*\bin und wird abhängig von Ihrem Betriebssystem **QueryServiceAdminTask.sh** oder **QueryServiceAdminTask.bat**genannt.

Geben Sie QueryServiceAdminTask -help in eine Befehlsshell ein, um Anweisungen für die Verwendung des Dienstprogramms anzuzeigen.

Das Befehlszeilendienstprogramm stellt eine sofortige Taskanforderung dar und verwendet den Job-Scheduler und den Überwachungsservice nicht. Als Ergebnis wirken sich Befehle nur auf den IBM Cognos Analytics -Server aus, auf dem sie ausgeführt werden.

Abfragen für hochgeladene Dateien und Dateien

Abfragen für hochgeladene Dateien und Dateien werden von **Abfrageservice** und **Rechenservice**verarbeitet. Diese Art der Co-Verarbeitung erhöht die Leistung von Abfragen.

Der **Rechenservice** verarbeitet die Abfragen ganz oder teilweise und gibt das Ergebnis an den Abfrageservice zurück. Möglicherweise kann die gesamte Abfrage von der **Rechenservice**verarbeitet werden, und der Abfrageservice muss möglicherweise nur eine zusätzliche lokale Verarbeitung des Ergebnisses ausführen.

Tipp: Die **Rechenservice** und **Abfrageservice** befinden sich auf demselben Computer und kommunizieren standardmäßig miteinander, indem sie einen ephemeren Port verwenden, der vom Betriebssystem angefordert wird.

Upgrade von Daten auf das neue Parkett-Format

Das Parkett-Format, das zum Speichern hochgeladener Dateien und Dateien verwendet wird, hat sich zwischen den Cognos Analytics -Versionen 11.0.x und 11.1 geändert. Führen Sie den Befehl ParquetUpgrade aus, bevor Benutzer mit der Ausführung von Dashboards und Berichten beginnen. Auf diese Weise wird sichergestellt, dass alle Workloads sofort von den **Rechenservice** -Leistungsgewinnen profitieren. Wenn eine Abfrage Daten verwendet, die nicht konvertiert wurden, leitet der Abfrageservice intern die Konvertierung ein, und die Benutzer erfahren eine einmalige Leistungsverschlechterung, wenn sie die Dashboards, Storys, Berichte oder Erkundungen in Cognos Analytics 11.1 ausführen. Nachfolgende Abfragen, die vom Rechenservice ausgeführt werden, verwenden die konvertierten Daten.

Weitere Informationen finden Sie im Upgradeabschnitt in der *IBM Cognos Analytics -Konfigurationshandbuch*.

Bewährte Verfahren zur Verbesserung der Abfrageleistung bei hochgeladenen Dateien und Dateien

Verwenden Sie die folgenden bewährten Verfahren, wenn Sie mit Abfragen arbeiten, die auf hochgeladenen Dateien und Dateien basieren:

- Speichern Sie häufig berechnete Ausdrücke als Spalten.

  Diese Praxis reduziert die Anzahl der Ausdruckserwertungen während der Laufzeit. Das Projizieren, Vergleichen und Sortieren von einfachen Spaltenreferenzen und einfachen Werten (Literalen) ist effizienter als die Auswertung von Ausdrücken.
- Vermeiden Sie es, eine große Anzahl von Spalten zu speichern, die niemals von Abfragen verwendet werden.

  Während Daten sowohl komprimiert als auch codiert sind, um die Speichermenge zu reduzieren, ist es dennoch empfehlenswert, das Speichern redundanter oder unnötiger Spalten zu vermeiden.
- Sortieren Sie die Eingabe in der Spalte, die am häufigsten in Filtern verwendet wird.

  Bei großen hochgeladenen Dateien und Datensätzen kann das Sortieren der Eingabe die Auswertung von Vergleichselementen verbessern. Bei der Sortierung der Daten in der allgemeinen Spalte, die in einem Filter verwendet wird (z. B. Land oder Speicher), werden Zeilen mit demselben Wert gruppiert. Wenn eine Abfrage Prädikate für diese Spalte enthält, kann die Abfrage effizienter ermitteln, welche

Datenblöcke sie ignorieren können, wenn sie die Daten navigiert. Verwenden Sie die Sortieroption, wenn Sie eine Datei erstellen, und sortieren Sie die Eingabe vor dem Hochladen einer Datei.

Datentypen zum Speichern von Daten aus hochgeladenen Dateien und Dateien

Die Daten in hochgeladenen Dateien und Dateien werden in den folgenden Datentypen gespeichert:

- Alle ganzzahligen Typen (klein, integer und bigint) werden als bigint gespeichert.
- Alle ungefähren numerischen Typen (real, float und double) werden als Double gespeichert.
- Alle präzisen numerischen Werte werden als dezimal auf die maximale Genauigkeit von 38 gespeichert.
- Alle Zeichentypen (char, nchar, varchar, nvarchar, clob, nlclob) werden als nationale varchar ohne maximale Präzision gespeichert.
- Alle Zeittypen (Datum, Zeitmarke, Zeit, Zeitstempel/Zeit mit Zeitzone) werden als Zeitmarke gespeichert.
- Intervalltypen werden in einem Format gespeichert, das als Intervall verstanden wird. In früheren Releases wurde der Wert als Zeichenfolge gespeichert. Der Berichtsserver gibt die Intervallwerte wieder.

Wenn es sich bei einem Quellenwert um einen Dezimaldatentyp mit einer Genauigkeit > 38 handelt, versucht der Abfrageservice, den Wert als Dezimaltyp mit einer Genauigkeit von 38 zu speichern. Wenn ein Wert zu groß ist, gibt der Abfrageservice einen Fehler zurück, der die Quellenspalte, den Wert und die logische Zeilennummer in den Eingabedaten angibt.

Abschließende Leerzeichen werden aus beliebigen Zeichenwerten entfernt.

Zeitmarken und Uhrzeiten mit Zeitzonen werden auf einen Wert normalisiert, der auf der koordinierten Weltzeit (UTC) basiert.

Rechenservice konfigurieren

Die erweiterten **Abfrageservice** -Einstellungen werden verwendet, um die **Rechenservice** zu konfigurieren, die zum Verarbeiten von Daten aus hochgeladenen Dateien und Dateien verwendet wird.

Die folgenden erweiterten **Abfrageservice** -Einstellungen können angegeben werden:

qs.queryExecution.flintServer.queryTimeoutInterval

Gibt die maximale Zeit (in Sekunden) an, die eine Abfrage ausgeführt werden kann, bevor sie das zulässige Zeitlimit überschritten hat. Zeitlimits können auftreten, wenn gleichzeitig konkurrierende Lasten um Systemressourcen konkurrieren, z. B. CPU-, Speicher-und Platteneinheiten oder langsame Einheiten (Disk).

Der Wert kann `300` (Standardeinstellung) oder eine positive ganze Zahl kleiner oder gleich `3600` (eine Stunde) sein.

qs.queryExecution.flintServer.loadingPolicy

Gibt die Laderichtlinie für den Compute-Service an. Dieser Service kann gestartet werden, wenn der Abfrageservice gestartet wird, oder verzögert werden, bis eine Abfrage erforderlich ist, für die der Rechenservice erforderlich ist.

Wenn ein Cognos Application-Tier-Server einen großen Prozentsatz des verfügbaren RAM verwendet und keine Workload, die hochgeladene Dateien oder Dateien verwendet, den Prozess verzögert, bis der Server gestartet wird, ist eine kleine Speicherersparnis möglich.

Der folgende Wert kann verwendet werden:

- `Einsatz` (Standardeinstellung)-Der Rechenservice wird gestartet, wenn der Abfrageservice gestartet wird.
- `faul` -Der Rechenservice wird verzögert, bis eine Abfrage erforderlich ist, für die dieser Co-Prozess erforderlich ist.

qs.queryExecution.flintServer.maxHeap

Gibt die maximale Speichermenge an, die der Compute-Service verwenden darf.

Der Wert kann 4096 (Standardwert) oder eine positive ganze Zahl größer als 4096 sein. Die Verwendung eines höheren Werts ist möglicherweise erforderlich, wenn Workloads mehr Speicher benötigen, um abgeschlossen zu werden.

qs.queryExecution.flintServer.minHeap

Die Mindestspeicherkapazität, die der Compute-Service verwenden darf.

Der Wert kann 1024 (Standardwert) oder eine positive ganze Zahl größer als 1024 sein.

qs.queryExecution.flintServer.sparkThreads

Gibt die maximale Anzahl der Threads an, die der Compute-Service für Serviceabfragen verwenden kann. Der angegebene Wert muss eine positive ganze Zahl größer als 1 sein.

qs.queryExecution.flintServer.extraJavaOptions

Gibt zusätzliche Argumente für den Compute-Service an.

Vorgehensweise

1. Öffnen Sie **Cognos-Verwaltung**von **Verwalten** > **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Dispatcher und Services**, und klicken Sie auf den Namen Ihres Dispatchers.
3. Suchen Sie in der Liste der Services nach dem **Abfrageservice**und klicken Sie auf das zugehörige Eigenschaftssymbol  .
4. Wählen Sie auf der Registerkarte **Einstellungen** unter **Kategorie**die Option **Umwelt**aus.
5. Klicken Sie neben **Erweiterte Einstellungen**auf **Bearbeiten**.
6. Wählen Sie das Markierungsfeld **Über den übergeordneten Eintrag erfasste Einstellungen außer Kraft setzen** aus.
7. Geben Sie die Parameternamen und ihre Werte ein, oder kopieren Sie sie, wie oben in diesem Abschnitt angegeben.
8. Klicken Sie auf **OK**.
9. Starten Sie **Abfrageservice**erneut.

Kapitel 8. Daten sichern

Es wird empfohlen, regelmäßig Ihre IBM Cognos -Software-Daten und -Konfigurationseinstellungen sowie die Framework Manager-Projekte und -Modelle zu sichern. Dies verhindert den Verlust Ihrer Daten, wenn Ihr Computer beschädigt oder gestohlen wird. Nachdem Ihr Computer betriebsbereit ist, können Sie Ihre Daten wiederherstellen.

Da die Sicherung von Systemressourcen unterstützt wird, wenn die IBM Cognos -Software ausgeführt wird, während die Datenbank gesichert wird, ist ihre Leistung betroffen.

Wenn Sie die Position der Verschlüsselung und die Signierschlüsseleinstellungen von der Standardposition geändert haben, stellen Sie sicher, dass Sie das Verzeichnis, in dem diese Einstellungen enthalten sind, sichern. Wenn die Keystores mit Kennwörtern gesichert sind, müssen Sie außerdem sicherstellen, dass diese Kennwörter beibehalten werden.

Daten, die gesichert werden sollen, sollen auf demselben Computer wiederhergestellt werden. Informationen zum Versetzen von Daten von einem Computer in einen anderen finden Sie unter Kapitel 19, „Implementierung”, auf Seite 299.

Informationen zum Sichern von Daten, bevor Sie ein Upgrade für Ihre Software durchführen, finden Sie im Upgrade-Thema in IBM Cognos Analytics *Installations-und Konfigurationshandbuch*.

Wenn Sie ein Quellcodeverwaltungssystem zum Speichern Ihrer Framework Manager-Projekte verwenden, müssen Sie Ihre Projekte nicht sichern.

Wenn Sie Informationen in IBM Cognos -Konfiguration oder im Content-Store angepasst haben, müssen Sie sicherstellen, dass diese korrekt gesichert werden.

Sichern Sie den Content Store.

Sie können den Content Store sichern.

Vorgehensweise

1. Sichern Sie den Content Store.

   Weitere Informationen finden Sie in Ihrer Datenbankdokumentation.
2. Kopieren Sie das Verzeichnis *Installationsposition*/configuration in die Sicherungsposition.

   Dieses Verzeichnis enthält die Konfigurationseinstellungen.

Ergebnisse

Wenn Sie jemals die Konfigurationseinstellungen wiederherstellen müssen, können Sie das Backedup-Verzeichnis an die richtige Position kopieren.

Informationen zum Wiederherstellen des Content Store finden Sie in Ihrer Datenbankdokumentation.

Framework Manager-Projekte und -Modelle sichern

Sie können Framework Manager-Projekte und -Modelle sichern.

Vorgehensweise

Kopieren Sie das Projektverzeichnis des Framework Manager und seine Unterverzeichnisse in die Sicherungsposition.

Standardmäßig befinden sich die Projekte und Modelle in "Eigene Dateien"/"Meine Projekte".

Ergebnisse

Wenn Sie die Framework Manager-Projekte und -Modelle jemals wiederherstellen müssen, können Sie die Backed-up-Verzeichnisse an die richtige Position kopieren.

Kapitel 9. 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.

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.

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 `CMECMIntegrationTypes_RMImport_Manifest.xsd` -Datei aus, aus der die Objekte importiert werden sollen.
   - Klicken Sie im Feld **Verwaltungsobjektdatei** auf **Durchsuchen**, und wählen Sie die Datei `CMECMIntegrationTypes_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="ASSOCIATED"
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*.

Inhaltsarchivierung verwalten

Die Verwaltung Ihrer Content-Archivierung umfasst das Erstellen von Archivierungsaufgaben und die Angabe von archivalen Positionen.

Die Berichtsausgabe kann in einem externen Berichtsrepository für die Langzeitspeicherung archiviert werden. Weitere Informationen finden Sie unter „Datenquellenverbindungen für externe Repositorys" auf Seite 121.

Externes Repository für Berichtsausgabe angeben

Sie müssen ein Repository in der Ordner-und Paketebene angeben, bevor Inhalte in das Repository archiviert werden können.

Um ein Repository anzugeben, muss eine Verbindung zum Repository vorhanden sein, und Sie müssen über ausreichende Berechtigungen zum Auswählen des Repositorys verfügen. Sie müssen über die Ausführungsberechtigung für das gesicherte Feature **Repository-Verbindungen verwalten** für die Funktionalität von **Externe Repositorys** verfügen. Wenn eine Verbindung angegeben wird, werden alle neuen Berichtsausgabeversionen automatisch in das externe Repository kopiert.

Wenn bereits eine Datenquellenverbindung zu einem externen Repository angegeben ist, kann sie überschrieben und ein anderes Repository ausgewählt werden. Wenn der Inhalt des Pakets oder Ordners nicht mehr archiviert werden soll, können Sie den Verweis auf die Verbindung mit der Option **Löschen** entfernen. Hier ist ein Beispiel. Ein Unterordner erwirbt standardmäßig eine Repository-Verbindung aus dem übergeordneten Ordner. Sie möchten jedoch entweder nicht, dass der Inhalt des Unterordners archiviert werden soll, oder Sie möchten nicht, dass der Inhalt des Unterordners in dem für den übergeordneten Ordner angegebenen Repository archiviert wird. Um den Inhalt eines Unterordners von der Archivierung auszuschließen, verwenden Sie die Option **Löschen** . Wenn Sie ein anderes Repository aus dem übergeordneten Ordner verwenden möchten, geben Sie eine Verbindung für den Unterordner an.

Sie können auch eine Datenquellenverbindung zu einem externen Repository für einen Ordner oder ein Paket erstellen, wenn das Repository vorhanden ist und Sie über die erforderliche Berechtigung zum Erstellen einer Repository-Verbindung verfügen. Weitere Informationen finden Sie unter „Datenquellenverbindungen für externe Repositorys" auf Seite 121.

Vorgehensweise

1. Klicken Sie mit einem ausgewählten Ordner oder Paket auf das Symbol Eigenschaften festlegen.
2. Rufen Sie auf der Registerkarte **Allgemein** den Abschnitt **Berichtsrepository** auf.
3. Wenn Sie eine Datenquelle angeben oder eine vorhandene Datenquelle ändern möchten, wählen Sie **Überschreibung des Berichtsrepositorys, das aus dem übergeordneten Eintrag angefordert wurde**aus.
4. Klicken Sie unter **Verbindung**auf **Verbindung auswählen**.
5. Wählen Sie im Fenster **Datenquelle auswählen (Navigieren)** die Datenquelle aus.

Verwalten von Inhaltsarchivierungsaufgaben für Inhalte erstellen

Erstellen Sie eine Wartungstask für die Inhaltsarchivierung, um die Berichtsausgabe in Ordnern und Paketen für die Archivierung in Ihrem externen Repository zu verschieben.

Informationen zu diesem Vorgang

Sie können eine Content-Archivierungstask erstellen und planen, um Berichtsausgabeversionen, die sich in Ordnern und Paketen befinden, für die Archivierung zu markieren. Der Inhalt, der für die Archivierung markiert ist, wird kopiert und in Ihrem externen Repository gespeichert.

Ordner und Pakete, die für die Archivierung markiert sind, können erst dann aus dem Content Store gelöscht werden, wenn sie erfolgreich verschoben und im externen Repository gespeichert wurden.

Vorgehensweise

1. Starten Sie IBM Cognos Administration.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
3. Klicken Sie in der Symbolleiste auf das Symbol für die neue Inhaltsverwaltung und klicken Sie dann auf **Inhaltsarchival**.
4. Geben Sie einen Namen für die Content-Archivierungstask und optional eine Beschreibung und einen Anzeigentipp ein. Klicken Sie auf **Weiter**.
5. Wählen Sie die Aufzeichnungsstufe aus.
6. Klicken Sie **Hinzufügen**
7. Wählen Sie Ordner, Pakete, Namensbereiche oder Namensbereichsordner aus, die für die Archivierung markiert werden sollen, und klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf **OK**.
9. Klicken Sie auf **Weiter**.
10. Wählen Sie eine der folgenden Optionen aus:
    - Klicken Sie auf **Speichern und einmal ausführen**, um es jetzt oder später auszuführen. Klicken Sie auf **Fertigstellen**, geben Sie die Uhrzeit und das Datum für die Ausführung an, und klicken Sie anschließend auf **Ausführen**. Überprüfen Sie die Laufzeit und klicken Sie auf **OK**.
    - Klicken Sie auf **Speichern und planen**, um den Zeitplan zu einem wiederkehrenden Zeitpunkt zu planen. Klicken Sie auf **Fertigstellen**, und wählen Sie dann Häufigkeit und Start-und Enddaten aus. Klicken Sie auf **OK**.
    - Klicken Sie zum Speichern ohne Terminierung oder Ausführung auf **Nur speichern** und klicken Sie auf **Fertigstellen**.

Wartungstask für Aufbewahrungsregelaktualisierung erstellen

Erstellen Sie eine Wartungsaufgabe für Aufbewahrungsregeln, um die Anzahl der Berichtsausgabeversionen, Dokumentinhaltsversionen und Berichtsverlauf global zu ändern, die derzeit im Content Store aufbewahrt werden.

Informationen zu diesem Vorgang

Administratoren verwenden die Aktualisierungsaufgabe für die Aufbewahrungsregel, um die Anzahl der Berichte, Abfragen, Analysen und Dokumentobjekte anzugeben, die im Content-Store gespeichert werden sollen. Sie können angeben, wie lange die Protokoll-und Ausgabeversionen im Content Store aufbewahrt werden sollen. Alles, was älter ist als das von Ihnen angegebene Datum, wird aus dem Content Store gelöscht. Diese Aktualisierungsaufgabe markiert Ausgabeversionen, die aus dem Content Store gelöscht werden sollen, wenn die Ausgabeversionen der definierten Aufbewahrungsregel nicht folgen. Eine Hintergrundtask im Content Manager löscht die markierten Objekte aus dem Content Store. Um den Inhalt im Content Store zu reduzieren, sollten Sie in Erwägung ziehen, im Content-Store maximal zwei Versionen zu halten und ältere Versionen in Ihrem externen Repository zu archivieren.

Wichtig: Führen Sie diese Task nur nach der Erstellung und Ausführung der Content-Archivierungstask aus. Wenn Sie den Inhalt zuvor ausführen, wird der Inhalt, der nicht für die Archivierung markiert war, dauerhaft aus dem Content Store gelöscht.

Vorgehensweise

1. Starten Sie IBM Cognos Administration.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
3. Klicken Sie in der Symbolleiste auf das Symbol für die neue Inhaltsverwaltung und klicken Sie dann auf **Aktualisierung der Aufbewahrungsregel**.
4. Geben Sie einen Namen für die Aktualisierungsaufgabe für die Aufbewahrungsregel und optional eine Beschreibung und einen Anzeigentipp ein. Klicken Sie auf **Weiter**.
5. Wählen Sie die Ordner und Pakete aus, die Sie einschließen möchten.
6. Führen Sie für die Aufbewahrungseinstellungen für **Protokoll ausführen** einen der folgenden Schritte aus:
   - Um das Ausführungsprotokoll für eine bestimmte Anzahl von Vorkommen beizubehalten, klicken Sie auf **Anzahl Vorkommen** , und geben Sie die Nummer ein. Wenn Sie eine unbegrenzte Anzahl von Berichtsausgaben speichern möchten, setzen Sie diesen Wert auf 0.
   - Um das Ausführungsprotokoll für eine bestimmte Zeitdauer beizubehalten, klicken Sie auf **Dauer** und klicken Sie entweder auf **Tage** oder auf **Monate**. Geben Sie den entsprechenden Wert in das Feld ein.
7. Führen Sie für die Aufbewahrungseinstellungen für **Ausgabeversionen** einen der folgenden Schritte aus:
   - Um die Berichtsausgabe für eine bestimmte Anzahl von Vorkommen beizubehalten, klicken Sie auf **Anzahl Vorkommen** , und geben Sie die Nummer ein. Wenn Sie eine unbegrenzte Anzahl von Berichtsausgaben speichern möchten, setzen Sie diesen Wert auf 0.
   - Um die Berichtsausgabe für eine bestimmte Zeit zu halten, klicken Sie auf **Dauer** und klicken Sie entweder auf **Tage** oder auf **Monate**. Geben Sie den entsprechenden Wert in das Feld ein.
8. Wählen Sie die Aufzeichnungsstufe aus und klicken Sie auf **OK**.
9. Wählen Sie eine der folgenden Optionen aus:
   - Klicken Sie auf **Speichern und einmal ausführen**, um es jetzt oder später auszuführen. Klicken Sie auf **Fertigstellen**, geben Sie die Uhrzeit und das Datum für die Ausführung an, und klicken Sie anschließend auf **Ausführen**. Überprüfen Sie die Laufzeit und klicken Sie auf **OK**.
   - Klicken Sie auf **Speichern und planen**, um den Zeitplan zu einem wiederkehrenden Zeitpunkt zu planen. Klicken Sie auf **Fertigstellen**, und wählen Sie dann Häufigkeit und Start-und Enddaten aus. Klicken Sie auf **OK**.
   - Klicken Sie zum Speichern ohne Terminierung oder Ausführung auf **Nur speichern** und klicken Sie auf **Fertigstellen**.

Wartungstask für Inhaltsentfernungsinhalte erstellen

Erstellen Sie eine neue Inhaltserwartungs-Task zum Entfernen von Inhalten, um die Protokollobjekte zu markieren und Ausgabeversionen zu melden, die in Ordnern und Paketen enthalten sind, um sie zu löschen.

Informationen zu diesem Vorgang

Sie können angeben, wie lange die Protokoll-und Ausgabeversionen im Content Store aufbewahrt werden sollen. Alles, was älter ist als das von Ihnen angegebene Datum, wird aus dem Content Store gelöscht.

Wichtig: Beachten Sie die folgenden Umstände bei der Ausführung von Wartungstasks für die Inhaltsentfernung:

- Führen Sie diese Task nur nach der Erstellung und Ausführung der Content-Archivierungstask aus. Wenn Sie den Inhalt zuvor ausführen, wird der Inhalt, der nicht für die Archivierung markiert war, dauerhaft aus dem Content Store gelöscht.
- Der Inhalt, der zum Löschen markiert ist, wird nur in IBM Cognos Analyticsgelöscht. Der Inhalt wird in Ihrem externen Repository nicht gelöscht.

Vorgehensweise

1. Starten Sie IBM Cognos Administration.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
3. Klicken Sie in der Symbolleiste auf das Symbol für die neue Inhaltsverwaltung und klicken Sie dann auf **Inhaltsentfernung**.
4. Geben Sie einen Namen für die Task zum Entfernen von Inhalten und optional eine Beschreibung und einen Anzeigentipp ein.
5. Klicken Sie auf **Eine andere Position auswählen** , wenn Sie die Position bearbeiten möchten. Navigieren Sie zum Auswählen des Ordners, oder klicken Sie auf **Neuer Ordner** , um eine neue Position hinzuzufügen. Klicken Sie auf **OK**.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Ordner und Pakete aus, die Sie einschließen möchten.
8. Klicken Sie für die **Protokoll ausführen** -Einstellungen auf das Kontrollkästchen **Protokoll ausführen** , geben Sie den entsprechenden Wert in das Feld ein und wählen Sie dann **Tage** oder **Monate**aus.
9. Klicken Sie für die **Ausgabeversionen** -Einstellungen auf das Kontrollkästchen **Ausgabeversionen** , geben Sie den entsprechenden Wert in das Feld ein und klicken Sie anschließend entweder auf **Tage** oder auf **Monate**.
10. Wählen Sie die Aufzeichnungsstufe aus und klicken Sie auf **OK**.
11. Wählen Sie eine der folgenden Optionen aus:
    - Klicken Sie auf **Speichern und einmal ausführen**, um es jetzt oder später auszuführen. Klicken Sie auf **Fertigstellen**, geben Sie die Uhrzeit und das Datum für die Ausführung an, und klicken Sie anschließend auf **Ausführen**. Überprüfen Sie die Laufzeit und klicken Sie auf **OK**.
    - Klicken Sie auf **Speichern und planen**, um den Zeitplan zu einem wiederkehrenden Zeitpunkt zu planen. Klicken Sie auf **Fertigstellen**, und wählen Sie dann Häufigkeit und Start-und Enddaten aus. Klicken Sie auf **OK**.
    - Klicken Sie zum Speichern ohne Terminierung oder Ausführung auf **Nur speichern** und klicken Sie auf **Fertigstellen**.

Inhalt in Ihrem externen Repository suchen

Ihr archivierter Inhalt kann in IBM Cognos Analytics oder in Ihrem externen Repository angezeigt werden.

Nachdem der Inhalt verschoben und archiviert wurde, wird er an der Position gespeichert, die angegeben wurde, als Sie die Datenquellenverbindung zu Ihrem externen Repository erstellt haben.

Archivierte Inhalte durchsuchen

Sie können auf Inhalte zugreifen, die im Content-Store von IBM Cognos und in einem externen Repository gespeichert sind. Durch die Anzeige von Suchergebnissen für aktuelle und archivierte Inhalte können Benutzer kritische Vergleiche zwischen aktuellen Daten und historischen Daten vornehmen.

Bei der Suche nach archivierten Inhalten können Benutzer in einem Berichtsnamen oder in einem Datenelement in einem Bericht nach einem Element suchen. Der archivierte Inhalt kann angezeigt werden, indem Sie auf die Links in den Suchergebnissen klicken.

Der Inhalt, der in einem Berichtsrepository gespeichert ist, ist für IBM Cognos Arbeitsbereich nicht verfügbar. Wenn eine Suche in IBM Cognos ausgeführt wird, wird die archivierte Berichtsausgabe nicht gemeldet.

Kapitel 10. Sicherheitsmodell

Die Softwaresicherheit von IBM Cognos ist so konzipiert, dass die Sicherheitsanforderungen in verschiedenen Umgebungen erfüllt werden. Sie können sie in allen Bereichen von einer Konzeptanwendung verwenden, bei der die Sicherheit nur selten für eine große Enterprise-Implementierung aktiviert ist.

Das Sicherheitsmodell kann einfach mit der vorhandenen Sicherheitsinfrastruktur in Ihrem Unternehmen integriert werden. Er wird auf einer oder mehreren Authentifizierungsprovidererstellt. Sie verwenden die Provider, um Benutzer, Gruppen und Rollen zu definieren und zu verwalten und um den Authentifizierungsprozess zu steuern. Jeder Authentifizierungsprovider, der der IBM Cognos -Software bekannt ist, wird als Namespace  bezeichnet.

Zusätzlich zu den Namespaces, die die Authentifizierungsprovider darstellen, verfügt IBM Cognos über einen integrierten Namespace mit dem Namen „Cognos -Namespace” auf Seite 183. Der Cognos -Namespace verbessert Ihre Organisationssicherheitsrichtlinien und die Implementierungsfähigkeit von Anwendungen.

Die Sicherheit in der IBM Cognos -Software ist optional. Wenn die Sicherheit nicht aktiviert ist, bedeutet dies, dass keine Authentifizierungsprovider konfiguriert sind und daher der gesamte Benutzerzugriff anonym ist. In der Regel haben anonyme Benutzer nur einen begrenzten Lesezugriff.

Authentifizierungsprovider

Die Benutzerauthentifizierung in der IBM Cognos -Software wird von Authentifizierungsprovidern verwaltet. Authentifizierungsprovider definieren Benutzer, Gruppen und Rollen, die für die Authentifizierung verwendet werden. Benutzernamen, IDs, Passwörter, regionale Einstellungen, persönliche Vorlieben sind einige Beispiele für Informationen, die in den Anbietern gespeichert werden.

Wenn Sie die Authentifizierung für IBM Cognos -Software einrichten, müssen Benutzer bei der Anmeldezeit gültige Berechtigungsnachweise, wie z. B. die Benutzer-ID und das Kennwort, angeben. In einer IBM Cognos -Softwareumgebung werden Authentifizierungsprovider auch als Namespaces bezeichnet, und sie werden durch Namensbereichseinträge  in der Benutzerschnittstelle dargestellt.

IBM Cognos software does not replicate the users, groups, and roles defined in your authentication provider. Sie können sie jedoch in der IBM Cognos -Software referenzieren, wenn Sie Zugriffsberechtigungen für Berichte und andere Inhalte festlegen. Sie können auch Mitglieder von Cognos -Gruppen und -Rollen werden.

Die folgenden Authentifizierungsprovider werden in diesem Release unterstützt:

- Active Directory
- OpenID Connect
- Angepasster Java-Provider
- OpenID Connect-Authentifizierungsproxy
- IBM Cognos Series 7
- LDAP
- SAP
- SiteMinder

Sie konfigurieren Authentifizierungsprovider mit IBM Cognos -Konfiguration. Weitere Informationen finden Sie im *Installations-und Konfigurationshandbuch*.

Mehrere Namespaces

Wenn mehrere Namespaces für Ihr System konfiguriert sind, müssen Sie zu Beginn einer Sitzung einen Namespace auswählen, den Sie verwenden möchten. Dies hindert Sie jedoch nicht daran, sich später in der Sitzung bei anderen Namespaces anzumelden. Wenn Sie zum Beispiel Zugriffsberechtigungen festlegen, können Sie auf Einträge aus verschiedenen Namespaces verweisen. Wenn Sie sich an einem anderen Namespace anmelden möchten, müssen Sie sich nicht von dem Namespace abmelden, den Sie gerade verwenden. Sie können bei mehreren Namespaces gleichzeitig angemeldet sein.

Bei Ihrer primären Anmeldung handelt es sich um den Namespace und die Berechtigungsnachweise, die Sie für die Anmeldung zu Beginn der Sitzung verwenden. Die Namensbereiche, auf die Sie sich später in der Sitzung anmelden, und die Berechtigungsnachweise, die Sie verwenden, werden zu Ihren sekundären Anmeldungen.

Wenn Sie eines der Namespaces löschen, können Sie sich mit einem anderen Namespace anmelden. Wenn Sie alle Namensbereiche mit Ausnahme des Namespace Cognos löschen, werden Sie nicht zur Anmeldung aufgefordert. Wenn der anonyme Zugriff aktiviert ist, werden Sie automatisch als anonymer Benutzer angemeldet. Wenn der anonyme Zugriff nicht aktiviert ist, können Sie nicht auf die Anmeldeseite zugreifen. Verwenden Sie in dieser Situation die IBM Cognos -Konfiguration, um den anonymen Zugriff zu aktivieren.

Namensbereiche ausblenden

Sie können während der Anmeldung Namespaces von Benutzern ausblenden. Auf diese Weise können Sie anerkannte Namespaces signieren, ohne sie in der Namensbereichsauswahlliste anzuzeigen, die angezeigt wird, wenn sich die Benutzer anmelden.

Sie können beispielsweise die Einzelanmeldung über Systeme hinweg integrieren, aber die Möglichkeit für Kunden, sich direkt bei der IBM Cognos -Software zu authentifizieren, ohne dazu aufgefordert zu werden, einen Namespace auszuwählen.

Sie können angepasste Java -Provider-und eTrust-SiteMinder-Namespaces ausblenden, die Sie konfiguriert haben.

Weitere Informationen finden Sie im *Installations-und Konfigurationshandbuch*.

Nicht konfigurierte Namensbereiche löschen oder wiederherstellen

Sie können Namensbereiche und ihren gesamten Inhalt im Content-Store beibehalten, auch wenn sie nicht mehr für die Verwendung in IBM Cognos konfiguriert sind. Wenn ein Namespace nicht konfiguriert ist, wird er im Verzeichnis-Tool als inaktiv aufgelistet.

Ein inaktiver Namespace wurde konfiguriert, aber später in IBM Cognos Configuration gelöscht. Der Namespace kann von Mitgliedern der Rolle "Systemadministratoren" aus dem Content-Store gelöscht werden. Sie können sich nicht an einem inaktiven Namespace anmelden.

Wenn eine neue Version der IBM Cognos -Software einen zuvor konfigurierten Namespace erkennt, der nicht mehr verwendet wird, wird der Namespace im Verzeichnistool als inaktiv angezeigt. Sie können den Namensbereich erneut konfigurieren, wenn die Daten weiterhin erforderlich sind. Wenn der Namespace nicht erforderlich ist, können Sie ihn löschen.

Wenn Sie einen Namespace löschen, löschen Sie auch alle Einträge in "Meine Ordner", die diesem Namespace zugeordnet sind, und deren Inhalt.

Ein aktiver Namespace kann nicht gelöscht werden, sondern kann aktualisiert werden.

Wenn Sie einen Namespace in IBM Cognos Konfiguration erneut erstellen möchten, müssen Sie die ursprüngliche ID des Namespace verwenden. Informationen zum Konfigurieren und erneuten Erstellen von Namespaces finden Sie im *Installations-und Konfigurationshandbuch*.

Inaktiven Namensbereich löschen

Wenn ein Namespace aus IBM Cognos Configuration entfernt wurde und nicht mehr erforderlich ist, kann ein Mitglied der Rolle "Systemadministratoren" das Element dauerhaft im Verzeichniswerkzeug löschen. Durch das Löschen eines Namensbereichs werden auch alle Einträge in 'Eigene Ordner' gelöscht, die dem Namensbereich zugeordnet sind.

Um auf das Verzeichnisverwaltungstool zugreifen zu können, müssen Sie über Ausführungsberechtigungen für die gesicherte Funktion von **Datenquellenverbindungen** verfügen und Berechtigungen für die gesicherte Verwaltungsfunktion durchlaufen haben.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Sicherheit** auf **Benutzer, Gruppen und Rollen**.

   Wenn der Namespace, den Sie löschen möchten, kein Häkchen in der Spalte **Aktiv** hat, ist er inaktiv und kann gelöscht werden.
2. Klicken Sie in der Spalte **Aktionen** auf die Schaltfläche zum Löschen.

   Wenn der Namensbereich aktiv ist, ist die Schaltfläche zum Löschen nicht verfügbar.

Ergebnisse

Der Namespace wird dauerhaft gelöscht. Wenn Sie den Namespace in IBM Cognos erneut verwenden möchten, müssen Sie ihn mit IBM Cognos Configuration hinzufügen.

Berechtigung

Die Berechtigung ist der Prozess, bei dem der Zugriff auf Daten erteilt oder verweigert wird, und die Aktionen, die für diese Daten ausgeführt werden können, basierend auf einer Benutzeridentität.

IBM Cognos software authorization assigns permissions to users, groups, and roles that allow them to perform actions, such as read or write, on content store objects, such as folders and reports. Der Content-Store kann als Hierarchie von Datenobjekten angezeigt werden. Zu diesen Objekten gehören nicht nur Ordner und Berichte, sondern Pakete für die Erstellung von Berichten, Verzeichnissen und Servern.

Wenn IBM Cognos -Administratoren Berichte an Benutzer verteilen, können sie Ordner einrichten, in denen Berichte und andere Objekte gespeichert werden können. Sie können diese Ordner dann sichern, so dass nur autorisierte Mitarbeiter mit dem Ordnerinhalt andere Tasks anzeigen, ändern oder ausführen können.

Informationen zum Festlegen von Zugriffsberechtigungen für die IBM Cognos -Einträge finden Sie im Artikel Kapitel 12, „Zugriffsberechtigungen und Berechtigungsnachweise”, auf Seite 193. Informationen zur Content Manager-Hierarchie von Objekten und zu den ursprünglichen Zugriffsberechtigungen finden Sie im Artikel Anhang C, „Anfangszugriffsberechtigungen”, auf Seite 441.

Cognos -Namespace

Der Cognos -Namespace ist der integrierte Namespace für die IBM Cognos -Software. Sie enthält die IBM Cognos -Objekte, wie z. B. Gruppen, Rollen, Datenquellen, Verteilerlisten und Kontakte.

Während der Initialisierung des Content Store werden integrierte und vordefinierte Sicherheitseinträge in diesem Namespace Kapitel 15, „Anfangssicherheit”, auf Seite 223erstellt. You must modify the initial security settings for those entries and for the Cognos namespace immediately after installing and configuring IBM Cognos software „Sicherheitseinstellungen nach der Installation” auf Seite 238.

Sie können den Cognos -Namespace mit IBM Cognos -Konfiguration umbenennen, aber nicht löschen. Der Namespace ist immer aktiv.

Wenn Sie die Sicherheit in der IBM Cognos -Software festlegen, können Sie den Cognos -Namespace verwenden, um Gruppen und Rollen zu erstellen, die speziell für IBM Cognos -Software gelten. In diesem

Namespace können Sie auch Sicherheitsrichtlinien erstellen, die indirekt auf die Sicherheitseinträge in Authentifizierungsprovidern verweisen, so dass IBM Cognos Software leichter von einer Installation auf eine andere „Sicherheit und Implementierung“ auf Seite 300implementiert werden kann.

Der Cognos -Namespace ist in der IBM Cognos -Software immer vorhanden, aber die Verwendung von Cognos -Gruppen und -rollen, die er enthält, ist optional. Die im Namespace von Cognos erstellten Gruppen und Rollen packen die Benutzer, Gruppen und Rollen neu, die in den Authentifizierungsprovidern vorhanden sind, um ihre Verwendung in der IBM Cognos -Umgebung zu optimieren. Beispielsweise können Sie im Namespace von Cognos eine Gruppe mit dem Namen HR-Manager erstellen und diesen bestimmten Benutzern und Gruppen aus Ihren Unternehmens-IT-und HR-Organisationen, die in Ihrem Authentifizierungsprovider definiert sind, hinzufügen. Später können Sie Zugriffsberechtigungen für die HR-Manager-Gruppe auf Einträge in der IBM Cognos -Software festlegen.

IBM Cognos Application Firewall

IBM Cognos Application Firewall (CAF) ist ein Sicherheitstool, das zur Ergänzung der vorhandenen IBM Cognos -Softwaresicherheitsinfrastruktur auf Anwendungsebene verwendet wird. Die IBM Cognos Application Firewall analysiert, ändert und validiert HTTP-und XML-Anforderungen, bevor sie von den Gateways oder Dispatchern verarbeitet werden, und bevor sie an den anfordernden Client oder Service gesendet werden. Es handelt sich dabei um einen intelligenten Proxy für die IBM Cognos -Produktgateways und -Dispatcher und verhindert, dass die IBM Cognos -Komponenten zerstörerische Daten verwenden. Die häufigsten Arten von zerstörerischen Daten sind Pufferüberläufe und Cross-Site Scripting (XSS) Angriffe, entweder durch Skripteinspritzung in gültige Seiten oder Umleitung zu anderen Websites.

Die IBM Cognos Application Firewall stellt IBM Cognos -Komponenten mit Sicherheitsfunktionen bereit, die die Datenvalidierung und -sicherung, die Protokollierung und Überwachung sowie den Ausgabeschutz umfassen. Weitere Informationen finden Sie unter „Datenvalidierung und -schutz“ auf Seite 184 und „Protokollierung und Überwachung“ auf Seite 185.

Die IBM Cognos Application Firewall ist standardmäßig aktiviert und sollte nicht inaktiviert werden.

Sie können die IBM Cognos Application Firewall unabhängig von den anderen IBM Cognos -Komponenten aktualisieren.

Weitere Informationen zur IBM Cognos Application Firewall finden Sie im *Installations-und Konfigurationshandbuch*.

Datenvalidierung und -schutz

Durch die Validierung von Eingabedaten wird sichergestellt, dass die Daten im erwarteten Format basieren, basierend auf einer Gruppe vordefinierter Variablenregeln. HTML-Variablen, XML-Daten, Cookiewerte und Parameter werden auf diese Gruppe von Regeln überprüft.

IBM Cognos Application Firewall (CAF) führt eine positive Validierung von Parametern durch, anstatt nur nach bekannten Script-Injection-Tags oder allgemeinen SQL-Injection-Signaturen zu suchen. Jeder Parameter wird anhand einer Regel überprüft, die einen bestimmten Datentyp in einem bestimmten Format erwartet. Wenn die Daten nicht mit der CAF-Regel übereinstimmen, wird sie zurückgewiesen.

Um eine noch stärkere Validierung zu ermöglichen, gleicht CAF mit regulären Ausdrucksmustern ab, um Dateneingaben zu schützen, die komplizierte Formate verwenden.

Eine häufige Art des Angriffs ist es, einen Benutzer durch Änderung der Formparameter zu täuschen, in eine schädliche Website zu gehen. Die Back-Button-und Fehler-URL-Features eines Produkts stellen ein prickeltes Ziel für diese Art von Angriff dar.

CAF begrenzt die Liste der Hosts und Domänen, auf die eine Back-URL zugreifen kann. CAF kann mit einer Liste von Hostnamen, einschließlich Portnummern und Domänen, konfiguriert werden. Wenn eine Back-URL einen Host oder eine Domäne enthält, die nicht in der Liste enthalten ist, wird die Anforderung zurückgewiesen. Standardmäßig wird der Hostname des Dispatchers der Liste hinzugefügt. You can configure the list using IBM Cognos Configuration.

Weitere Informationen finden Sie im *Installations-und Konfigurationshandbuch*.

Protokollierung und Überwachung

IBM Cognos Application Firewall (CAF) kann alle Zugriffe auf IBM Cognos -Gateways und -Dispatcher überwachen und protokollieren. Verwenden Sie die Protokollierung, um mögliche Angriffe oder Missbrauch Ihrer IBM Cognos -Anwendungen zu verfolgen.

You can configure CAF to log access to a specific file or to use IBM Cognos log application (IPF) logging. Wenn die Protokollierung aktiviert ist, werden alle Anforderungen protokolliert, die die Validierung durch CAF fehlschlagen lassen.

Weitere Informationen finden Sie im *Installations-und Konfigurationshandbuch*.

Sie können das Web-Server-Anforderungsprotokoll verwenden, um detaillierte Informationen zu der IP-Adresse des Quellenclients bei einem mutmaßlichen Angriff abzurufen.

Cross-Site Scripting (XSS) -Codierung

Viele Kunden nutzen andere Anwendungen, wie z. B. eTrust SiteMinder, um Sicherheitslücken im Cross-Site Scripting zu überprüfen. Diese Produkte blockieren HTTP-Get-Anforderungen, die bestimmte Zeichen enthalten.

CAF codiert Zeichen in Cascading Style Sheets (CSS) mit URLs, um zu verhindern, dass andere Cross-Site Scripting-Tools die Zeichen blockieren.

Die CAF-XSS-Codierungsfunktion gilt nur für Kunden, die das IBM Cognos Analytics -Portal verwenden.

Die CAF-XSS-Codierung ist standardmäßig inaktiviert. Um diese Funktion zu aktivieren, verwenden Sie die IBM Cognos -Konfiguration.

Weitere Informationen finden Sie im *Installations-und Konfigurationshandbuch*.

Filtern von Fehlernachrichten

Einige Fehlernachrichten enthalten möglicherweise sensible Informationen, wie z. B. Servernamen. Standardmäßig werden die Fehlernachrichtendetails in der IBM Cognos -Software an IPF-Protokolldateien weitergeleitet und die Option für die sichere Fehlernachricht ist aktiviert. Die den Benutzern vorgestellten Informationen geben nur das Auftreten eines Fehlers an, ohne dass Details dazu vorhanden sind.

Sie können angeben, wer vollständige Fehlerdetails abrufen kann, die sensible Informationen enthalten können, indem Sie die Funktionalität von **Detaillierte Fehler** in der IBM Cognos -Verwaltung ändern. Normalerweise wird diese Funktion Verzeichnisadministratoren zugeordnet, aber Sie können sie auch anderen Benutzern zuordnen. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen”, auf Seite 207.

Informationen zum Abrufen von vollständigen Fehlerdetails finden Sie im Artikel „Vollständige Details für Secure Error-Nachrichten anzeigen” auf Seite 20.

Parametersignierung

Die Parametersignatur schützt Parameterwerte vor Manipulationen, wenn sie an einen Web-Browser gesendet werden. CAF kann Parameter oder bestimmte Teile von Daten signieren. Die Signatur wird nur in bestimmten Situationen verwendet. Sie ist aktiviert, wenn CAF aktiviert ist.

Kapitel 11. Benutzer, Gruppen und Rollen

Benutzer, Gruppen und Rollen werden für Authentifizierungs-und Berechtigungszwecke erstellt.

Sie können Gruppen und Rollen verwenden, die in IBM Cognos -Software erstellt wurden, sowie Benutzer, Gruppen und Rollen, die in Authentifizierungsprovidern erstellt wurden. Die Gruppen und Rollen, die in IBM Cognos -Software erstellt wurden, werden als Cognos -Gruppen und Cognos -Rollen bezeichnet.

Benutzer

Ein Benutzereintrag wird in einem Authentifizierungsprovider erstellt und verwaltet, um einen menschlichen oder einen Computeraccount eindeutig zu identifizieren. Sie können keine Benutzereinträge in der IBM Cognos -Software erstellen.

In den Providern werden Informationen über Benutzer, wie z. B. erste und letzte Namen, Kennwörter, IDs, Ländereinstellungen und E-Mail-Adressen, gespeichert. Dies sind jedoch möglicherweise nicht alle Informationen, die für die IBM Cognos -Software erforderlich sind. Sie gibt beispielsweise nicht die Position der persönlichen Ordner der Benutzer an, oder die Formatvorgaben für die Anzeige von Berichten. Diese zusätzlichen Informationen zu Benutzern werden in der IBM Cognos -Software gespeichert, aber wenn sie in IBM Cognos -Software adressiert sind, werden die Informationen als Teil des externen Namespace angezeigt.

Serie 7 Benutzer

Wenn Sie den Authentifizierungsprovider der IBM Cognos Series 7 konfiguriert haben, muss ein Benutzer aus diesem Namespace mindestens einer Access Manager-Benutzerklasse angehören, damit der Benutzer in der IBM Cognos -Software verwendet werden kann. Weitere Informationen finden Sie unter „Authentifizierungsprovider“ auf Seite 181.

Wenn Sie beispielsweise einen neuen Benutzer in Series 7 Access Manager erstellen und den Benutzer einer Benutzerklasse zuordnen, aber dann den Benutzer aus dieser Benutzerklasse entfernen, können Sie sich nicht als dieser Benutzer in der IBM Cognos -Software anmelden.

Benutzer löschen und erneut erstellen

Bei Authentifizierungsprovidern der Serie 7 können Sie keine zugeordneten Eigenschaften und Elemente verwalten, wenn Sie einen Benutzer löschen und erneut erstellen. Wenn ein Benutzer beispielsweise ein Objekt in **Meine Ordner**erstellt und dieser Benutzer dann gelöscht wird, werden die **Meine Ordner** -Objekte diesem Benutzer nicht mehr zugeordnet. Wenn ein Benutzer mit dem gleichen Namen erneut erstellt wird, werden die Objekte nicht wieder eingesetzt.

Wenn Sie einen LDAP-Server verwenden, hängt die Stabilität von **Meine Ordner** -Objekten davon ab, wie Sie die IDs verwenden. Wenn die Konfiguration des LDAP-Providers das Standardattribut "dn" für den Parameter "Unique Identifier" verwendet, behält ein wiederverwendter Benutzer mit demselben Namen die **Meine Ordner** -Objekte des ursprünglichen Benutzers ab. Wenn Sie den Parameter "Eindeutige ID" in ein eindeutiges Attribut ändern, das vom LDAP-Server festgelegt wurde, z. B. "nsuniqueid für Sun Java System", geht die Zuordnung von **Meine Ordner** -Objekten für einen gelöschten Benutzer verloren, und es wird ein neues **Meine Ordner** für einen Benutzer mit demselben Namen erstellt.

Sie können Benutzerprofile löschen, kopieren und ändern. Weitere Informationen finden Sie unter Kapitel 21, „Benutzerprofile verwalten“, auf Seite 331.

Benutzer-Locales

Eine Ländereinstellung gibt linguistische Informationen und kulturelle Konventionen für den Zeichentyp, die Sortierfolge, das Format von Datum und Uhrzeit, die Währungseinheit und die Nachrichten an. Sie können Locales für einzelne Produkte, Inhalte, Server, Autoren und Benutzer in der IBM Cognos -Software angeben.

Die Benutzerländereinstellung bezieht sich auf die Produkt-und Inhaltslocales für jeden IBM Cognos -Benutzer. Anforderungen von Benutzern kommen mit einer zugeordneten Ländereinstellung an. IBM Cognos software must determine the language and locale preferences of users and enforce an appropriate response locale when you distribute reports in different languages.

Eine Benutzerländereinstellung gibt die Standardeinstellungen an, die ein Benutzer für die Formatierung von Datumsangaben, Uhrzeiten, Währungen und Zahlen verwenden möchte. IBM Cognos software uses this information to present data to the user.

IBM Cognos software obtains a value for user locale by checking these sources, in the order listed:

- Einstellungen für Benutzervorgaben

  Wenn der Benutzer die Benutzervorgabeneinstellungen festlegt, verwendet die IBM Cognos -Software diese Einstellungen für die Produkt-und Inhaltsländereinstellung des Benutzers und für die Standardformatierungsoptionen. Die Benutzervorgabeneinstellungen überschreiben die Werte, die vom Authentifizierungsprovider abgerufen werden.

- Authentifizierungsprovider

  Wenn für den Authentifizierungsprovider Ländereinstellungen konfiguriert sind, die konfiguriert sind, verwendet IBM Cognos -Software diese Werte für die Produkt-und Inhaltsländereinstellung des Benutzers.

- Browsereinstellung

  Anonyme und Gastbenutzer können keine Benutzervorgabeneinstellungen festlegen. Für diese Benutzer ruft IBM Cognos eine Benutzerländereinstellung aus dem Browser ab, der auf dem Computer des Benutzers gespeichert ist.

Gruppen und Rollen

Gruppen und Rollen können wie folgt definiert werden.

Gruppen und Rollen stellen Sammlungen von Benutzern dar, die ähnliche Funktionen ausführen oder einen ähnlichen Status in einer Organisation haben. Beispiele für Gruppen sind Mitarbeiter, Entwickler oder Vertriebspersonal. Mitglieder von Gruppen können Benutzer und andere Gruppen sein. Wenn Benutzer sich anmelden, können sie keine Gruppe auswählen, die für eine Sitzung verwendet werden soll. Sie melden sich immer mit allen Berechtigungen an, die den Gruppen zugeordnet sind, zu denen sie gehören.

Roles in IBM Cognos software have a similar function as groups. Mitglieder von Rollen können Benutzer, Gruppen und andere Rollen sein.

Das folgende Diagramm zeigt die Struktur von Gruppen und Rollen.

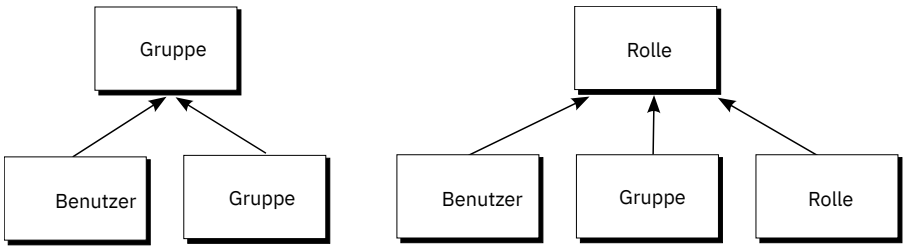


Abbildung 4. Struktur von Gruppen und Rollen

Benutzer können zu Mitgliedern von Gruppen und Rollen werden, die in IBM Cognos -Software definiert sind, sowie Gruppen und Rollen, die in Authentifizierungsprovidern definiert sind. Ein Benutzer kann zu einer oder mehreren Gruppen oder Rollen gehören. Wenn Benutzer Mitglieder von mehr als einer Gruppe sind, werden deren Zugriffsberechtigungen zusammengeführt.

Sie erstellen Cognos -Gruppen und -Rollen, wenn

- Sie können keine Gruppen oder Rollen in Ihrem Authentifizierungsprovider erstellen.

- Gruppen oder Rollen erforderlich sind, die mehrere Namespaces umfassen
- Es sind tragbare Gruppen und Rollen erforderlich, die implementiert werden können.

  Erstellen Sie die erforderlichen Gruppen und Rollen in Ihrem Authentifizierungsprovider, und fügen Sie sie zu den entsprechenden Cognos -Gruppen und -Rollen hinzu.
- Sie möchten die spezifischen Anforderungen der IBM Cognos -Administration adressieren.
- Sie möchten vermeiden, dass die Sicherheitssysteme Ihrer Organisation mit Informationen, die nur in der IBM Cognos -Software verwendet werden,

Serie 7-Rollen

Wenn Sie den Authentifizierungsprovider IBM Cognos Series 7 konfiguriert haben, werden Benutzerobjektgruppen, die als Benutzerklassen in Series 7 bezeichnet werden, als Rollen in der IBM Cognos -Software angezeigt. Sie können auf die Software Series 7 und IBM Cognos zugreifen, indem Sie eine einzelne Anmeldung verwenden. Wenn Sie Ihre Sitzung starten, indem Sie sich bei Series 7 anmelden und dann auf die IBM Cognos -Software zugreifen, übernehmen Sie automatisch die Rollen, die für Sie in Series 7 in Kraft waren, als Sie sich zuerst angemeldet haben. Sie können nicht verschiedene Rollen der Serie 7 übernehmen. Weitere Informationen zum Konfigurieren des Authentifizierungsproviders finden Sie im Artikel „Authentifizierungsprovider" auf Seite 181.

Benutzer können unterschiedliche Rollen in Series 7 übernehmen, nachdem sie auf die IBM Cognos -Software zugreifen.

Für die Ausführung von Berichten und Jobs verwendete Rollen

Die Rollen, die für die Ausführung von Berichten und Jobs verwendet werden, sind den Benutzern zugeordnet, die die Berichte interaktiv ausführen, die Berichtseigner sind und deren Berechtigungsnachweise für die Ausführung von geplanten Berichten und Jobs verwendet werden. Abhängig von den Optionen, die für die Ausführung von Berichten ausgewählt wurden, können von dem Prozess verschiedene Rollen angenommen werden.

- Wenn ein Bericht ausgeführt wird, der die Ausführung als Eigentümeroption ausgewählt hat, übernimmt der Prozess alle Rollen, die dem Berichtseigner zugeordnet sind.
- Wenn ein geplanter Bericht oder ein geplanter Job ausgeführt wird, übernimmt die Sitzung alle Rollen, die dem Benutzer zugeordnet sind, dessen Berechtigungsnachweise für die Verarbeitung der Anforderung „Vertrauenswürdige Berechtigungsnachweise" auf Seite 202verwendet wurden.

Verteilerlisten als Mitglieder von Gruppen und Rollen

In einigen Namespaces, wie z. B. Microsoft Active Directory, kann eine Verteilerliste auf der Registerkarte **Mitglieder** der **Eigenschaften festlegen** -Seite für eine Gruppe oder Rolle angezeigt werden. Sie können keine Verteilerlisten zu einer Gruppe oder einer Rollenzugehörigkeit hinzufügen, und Sie können diese nicht verwenden, um Zugriffsberechtigungen für Einträge in der IBM Cognos -Benutzerschnittstelle festzulegen.

Sie können eine IBM Cognos -Verteilerliste zu einer Cognos -Gruppe oder einer Rollenzugehörigkeit hinzufügen, indem Sie das Software Development Kit verwenden. Das Software Development Kit kann jedoch nicht zum Hinzufügen einer Active Directory-Verteilerliste zu einer Active Directory-Gruppe verwendet werden. Um dies zu tun, müssen die Active Directory-Verwaltungstools verwendet werden.

IBM Cognos Controller Groups and Roles

Für IBM Cognos -Software verwenden Sie IBM Cognos Controller-Gruppen und -Rollen, um die Sicherheit zu konfigurieren. For information about using these groups and roles to configure security, see the IBM Cognos Controller *Installations-und Konfigurationshandbuch*.

Cognos -Gruppe oder -Rolle erstellen

Sie können Einträge aus mehreren Namespaces hinzufügen, die sowohl in den Authentifizierungsprovidern als auch in der IBM Cognos -Software als Mitglieder von Cognos -Gruppen erstellt wurden. Sie können auch leere Gruppen erstellen, die keine Mitglieder haben.

Die Mitglieder von Cognos -Gruppen können Benutzer oder andere Gruppen sein. Die Mitglieder von Cognos -Rollen können Benutzer, Gruppen oder andere Rollen sein.

Wenn Sie planen, Gruppen oder Rollen zu erstellen, die auf Einträge aus mehreren Namespaces verweisen, müssen Sie sich bei jedem dieser Namespaces anmelden, bevor Sie Ihre Task starten. Andernfalls verfügen Sie nicht über vollständige Administratorberechtigungen für die Einträge, die Sie referenzieren möchten.

Es wird empfohlen, die Cognos -Gruppen und -Rollen zu verwenden, wenn Sie Zugriffsberechtigungen für Einträge in IBM Cognos -Software einrichten, da der Prozess der Implementierung vereinfacht wird. Weitere Informationen finden Sie unter „Sicherheit und Implementierung” auf Seite 300.

Wenn Sie eine Cognos -Gruppe oder -Rolle löschen, sind die Zugriffsberechtigungen der Benutzer auf der Basis dieser Gruppe nicht mehr aktiv. Sie können die Zugriffsberechtigungen nicht wiederherstellen, indem Sie eine Gruppe oder eine Rolle mit demselben Namen erstellen.

Um Benutzer, Gruppen und Rollen zu verwalten, müssen Sie über Ausführungsberechtigungen für das **Benutzer, Gruppen und Rollen** -gesicherte Feature verfügen und Berechtigungen für die geschützte **Verwaltung** -Funktion durchqueren. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen”, auf Seite 207.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Sicherheit** auf **Benutzer, Gruppen und Rollen**.
2. Klicken Sie auf den **Cognos** -Namespace.

   Tipp: Wenn Sie eine Cognos -Gruppe oder eine Rolle löschen möchten, wählen Sie das Kontrollkästchen neben dem Kontrollkästchen aus, und klicken Sie auf die Schaltfläche zum Löschen.
3. Klicken Sie in der Symbolleiste auf die neue Gruppe  oder auf die neue Rolle  .
4. Geben Sie auf der Seite **Geben Sie einen Namen und eine Beschreibung an** einen Namen und, wenn Sie möchten, eine Beschreibung für die neue Gruppe oder Rolle ein, und wählen Sie dann einen Zielordner aus und klicken Sie auf **Weiter**.
5. Wenn Sie eine Gruppe ohne Mitglieder erstellen möchten, klicken Sie auf **Fertigstellen**.
6. Wenn Sie der neuen Gruppe oder Rolle Mitglieder hinzufügen möchten, klicken Sie auf **Hinzufügen** und wählen Sie aus, wie die Benutzer, Gruppen oder Rollen ausgewählt werden sollen:
   - Wenn Sie aus aufgelisteten Einträgen auswählen möchten, klicken Sie auf den entsprechenden Namespace und wählen Sie anschließend die Kontrollkästchen neben den Benutzern, Gruppen oder Rollen aus.
   - Um nach Einträgen zu suchen, klicken Sie auf **Suchen** und geben Sie in das Feld **Suchbegriff** den Ausdruck ein, nach dem gesucht werden soll. Klicken Sie für Suchoptionen auf **Bearbeiten**. Suchen und klicken Sie auf den gewünschten Eintrag.
   - Wenn Sie den Namen der Einträge eingeben möchten, die hinzugefügt werden sollen, klicken Sie auf **Typ** , und geben Sie die Namen der Gruppen, Rollen oder Benutzer ein. Verwenden Sie dabei das folgende Format, wobei ein Semikolon (;) jeden Eintrag trennt: *namespace/group_name*;*namespace/role_name*;*namespace/user_name*;

     Im Folgenden sehen Sie ein Beispiel:

     Cognos/Authors; LDAP/scarter;
7. Klicken Sie auf die Schaltfläche mit der Rechtspfeiltaste, und klicken Sie auf **OK**, wenn die gewünschten Einträge im Feld **Ausgewählte Einträge** angezeigt werden.

Tipp: Wenn Sie Einträge aus der Liste **Ausgewählte Einträge** entfernen möchten, wählen Sie sie aus und klicken Sie auf **Entfernen**. Wenn Sie alle Einträge in der Liste auswählen möchten, wählen Sie das Kontrollkästchen für die Liste aus. Um die Benutzereinträge sichtbar zu machen, klicken Sie auf **Benutzer in der Liste anzeigen**.

8. Klicken Sie auf **Fertigstellen**.

Mitglieder einer Cognos -Gruppe oder einer Rolle hinzufügen oder entfernen

Sie können die Zugehörigkeit zu einer Cognos -Gruppe oder -Rolle ändern, indem Sie Mitglieder hinzufügen oder entfernen.

Wenn Sie Benutzer, Gruppen oder Rollen aus einer Cognos -Gruppe oder einer Rolle entfernen, löschen Sie sie nicht aus dem Authentifizierungsprovider oder aus der IBM Cognos -Software.

Wenn Sie Gruppen oder Rollen, die auf Einträge aus mehreren Namespaces verweisen, ändern möchten, müssen Sie sich bei jedem dieser Namespaces anmelden, bevor Sie Ihre Task starten. Andernfalls verfügen Sie nicht über die vollen Administratorberechtigungen für die Einträge, die Sie ändern möchten.

Um Benutzer, Gruppen und Rollen zu verwalten, müssen Sie über Ausführungsberechtigungen für das **Benutzer, Gruppen und Rollen** -gesicherte Feature verfügen und Berechtigungen für die geschützte **Verwaltung** -Funktion durchqueren. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen”, auf Seite 207.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Sicherheit** auf **Benutzer, Gruppen und Rollen**.
2. Klicken Sie auf den **Cognos** -Namespace.
3. Klicken Sie in der Spalte **Aktionen** auf die Schaltfläche Eigenschaften für die Gruppe oder die Rolle, deren Zugehörigkeit Sie ändern möchten.
4. Klicken Sie auf die Registerkarte **Mitglieder** .
5. Wenn Sie Mitglieder hinzufügen möchten, klicken Sie auf **Hinzufügen** , und wählen Sie aus, wie Mitglieder ausgewählt werden sollen:
   - Wenn Sie aus aufgelisteten Einträgen auswählen möchten, klicken Sie auf den entsprechenden Namespace und wählen Sie anschließend die Kontrollkästchen neben den Benutzern, Gruppen oder Rollen aus.
   - Um nach Einträgen zu suchen, klicken Sie auf **Suchen** und geben Sie in das Feld **Suchbegriff** den Ausdruck ein, nach dem gesucht werden soll. Klicken Sie für Suchoptionen auf **Bearbeiten**. Suchen und klicken Sie auf den gewünschten Eintrag.
   - Wenn Sie den Namen der Einträge eingeben möchten, die hinzugefügt werden sollen, klicken Sie auf **Typ** , und geben Sie die Namen von Gruppen, Rollen oder Benutzern ein. Verwenden Sie dabei das folgende Format, wobei ein Semikolon (;) jeden Eintrag trennt:

     namespace/group_name;*namespace/role_name*;*namespace/user_name*;

     Im Folgenden sehen Sie ein Beispiel:

     Cognos/Authors; LDAP/scarter;
6. Klicken Sie auf die Schaltfläche mit der Rechtspfeiltaste, und klicken Sie auf **OK**, wenn die gewünschten Einträge im Feld **Ausgewählte Einträge** angezeigt werden.

   Tipp: Wenn Sie Einträge aus der Liste **Ausgewählte Einträge** entfernen möchten, wählen Sie sie aus und klicken Sie auf **Entfernen**. Wenn Sie alle Einträge in der Liste auswählen möchten, wählen Sie das Kontrollkästchen für die Liste aus. Um die Benutzereinträge sichtbar zu machen, klicken Sie auf **Benutzer in der Liste anzeigen**.
7. Um Mitglieder aus einer Cognos -Gruppe oder einer Rolle zu entfernen, geben Sie auf der **Eigenschaften festlegen** -Seite an, welche Benutzer, Gruppen oder Rollen entfernt werden sollen, und klicken Sie auf **Entfernen**.

8. Klicken Sie auf **OK**.

Kapitel 12. Zugriffsberechtigungen und Berechtigungsnachweise

Sie verwenden Zugriffsberechtigungen und Berechtigungsnachweise, um die Daten Ihrer Organisation zu sichern. Sie geben an, welche Benutzer und Gruppen Zugriff auf einen bestimmten Bericht oder einen anderen Inhalt in der IBM Cognos -Software haben. Sie geben auch die Aktionen an, die sie für den Inhalt ausführen können.

Wenn Sie Zugriffsberechtigungen festlegen, können Sie sowohl Benutzer-, Gruppen-als auch Rollen-und Cognos -Gruppen und -Rollen für Authentifizierungsprovider referenzieren. Wenn Sie jedoch planen, Ihre Anwendung in der Zukunft zu implementieren, empfehlen wir Ihnen, nur die Gruppen und Rollen von Cognos zu verwenden, um den Zugriff auf Einträge in IBM Cognos -Software einzurichten, um den Prozess zu vereinfachen.

Berechtigungen und übertragene Aktionen

In der folgenden Tabelle werden die Zugriffsberechtigungen beschrieben, die Sie erteilen oder verweigern können.

Tabelle 51. Berechtigungen und zulässige Aktionen

Berechtigungen	Symbole	Zulässige Aktionen
Lesen		Zeigen Sie alle Eigenschaften eines Eintrags an, einschließlich der Berichtsspezifikation, der Berichtsausgabe usw., die Eigenschaften eines Berichts sind.
Schreiben		Eigenschaften eines Eintrags ändern. Löschen Sie einen Eintrag. Erstellen Sie Einträge in einem Container, wie z. B. einem Paket oder einem Ordner. Ändern Sie die Berichtsspezifikation für Berichte, die in Reporting und Query Studio erstellt wurden. Erstellen Sie neue Ausgaben für einen Bericht.

Tabelle 51. Berechtigungen und zulässige Aktionen (Forts.)		
Berechtigungen	**Symbole**	**Zulässige Aktionen**
Ausführen	  	Einen Eintrag verarbeiten. Bei Einträgen wie Berichten, Agenten und Metriken kann der Benutzer den Eintrag ausführen. Für Datenquellen, Verbindungen und Anmeldungen können die Einträge zum Abrufen von Daten von einem Datenprovider verwendet werden. Der Benutzer kann die Datenbankinformationen nicht direkt lesen. Der Berichtsserver kann auf die Datenbankinformationen im Namen des Benutzers zugreifen, um eine Anforderung zu verarbeiten. IBM Cognos software verifies whether users have execute permissions for an entry before they can use the entry. Für Berechtigungsnachweise können Benutzer eine andere Person für die Verwendung ihrer Berechtigungsnachweise zulassen. **Anmerkung:** Benutzer müssen über Ausführungsberechtigungen für das Konto verfügen, das sie mit der Ausführung als Eigner-Berichtsoption verwenden.
Richtlinie festlegen	  	Lesen und ändern Sie die Sicherheitseinstellungen für einen Eintrag.
Traverse	  	Zeigen Sie den Inhalt eines Containereintrags an, z. B. ein Paket oder einen Ordner, und zeigen Sie die allgemeinen Eigenschaften des Containers an, ohne den vollen Zugriff auf den Inhalt zu erhalten. **Anmerkung:** Benutzer können die allgemeinen Eigenschaften der Einträge anzeigen, für die sie einen beliebigen Zugriffstyp haben. Zu den allgemeinen Eigenschaften gehören Name, Beschreibung, Erstellungsdatum usw., die für alle Einträge gemeinsam sind.

Zugriffsberechtigungen für Benutzer

Benutzer müssen über mindestens Durchquemberechtigungen für die übergeordneten Einträge der Einträge verfügen, auf die sie zugreifen möchten. Zu den übergeordneten Einträgen gehören Container-Objekte wie Ordner, Pakete, Gruppen, Rollen und Namespaces.

Die Berechtigungen für Benutzer basieren auf Berechtigungen, die für einzelne Benutzerkonten und für die Namespaces, Gruppen und Rollen festgelegt sind, zu denen die Benutzer gehören. Berechtigungen sind auch von den Mitgliedschaftseigenschaften und den Eigentümereigenschaften des Eintrags betroffen.

IBM Cognos software supports combined access permissions. Wenn Benutzer, die zu mehr als einer Gruppe gehören, sich anmelden, verfügen sie über die kombinierten Berechtigungen aller Gruppen, zu denen sie gehören. Dies ist wichtig, um sich zu erinnern, vor allem, wenn Sie den Zugriff verweigern.

Tipp: Um sicherzustellen, dass ein Benutzer oder eine Gruppe Berichte aus einem Paket ausführen kann, aber das Paket nicht in einem IBM Cognos -Studio öffnen, erteilen Sie dem Benutzer oder der Gruppe die

Ausführungsberechtigung und die Berechtigung für das Paket für das Paket. Benutzer benötigen außerdem Leseberechtigungen für das Paket, um Studios zu starten.

Für Aktionen erforderliche Zugriffsberechtigungen

Zur Ausführung bestimmter Aktionen benötigt jeder Benutzer, jede Gruppe oder jede Rolle die richtige Kombination von Zugriffsberechtigungen, die für den Eintrag, seinen übergeordneten Eintrag und seinen Quellen-und Zieleintrag erteilt wurden. In der folgenden Tabelle werden die für bestimmte Aktionen erforderlichen Berechtigungen aufgelistet.

Tabelle 52. Für Aktionen erforderliche Zugriffsberechtigungen

Aktion	**Erforderliche Berechtigungen**
Eintrag hinzufügen	Schreibberechtigungen für einen übergeordneten Eintrag
Eingabeeigenschaften abfragen	Leseberechtigungen für einen Eintrag
Die untergeordneten Elemente des Eintrags anzeigen	Berechtigungen für einen Eintrag traversieren
Eintrag aktualisieren	Schreibberechtigungen für einen Eintrag
Eintrag löschen	Berechtigungen für einen Eintrag schreiben und Berechtigungen für einen übergeordneten Eintrag schreiben
Eintrag kopieren	Leseberechtigungen für einen Eintrag und alle untergeordneten Einträge, Durchquerung der Berechtigungen für alle untergeordneten Elemente sowie Schreib-und Transitberechtigungen für den übergeordneten Zieleintrag
Eintrag verschieben	Lese-und Schreibberechtigungen für einen Eintrag, Schreibberechtigungen für den übergeordneten Quelleneintrag und den übergeordneten Zieleintrag sowie Berechtigungen für den übergeordneten Ziel-Eintrag

Berechtigungen und zulässige Aktionen für Cognos -Arbeitsbereichsberichte

Cognos Workspace-Benutzer können oder können keine Aktionen ausführen, abhängig von ihren Berechtigungen und Kombinationen von Berechtigungen für einen Bericht, einen Berichtsteil, einen Berichtsordner oder Arbeitsbereichsobjekte. Der Eigner eines Objekts erhält automatisch Lese-, Schreib-, Traverts-und Ausführungsberechtigungen. Wenn ein Objekt inaktiviert ist, müssen Sie Schreibzugriff erhalten, damit Sie es sehen und bearbeiten können.

Für Berichte können Benutzer mit den folgenden Zugriffsberechtigungen und Kombinationen von Berechtigungen die folgenden Aktionen ausführen:

Tabelle 53. Berichtszugriffsberechtigungen und zulässige Aktionen

Berechtigungen	**Zulässige Aktionen**
Lesen	Benutzer können den Bericht im Inhaltsteilfenster anzeigen. Benutzer können den Bericht nicht erweitern, um die Berichtsteile anzuzeigen. Benutzer können den Bericht nicht ziehen.

Tabelle 53. Berichtszugriffsberechtigungen und zulässige Aktionen (Forts.)	
Berechtigungen	**Zulässige Aktionen**
Lesen und Traverse	Benutzer können den Bericht im Inhaltsteilfenster anzeigen. Benutzer können den Bericht nicht erweitern, um die Berichtsteile anzuzeigen. Wenn die gespeicherte Ausgabe vorhanden ist, können Benutzer den Bericht in den Erstellungsbereich ziehen und die gespeicherte Ausgabe anzeigen. Wenn die gespeicherte Ausgabe nicht vorhanden ist, können die Benutzer den Bericht nicht ziehen. Wenn sie versuchen, diese Aktion auszuführen, sehen Benutzer die Fehlernachricht im Widget. `Der Inhalt kann nicht angezeigt werden. Sie wurde möglicherweise gelöscht oder Sie verfügen nicht über ausreichende Berechtigungen.` Benutzer können die gespeicherte Ausgabe im Arbeitsbereich anzeigen. Benutzer können keinen Livebericht in einem Arbeitsbereich ausführen. Wenn sie versuchen, diese Aktion auszuführen, sehen die Benutzer die Fehlernachricht `RSV-CM-0006. Der Benutzer verfügt nicht über die Ausführungsberechtigung für diesen Bericht.`
Ausführen	Benutzer können den Bericht im Inhaltsteilfenster anzeigen. Benutzer können den Bericht nicht erweitern, um die Berichtsteile anzuzeigen. Benutzer können den Bericht ausführen, aber Interaktionen sind nicht verfügbar. Interaktionen sind nicht verfügbar, wenn: · Ein Bericht wird in den Erstellungsbereich gezogen. · Wenn ein Benutzer mit Ausführungsberechtigungen einen Bericht speichert, und andere Benutzer den Bericht öffnen · Wenn ein Benutzer mit Ausführungsberechtigungen einen Arbeitsbereich öffnet, der von anderen Benutzern erstellt wurde Wenn die gespeicherte Ausgabe nicht in einem Arbeitsbereich angezeigt werden kann, sehen die Benutzer die Fehlernachricht: `Der Inhalt kann nicht angezeigt werden. Sie wurde möglicherweise gelöscht oder Sie verfügen nicht über ausreichende Berechtigungen.`
Lesen und ausführen	Benutzer können den Bericht im Inhaltsteilfenster anzeigen. Benutzer können den Bericht erweitern, um die Berichtsteile anzuzeigen. Benutzer können den Bericht ausführen, und Interaktionen sind verfügbar. Im Inhaltsteilfenster können Benutzer keine Berichtsänderungen speichern. Wenn Benutzer den Bericht zu dem Arbeitsbereich hinzufügen und speichern, können Berichtsänderungen gespeichert werden. Wenn der Bericht von einer Person, die nicht der Berichtseigner ist, dem Arbeitsbereich hinzugefügt wird, kann dieser Benutzer keine Änderungen speichern. Der Benutzer sieht die Fehlernachricht: `Der Inhalt kann nicht gespeichert werden. Sie verfügen nicht über ausreichende Berechtigungen.`

Tabelle 53. Berichtszugriffsberechtigungen und zulässige Aktionen (Forts.)	
Berechtigungen	**Zulässige Aktionen**
Lesen, ausführen, traversieren	Benutzer können den Bericht im Inhaltsteilfenster anzeigen. Benutzer können den Bericht erweitern, um die Berichtsteile anzuzeigen. Im Inhaltsteilfenster können Benutzer den Bericht ausführen und Interaktionen verfügbar sein. Benutzer können den Bericht als Live-Ausgabe oder als gespeicherte Ausgabe in den Erstellungsbereich aufnehmen. Die Art des Berichts, der hinzugefügt wird, hängt von der Standardaktion ab, die in den Eigenschaften des Berichts angegeben ist.
Lesen, Schreiben, Ausführen, Durchqueren	Benutzer können den Bericht im Inhaltsteilfenster anzeigen. Benutzer können den Bericht erweitern, um die Berichtsteile anzuzeigen. Benutzer können den Bericht zum Arbeitsbereich hinzufügen. Benutzer können den Bericht ausführen, und Interaktionen sind verfügbar. Benutzer können den Bericht ändern und speichern. Benutzer können den Bericht als Live-Ausgabe oder als gespeicherte Ausgabe in den Erstellungsbereich aufnehmen. Die Art des Berichts, der hinzugefügt wird, hängt von der Standardaktion ab, die in den Eigenschaften des Berichts angegeben ist.
Lesen, Ausführen, Festlegen der Richtlinie	Benutzer können den Bericht im Inhaltsteilfenster anzeigen. Benutzer können den Bericht erweitern, um die Berichtsteile anzuzeigen. Benutzer können den Bericht ausführen, und Interaktionen sind verfügbar. Im Inhaltsteilfenster können Benutzer keine Berichtsänderungen speichern. Wenn Benutzer den Bericht in den Arbeitsbereich ziehen und speichern, können Berichtsänderungen gespeichert werden. Mit dieser Aktion wird eine Kopie des Berichts erstellt. Der kopierte Arbeitsbereichsbericht übernimmt die Berechtigungen aus dem ursprünglichen Bericht, wenn der Benutzer über die Berechtigung zum Festlegen der Richtlinie verfügt.

Für Berichtsteile können Benutzer mit den folgenden Zugriffsberechtigungen und Kombinationen von Berechtigungen die folgenden Aktionen ausführen:

Tabelle 54. Zugriffsberechtigungen und zulässige Aktionen des Berichtsteils	
Berechtigungen	**Zulässige Aktionen**
Lesen und ausführen	Benutzer können den Bericht anzeigen. Benutzer können den Bericht erweitern, um die Berichtsteile anzuzeigen. Benutzer können den Berichtsteil in den Erstellungsbereich ziehen und den Berichtsteil ausführen.

Für Ordner können Benutzer mit den folgenden Zugriffsberechtigungen und Kombinationen von Berechtigungen die folgenden Aktionen ausführen:

Tabelle 55. Ordnerzugriffsberechtigungen und zulässige Aktionen	
Berechtigungen	**Zulässige Aktionen**
Lesen	Benutzer können den Ordner im Inhaltsteilfenster anzeigen und Ordnereigenschaften lesen. Benutzer können den Ordner nicht in den Erstellungsbereich ziehen. Benutzer können den Ordner nicht erweitern, um den Inhalt anzuzeigen. Benutzer können Arbeitsbereichsobjekte in diesem Ordner nicht speichern.
Traverse	Benutzer können den Ordner auf den Erstellungsbereich ziehen. Benutzer können den Ordner erweitern, um den Inhalt anzuzeigen. Benutzer können Arbeitsbereichsobjekte in diesem Ordner nicht speichern.
Schreiben und traversieren	Benutzer können den Ordner auf den Erstellungsbereich ziehen. Benutzer können den Ordner erweitern, um den Inhalt anzuzeigen. Benutzer können Arbeitsbereichsobjekte in diesem Ordner speichern.

Für Arbeitsbereiche können Benutzer mit den folgenden Zugriffsberechtigungen und Kombinationen von Berechtigungen die folgenden Aktionen ausführen:

Tabelle 56. Zugriffsberechtigungen für den Arbeitsbereich und zulässige Aktionen	
Berechtigungen	**Zulässige Aktionen**
Lesen	Benutzer können den Arbeitsbereich anzeigen. Benutzer können den Arbeitsbereich nicht öffnen.
Lesen und traversieren	Benutzer können den Arbeitsbereich öffnen. Mit der Berechtigung 'Traverse' können Benutzer die Arbeitsbereichswidgets anzeigen.
Lesen, Schreiben und Durchqueren	Benutzer können den Arbeitsbereich anzeigen, öffnen und speichern.

Eigentumsrecht an Einträgen

Wenn der Benutzer Eigentümer eines Eintrags ist, verfügt der Benutzer über vollständige Zugriffsberechtigungen für den Eintrag. Auf diese Weise wird sichergestellt, dass Benutzer die Einträge, die sie besitzen, jederzeit abrufen und ändern können. Standardmäßig ist der Eigner des Eintrags der Benutzer, der den Eintrag erstellt. Jeder andere Benutzer, der Richtlinienberechtigungen für den Eintrag festgelegt hat, kann jedoch das Eigentumsrecht für den Eintrag übernehmen.

Gewährter Zugriff und verweigerter Zugriff

Sie können Zugriff gewähren oder den Zugriff auf Einträge verweigern. Neben dem Eintragsnamen auf der Registerkarte **Berechtigungen** wird ein Symbol angezeigt, das den Typ des Zugriffs darstellt. Beispiel:

Wenn eine Gruppe über Ausführungsberechtigungen für einen Bericht verfügt, wird dieses Symbol  neben dem Gruppennamen auf der Registerkarte **Berechtigungen** für den Bericht angezeigt. Wenn eine Gruppe Ausführungsberechtigungen für einen Bericht verweigert hat, wird dieses Symbol  neben dem Gruppennamen angezeigt.

Der verweigert Zugriff hat Vorrang vor dem Zugriff auf den Zugriff. Wenn Sie bestimmten Benutzern oder Gruppen den Zugriff auf einen Eintrag verweigern, ersetzen Sie andere Sicherheitsrichtlinien, die den Zugriff auf den Eintrag erteilen.

Wenn die Berechtigungen für die Erteilung und Verweigerung von Berechtigungen in Konflikt stehen, wird der Zugriff auf den Eintrag immer verweigert. Ein Benutzer gehört zum Beispiel zu zwei Gruppen. Eine Gruppe hat Zugriff auf einen Bericht, und die andere Gruppe hat Zugriff auf den gleichen Bericht. Der Zugriff auf diesen Bericht wird für den Benutzer verweigert.

Den Zugriff nur verweigern, wenn er wirklich erforderlich ist. In der Regel ist es eine bessere Verwaltungspraxis, Berechtigungen zu erteilen, als sie zu verweigern.

Berechtigungen für übergeordnete und untergeordnete Elemente

Wenn Zugriffsberechtigungen nicht definiert sind, erwirbt der Eintrag in der Regel Berechtigungen von seinem übergeordneten Eintrag. Sie können übergeordnete Berechtigungen ersetzen, indem Sie Berechtigungen für den untergeordneten Eintrag definieren.

Anmerkung: Wenn Sie ein Framework Manager-Paket erstellen, aber seine Sicherheit nicht definieren, stimmen seine Standardzugriffsberechtigungen nicht mit denen des übergeordneten Ordners überein. Führen Sie die folgenden Schritte aus, um sicherzustellen, dass die Zugriffsberechtigungen eines neuen Pakets mit denen des übergeordneten Pakets übereinstimmen:

1. Bearbeiten Sie die Datei *Installationsverzeichnis*\configuration\fm.ini
2. Zeile ändern

   ```
   <Preference Name="SetPolicyPackage">TRUE</Preference>
   ```

   bis

   ```
   <Preference Name="SetPolicyPackage">FALSE</Preference>
   ```

Weitere Informationen finden Sie im Artikel "Kapitel 7: Verlagspakete" in der *IBM Cognos Analytics Framework Manager-Benutzerhandbuch*.

Objekte, die nur als untergeordnete Objekte von anderen Objekten vorhanden sind, erwerben immer Berechtigungen von ihren Eltern. Beispiele für solche Objekte sind Berichtsspezifikationen und Berichtsausgaben. Sie sind durch das Software Development Kit zu sehen. Sie können keine Berechtigungen speziell für diese Objekte festlegen.

Berechtigungen und Implementierung

Berechtigungen für Funktionen

Wenn Sie ein Administrator sind, legen Sie den Zugriff auf die gesicherten Funktionen und Features fest, indem Sie Ausführungsberechtigungen für angegebene Namespaces, Benutzer, Gruppen oder Rollen erteilen. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen”, auf Seite 207.

Cognos -Gruppen und -Rollen löschen

Wenn Sie eine Cognos -Gruppe oder -Rolle löschen, werden auch die auf ihr basierenden Zugriffsberechtigungen gelöscht. Sie können sie nicht wiederherstellen, indem Sie eine neue Gruppe oder eine neue Rolle mit demselben Namen erstellen, da dieser Eintrag über eine andere interne ID verfügt.

Wenn Ihre Gruppen oder Rollen von Authentifizierungsprovidern erstellt werden, prüfen Sie, wie sich Ihr Authentifizierungsprovider mit solchen Situationen befasst. Normalerweise können Sie Zugriffsberechtigungen nicht erneut erstellen, wenn sie auf IDs basieren, aber Sie können, wenn sie auf Namen basieren.

Zugriff auf Einträge, die mit Datenquellen verbunden sind, die gegen mehrere Namespaces gesichert sind

Datenquellen in der IBM Cognos -Software können gegen mehrere Namespaces gesichert werden. In einigen Umgebungen ist der Namespace, der zur Sicherung der Datenquelle verwendet wird, nicht der primäre Namespace, der für den Zugriff auf IBM Cognos Analyticsverwendet wird. Wenn Sie versuchen, auf einen Eintrag, wie z. B. einen Bericht, eine Abfrage oder eine Analyse zuzugreifen, die einer Datenquelle zugeordnet ist, die für mehrere Namespaces gesichert ist, und Sie nicht an allen erforderlichen Namespaces angemeldet sind, wird eine Eingabeaufforderung für die Authentifizierung angezeigt. Sie müssen sich an dem Namespace anmelden, bevor Sie auf den Eintrag zugreifen können.

Wenn SSO (Single Sign-on) aktiviert ist, wird die Eingabeaufforderung für die Authentifizierung nicht angezeigt. Sie werden automatisch an dem Namespace angemeldet.

Diese Funktionalität gilt nur für IBM Cognos Viewer. Wenn eine ähnliche Situation in einem IBM Cognos -Studio auftritt, müssen Sie Ihre Task beenden und sich bei allen Namespaces anmelden, die in der aktuellen Sitzung verwendet werden sollen.

Zugriffsberechtigungen für einen Eintrag festlegen

Das Festlegen von Zugriffsberechtigungen für einen Eintrag umfasst das Erstellen neuer Berechtigungen oder das Aktualisieren vorhandener Berechtigungen. Sie können Zugriffsberechtigungen für alle Einträge in der IBM Cognos -Software angeben. Einige Beispiele für solche Einträge sind Berichte, Abfragen, Analysen, Pakete, Agenten, Metriken, Namespaces, Gruppen, Benutzer oder Dispatcher. Sie können Benutzer, Gruppen und Rollen aus verschiedenen Namespaces in einer Sicherheitsrichtlinie für einen Eintrag referenzieren.

Wenn Sie planen, Einträge aus mehreren Namespaces zu referenzieren, melden Sie sich bei jedem Namespace an, bevor Sie mit dem Festlegen der Zugriffsberechtigungen beginnen. Andernfalls werden Einträge in Namensbereichen, an denen Sie nicht angemeldet sind, als **Nicht verfügbar**angezeigt.

Einträge, auf die von einer Sicherheitsrichtlinie verwiesen wird, können auch als **Nicht verfügbar** angezeigt werden, wenn

- Die Einträge wurden kürzlich aus einem externen Namespace gelöscht.

  IBM Cognos software has no control over the content of security providers.
- Die Einträge sind einem externen Namespace zugeordnet, der kürzlich gelöscht wurde.

  Um dieses Problem zu vermeiden, müssen Sie die Konsistenzprüfungsart der Inhaltserwartungstask ausführen, indem Sie die Option **Verweise auf externe Namespaces**auswählen. Content Manager löscht Einträge, die den gelöschten Namespaces aus Sicherheitsrichtlinien zugeordnet sind.

  Weitere Informationen finden Sie unter „Wartungstasks für Content-Store” auf Seite 60.

Um die Sicherheit zu verwalten, müssen Sie Richtlinienberechtigungen festgelegt haben. Weitere Informationen finden Sie unter Kapitel 12, „Zugriffsberechtigungen und Berechtigungsnachweise”, auf Seite 193.

Hinweis für Cognos Analytics on Demand-Benutzer:

- Die Integrierte Standardgruppen und -rollen im Cognos-Namespace sind nicht vorhanden.
- Sie können die Funktionalität eines Benutzers, einer Gruppe oder einer Rolle nicht ändern. Die Funktionalität wird durch den on Demand-Subskriptionsebenedes Benutzers bestimmt.

Vorgehensweise

1. Suchen Sie in der IBM Cognos -Software den Eintrag, für den Sie Zugriffsberechtigungen festlegen möchten.
2. Klicken Sie in der Spalte **Aktionen** auf die Schaltfläche 'Eigenschaften festlegen'  für den Eintrag.
3. Klicken Sie auf der **Eigenschaften festlegen** -Seite auf die Registerkarte **Berechtigungen** .

4. Wählen Sie aus, ob die Berechtigungen für den übergeordneten Eintrag verwendet werden sollen, oder geben Sie Berechtigungen speziell für den Eintrag an:
   - Wenn Sie die Berechtigungen des übergeordneten Eintrags verwenden möchten, wählen Sie das Kontrollkästchen **Über den übergeordneten Eintrag erworbene Zugriffsberechtigungen überschreiben** ab, und klicken Sie anschließend auf OK, wenn Sie zur Verwendung der übergeordneten Berechtigungen aufgefordert werden. Klicken Sie auf **OK**.
   - Wenn Sie Zugriffsberechtigungen für den Eintrag festlegen möchten, wählen Sie das Markierungsfeld **Über den übergeordneten Eintrag erworbene Zugriffsberechtigungen überschreiben** aus, und fahren Sie mit Schritt 5 fort.
5. Wenn Sie einen Eintrag aus der Liste entfernen möchten, wählen Sie das entsprechende Kontrollkästchen aus und klicken Sie auf **Entfernen**.

   Tipp: Wenn Sie alle Einträge in der Liste auswählen möchten, wählen Sie das Kontrollkästchen für die Liste aus.
6. Wenn Sie die Einträge angeben möchten, für die Sie den Zugriff erteilen oder verweigern möchten, klicken Sie auf **Hinzufügen**und wählen Sie anschließend die Option zum Auswählen von Einträgen aus:
   - Wenn Sie aus aufgelisteten Einträgen auswählen möchten, klicken Sie auf den entsprechenden Namespace und wählen Sie anschließend die Kontrollkästchen neben den Benutzern, Gruppen oder Rollen aus.
   - Um nach Einträgen zu suchen, klicken Sie auf **Suchen** und geben Sie in das Feld **Suchbegriff** den Ausdruck ein, nach dem gesucht werden soll. Klicken Sie für Suchoptionen auf **Bearbeiten**. Suchen und klicken Sie auf den gewünschten Eintrag.
   - Wenn Sie den Namen der Einträge eingeben möchten, die hinzugefügt werden sollen, klicken Sie auf **Typ** , und geben Sie die Namen von Gruppen, Rollen oder Benutzern ein. Verwenden Sie dabei das folgende Format, wobei ein Semikolon (;) jeden Eintrag trennt:

     namespace/group_name;*namespace/role_name*;*namespace/user_name*;

     Im Folgenden sehen Sie ein Beispiel:

     Cognos/Authors; LDAP/scarter;
7. Klicken Sie auf die Schaltfläche mit der Rechtspfeiltaste, und klicken Sie auf **OK**, wenn die gewünschten Einträge im Feld **Ausgewählte Einträge** angezeigt werden.

   Tipp: Wenn Sie Einträge aus der Liste **Ausgewählte Einträge** entfernen möchten, wählen Sie sie aus und klicken Sie auf **Entfernen**. Wenn Sie alle Einträge in der Liste auswählen möchten, wählen Sie das Kontrollkästchen für die Liste aus. Um die Benutzereinträge sichtbar zu machen, klicken Sie auf **Benutzer in der Liste anzeigen**.
8. Wählen Sie für jeden Eintrag in der Liste in der Liste neben der Liste Kontrollkästchen aus, um anzugeben, welche Art von Zugriff Sie erteilen oder verweigern möchten.
9. Klicken Sie auf **OK**.

   In der Spalte **Berechtigungen** wird neben dem Benutzer, der Gruppe oder der Rolle ein Symbol angezeigt. Dieses Symbol stellt die Art des Zugriffs dar, der für den Eintrag erteilt oder verweigert wurde.
10. Wenn Sie Zugriffsberechtigungen entfernen möchten, die zuvor für die untergeordneten Einträge festgelegt wurden, sodass die untergeordneten Einträge die für diesen Eintrag festgelegten Berechtigungen erwerben können, wählen Sie im Abschnitt **Option** das Kontrollkästchen **Zugriffsberechtigungen für alle untergeordneten Einträge löschen** aus.

    Diese Option wird nur bei Einträgen angezeigt, die Container sind. Sie können diese verwenden, um den Zugriff auf eine Hierarchie von Einträgen zu beschränken.

    Warnung: Wählen Sie diese Option nur aus, wenn Sie sicher sind, dass die Änderung der Zugriffsberechtigungen für die untergeordneten Einträge sicher ist.
11. Klicken Sie auf **OK**.

Vertrauenswürdige Berechtigungsnachweise

Vertrauenswürdige Berechtigungsnachweise werden für Benutzer verwendet, die eine Task oder einen Prozess ausführen müssen, aber nicht über ausreichende Zugriffsberechtigungen für Einträge verfügen, die sensible Daten enthalten, wie z. B. Datenbanksignonen und Gruppenzugehörigkeiten. Benutzer mit umfangreicheren Zugriffsberechtigungen, die Eigner der Einträge sind, können einem vertrauenswürdigen Benutzer die Berechtigung zur Verwendung ihrer Berechtigungsnachweise für den Zugriff auf die Einträge berechtigen.

Vertrauenswürdige Berechtigungsnachweise werden auch für die Ausführung geplanter Anforderungen verwendet, wenn Benutzer nicht bei IBM Cognos -Software angemeldet sind, z. B. über Nacht. Wenn die Anforderung ausgeführt wird, wird eine Benutzersitzung erstellt. Der vertrauenswürdige Berechtigungsnachweis wird für die Anmeldung bei IBM Cognos -Software verwendet, da der Benutzer, der vertrauenswürdige Berechtigungsnachweise darstellt, und die Zugriffsberechtigungen des Benutzers für die Ausführung des Berichts oder des Jobs verwendet werden.

Vertrauenswürdige Berechtigungsnachweise können aus einer oder mehreren Berechtigungsnachweis-Paarings (Benutzer-ID und Kennwort) bestehen. Die Anzahl der vertrauenswürdigen Berechtigungsnachweise hängt von der Anzahl der Namespaces ab, die Sie während Ihrer Sitzung anmelden, wenn Sie Ihre Berechtigungsnachweise erstellen oder erneuern. Der Account, auf den die vertrauenswürdigen Berechtigungsnachweise angewendet werden, ist der erste Namensbereich, in dem Sie sich für diese Sitzung anmelden, auch als primärer Namespace bezeichnet.

Vertrauenswürdige Berechtigungsnachweise werden als Teil des Accountobjekts im Namespace gespeichert.

Standardmäßig werden vertrauenswürdige Berechtigungsnachweise automatisch einmal am Tag erneuert. Ein Administrator kann die Standarderneuerungsfrequenz ändern, indem er die Eigenschaft **expiryRenewedTC** in der Konfiguration von IBM Cognos unter **Sicherheit** > **Authentifizierung** > **Erweiterte Eigenschaften**angibt. Nur ganze Zahlen, die die Anzahl der Tage darstellen, können als Werte für diese Eigenschaft verwendet werden. Der Mindestwert ist 1.

Wenn Sie Ihr Kennwort während des Tages ändern, nachdem Ihre Berechtigungsnachweise automatisch in einer Cognos Analytics -Sitzung erneuert wurden, müssen Sie sie manuell erneuern, um zu verhindern, dass Zeitpläne, die die Berechtigungsnachweise verwenden, später am Tag nicht mehr verwendet werden. Beispiel: Sie melden sich am Morgen bei Cognos Analytics an. Die automatische Verlängerung erfolgt. Am Nachmittag ändern Sie Ihr Kennwort und melden sich erneut bei Cognos Analytics an. Die automatische Verlängerung fand bereits in diesem 24-Stunden-Zeitraum statt, so dass sie erst in der nächsten Erneuerungszeit wieder passieren wird. In diesem Fall müssen Sie manuell erneuern, um sicherzustellen, dass Zeitpläne später an diesem Tag nicht fehlschlagen.

Vertrauenswürdige Berechtigungsnachweise erstellen

Sie können vertrauenswürdige Berechtigungsnachweise erstellen, wenn Sie andere Benutzer für die Verwendung Ihrer Berechtigungsnachweise berechtigen möchten, da diese Benutzer nicht über ausreichende Zugriffsberechtigungen für die Ausführung bestimmter Tasks verfügen.

Damit Benutzer vertrauenswürdige Berechtigungsnachweise verwenden können, müssen Transitberechtigungen für den Namespace erteilt werden.

Vorgehensweise

1. Klicken Sie auf die Schaltfläche 'Meine Bereichsoptionen'  , **Eigene Vorgaben**.
2. Klicken Sie auf der Registerkarte **Personal** unter **Berechtigungsnachweise**, wenn Sie zuvor keine Berechtigungsnachweise erstellt haben, auf **Berechtigungsnachweise erstellen**.

   Tipp: Wenn Ihre vertrauenswürdigen Berechtigungsnachweise bereits erstellt wurden, müssen Sie sie möglicherweise nur erneuern, indem Sie auf **Berechtigungsnachweise erneuern**klicken.
3. Wählen Sie die Benutzer, Gruppen oder Rollen aus, die Sie für die Verwendung Ihrer Berechtigungsnachweise berechtigen möchten.

Wenn Sie aufgefordert werden, Ihre Berechtigungsnachweise einzugeben, geben Sie Ihre Benutzer-ID und Ihr Kennwort an.

4. Wenn Sie Einträge hinzufügen möchten, klicken Sie auf **Hinzufügen** , und wählen Sie aus, wie Einträge ausgewählt werden sollen:
   - Wenn Sie aus aufgelisteten Einträgen auswählen möchten, klicken Sie auf den entsprechenden Namespace und wählen Sie anschließend die Kontrollkästchen neben den Benutzern, Gruppen oder Rollen aus.
   - Um nach Einträgen zu suchen, klicken Sie auf **Suchen** und geben Sie in das Feld **Suchbegriff** den Ausdruck ein, nach dem gesucht werden soll. Klicken Sie für Suchoptionen auf **Bearbeiten**. Suchen und klicken Sie auf den gewünschten Eintrag.
   - Wenn Sie den Namen der Einträge eingeben möchten, die hinzugefügt werden sollen, klicken Sie auf **Typ** , und geben Sie die Namen von Gruppen, Rollen oder Benutzern ein. Verwenden Sie dabei das folgende Format, wobei ein Semikolon (;) jeden Eintrag trennt:

     Namensbereich/*Gruppenname*;*Namensbereich*/*Role_name*;*Namensbereich*/*Benutzername*;

     Im Folgenden sehen Sie ein Beispiel:

     Cognos/Authors; LDAP/scarter;
5. Wenn Sie einen Eintrag aus der Liste entfernen möchten, wählen Sie das Kontrollkästchen neben dem Eintrag aus, und klicken Sie auf **Entfernen**.

Ergebnisse

Die Benutzer, Gruppen oder Rollen, die Ihre Berechtigungsnachweise verwenden können, werden jetzt im Abschnitt **Berechtigungsnachweise** aufgelistet.

Vertrauenswürdige Berechtigungsnachweise automatisch erneuern

Wenn Sie Ihre IBM Cognos Analytics -Umgebung zum automatischen Erneuern von vertrauenswürdigen Berechtigungsnachweisen festlegen, können fehlgeschlagene Aktivitäten, die durch geänderte oder abgelaufene Benutzerberechtigungsnachweise verursacht werden, automatisch beseitigt werden. Wenn sich ein Benutzer bei Cognos Analytics mit einem Benutzernamen und einem Kennwort anmeldet, wird auch der vertrauenswürdige Berechtigungsnachweis aktualisiert, der für die Ausführung der geplanten Jobs verwendet wird.

Vorbereitende Schritte

Diese Einstellung funktioniert nur, wenn Ihre IBM Cognos Analytics -Umgebung die Basisauthentifizierung verwendet (wenn ein Benutzer einen Benutzernamen und ein Kennwort für die Anmeldung bereitstellt). Wenn Ihre Umgebung Single Sign-on (SSO) verwendet, können Sie diese Einschränkung umgehen, indem Sie die REMOTE_USER -Umgebungsvariable für SSO konfigurieren. Weitere Informationen zur Konfiguration der REMOTE_USER -Umgebungsvariablen siehe *Single Sign-on zwischen Active Directory Server und IBM Cognos Components aktivieren, um REMOTE_USER zu verwenden* in *Cognos Analytics Installation & Konfiguration*finden Sie unter.

Vorgehensweise

1. Öffnen Sie IBM Cognos Configuration.
2. Klicken Sie im **Explorer** -Fenster unter **Sicherheit**auf **Authentifizierung**.
3. Wählen Sie im Feld **Vertrauenswürdigen Berechtigungsnachweis automatisch erneuern** einen der folgenden Werte aus:

   Nur primärer Namespace
   Ihr primärer Namespace für die Cognos Analytics -Sitzung ist der Namensbereich der ersten Sitzung, an der Sie sich anmelden. Der Account, bei dem Sie sich angemeldet haben, wird als Container für die vertrauenswürdigen Berechtigungsnachweise betrachtet, die Sie für diese

Sitzung erstellen oder erneuern. Wenn Sie als vertrauenswürdige Berechtigungsnachweise für dieses Konto verfügen, werden die Berechtigungsnachweise für sie aktualisiert. Alle anderen Berechtigungsnachweise für andere Namespaces, für die Sie sich anmelden, werden nicht aktualisiert.

Dies ist der Standardwert.

AUS
Berechtigungsnachweise werden in keinem Namespace aktualisiert.

Alle Namensbereiche
Wenn Sie sich am ersten Namespace anmelden, werden Ihre Berechtigungsnachweise wie für den **Nur primärer Namespace** -Wert beschrieben aktualisiert. Wenn Sie sich bei mehr Namespaces anmelden, enthalten die vertrauenswürdigen Berechtigungsnachweise, die dem primären Namespace-Account zugeordnet sind, Anmeldedaten für die zusätzlichen Namespaces, und diese vertrauenswürdigen Berechtigungsnachweise werden ebenfalls aktualisiert. Beispiel: Sie möchten eine geplante Konsistenzprüfung ausführen, die mehrere Namespaces umfasst.

Vorsicht: Hierbei handelt es sich um eine systemweite Einstellung, die nur dann verwendet wird, wenn dies erforderlich ist.

Anmerkung: Wählen Sie diesen Wert nicht aus, wenn Sie Benutzer haben, die sich in sekundären Namespaces mit unterschiedlichen Benutzer-IDs authentifizieren. Wenn Sie diesen Wert auswählen, kann dies zu Konflikten in den Berechtigungsnachweisen führen, die für den Namespace erneuert werden.

4. Klicken Sie im Menü **Datei** auf **Speichern**.

Eigene Datenquellen-Berechtigungsnachweise verwalten

Es ist wichtig, die Berechtigungsnachweise für die Datenquelle für Ihre Benutzer zu verwalten, da diese Berechtigungsnachweise für bestimmte Tasks erforderlich sind.

Wenn Sie die folgenden Aktionen ausführen, werden Sie möglicherweise zur Eingabe Ihrer Berechtigungsnachweise für die Datenquelle aufgefordert:

- Einen Eintrag anzeigen, ausführen oder öffnen
- Verwenden Sie einen Zeitplan oder einen Job.
- Wählen Sie die Datenquellen aus, die zum Erstellen eines Pakets verwendet werden können.

Sie können bei der Verwendung von Framework Manager (siehe Framework Manager *Benutzerhandbuch*) auch zur Eingabe von Berechtigungsnachweisen für die Datenquelle aufgefordert werden.

Wenn Sie ein Administrator sind, können Sie Datenquellensignonenauch erstellen oder ändern. Wenn Sie jedoch viele Benutzer haben, kann dies für Datenquellenkonfigurationen, für die jeder Benutzer eine eigene Anmeldung benötigt, unhandlich sein, da die Berechtigungsnachweise für jeden Benutzer einzeln ausgeführt werden müssen. Sie können auch die Berechtigungsnachweise für die Datenquelle für andere Benutzer anzeigen.

Beachten Sie, dass die Berechtigungsnachweise in der folgenden Reihenfolge geprüft werden:

- Zuerst werden die Anmeldungen geprüft, die Sie als Administrator erstellen.
- Wenn für den Benutzer keine Berechtigungsnachweise gefunden wurden, wird das Profil des Benutzers überprüft, um festzustellen, ob die eigenen Berechtigungsnachweise gespeichert wurden.
- Sind keine Berechtigungsnachweise für den Benutzer an einer Stelle gefunden, wird der Benutzer zur Eingabe von Berechtigungsnachweisen aufgefordert.

Dies ist wichtig, denn wenn Sie Berechtigungsnachweise erstellen, nachdem ein Benutzer seine eigenen Berechtigungsnachweise gespeichert hat, erhalten sie Daten, die den Berechtigungsnachweisen zugeordnet sind, die Sie für sie erstellt haben. Dies ist möglicherweise nicht das, was sie erwartet haben.

Vorbereitende Schritte

Wenn Sie ein Benutzer sind, muss Ihr Administrator Ihnen Ausführungsberechtigungen für die **Eigene Datenquellensignonen verwalten** -Funktionalität erteilen und Berechtigungen für seine Vorfahren durchqueren. Außerdem müssen Sie über Lese-und Transitberechtigungen für Ihr Konto verfügen. Sie können dann Berechtigungsnachweise in Ihrem persönlichen Profil speichern, sofern Sie keinen Zugriff auf vordefinierte Anmeldedaten für die Datenquelle haben. Sie werden nicht zur Eingabe Ihrer Berechtigungsnachweise aufgefordert, wenn Sie über die Berechtigung zum Zugriff auf einen vorhandenen Datenquellen-Berechtigungsnachweis verfügen und Sie den persönlichen Berechtigungsnachweis in Ihrem Profil gespeichert haben. Sie können Ihre Datenquellenberechtigungsnachweise über die Seite **Eigene Vorgaben** anzeigen und löschen.

Um die Berechtigungsnachweise eines anderen Benutzers anzuzeigen, müssen Sie über Lese-und Transitberechtigungen auf dem Konto des Benutzers verfügen. Um Berechtigungsnachweise für Datenquellen zu entfernen, müssen Sie über Lese-, Schreib-und Querberechtigungen auf dem Konto des Benutzers verfügen.

Berechtigungsnachweise für Datenquelle speichern

Sie können Ihre Datenquellenberechtigungsnachweise speichern, damit Sie nicht jedes Mal zur Eingabe aufgefordert werden.

Vorgehensweise

1. Wenn Sie aufgefordert werden, Ihre Berechtigungsnachweise für die Datenquelle einzugeben, geben Sie Ihre Benutzer-ID und Ihr Kennwort ein.
2. Wählen Sie das Markierungsfeld **Meine Benutzer-ID und das Kennwort merken, wenn eine Verbindung zu dieser Datenquelle hergestellt wird.** aus.
3. Klicken Sie auf **OK**.

Ergebnisse

Wenn Sie das nächste Mal eine Aktion ausführen, für die die Berechtigungsnachweise für die Datenquelle erforderlich sind, werden Sie nicht dazu aufgefordert, es sei denn, sie wurden entfernt oder gelöscht oder sind abgelaufen.

Berechtigungsnachweise für Datenquelle anzeigen und entfernen

Sie können Ihre Berechtigungsnachweise für die Datenquelle anzeigen und löschen.

Vorgehensweise

1. Klicken Sie auf **Meine Area-Optionen**, **Eigene Vorgaben**.
2. Klicken Sie auf die Registerkarte **Personal** .

   Ihre Berechtigungsnachweise für die Datenquelle werden unter **Berechtigungsnachweise für Datenquellen**aufgelistet. Sie können die Liste nach **Datenquellenname** oder **Name der Datenquelle-Verbindung**sortieren.
3. Wenn Sie einen Berechtigungsnachweis für Datenquellen entfernen möchten, wählen Sie das Kontrollkästchen aus und klicken Sie dann auf **Entfernen**.

Kapitel 13. Funktionen

Die Funktionen innerhalb der Funktionen, die auch als gesicherte Funktionen und geschützte Features bezeichnet werden, steuern den Zugriff auf verschiedene Verwaltungstasks und verschiedene Funktionsbereiche der Benutzerschnittstelle in der IBM Cognos -Software.

Beispiele für die gesicherten Funktionen sind **Verwaltung** und **Reporting**. Beispiele für die gesicherten Features sind **Benutzerdefiniertes SQL** und **Platzen**.

Content Manager liest die Berechtigungen der Benutzer bei der Anmeldezeit. Abhängig von den Berechtigungen für die gesicherten Funktionen und Features können Benutzer auf bestimmte Komponenten zugreifen und bestimmte Tasks in der IBM Cognos -Software ausführen.

Wenn ein Content-Store initialisiert wird, werden die Anfangsberechtigungen für die gesicherten Funktionen und Features erstellt. Die Berechtigungen definieren, welche der vordefinierten und integrierten Cognos -Gruppen und -Rollen Zugriff auf die gesicherten Funktionen und Features und die Art des Zugriffs haben. Die Anfangsberechtigungen gewähren uneingeschränkten Zugriff auf IBM Cognos -Software, da die integrierten Rollensystemadministratoren die Gruppe "Jeder" in seiner Mitgliedschaft enthalten. Sie müssen die Gruppe "Jeder" aus der Zugehörigkeit zu den Systemadministratoren entfernen, bevor Sie mit der Einstellung des Zugriffs auf die Funktionalität beginnen.

Wenn Sie einen Bericht mit der Option **Als Eigner ausführen** ausführen, werden die Funktionen des Eigners für das Bersten und das Berichtslayout im HTML-Format verwendet. Alle anderen Funktionen basieren auf dem Benutzer, der den Bericht ausführt.

Anweisungen zum Zuordnen von Funktionen zu Benutzern, Gruppen und Rollen finden Sie unter „Zugriff auf Funktionen festlegen" auf Seite 217.

Benutzer können eine Liste der gesicherten Funktionen und Funktionen anzeigen, die ihnen in **Eigene Vorgaben** auf der Registerkarte **Personal** zur Verfügung stehen.

Weitere Informationen finden Sie unter „Anfängliche Zugriffsberechtigungen für Funktionen" auf Seite 443.

Anmerkung: Sie müssen **Verwalten** > **Personen** > **Funktionen** auswählen, um die vollständige Liste der Funktionen anzuzeigen. Obwohl viele der Funktionen auch in der Administrationskonsole angezeigt werden, empfehlen wir Ihnen, die Komponente **Verwalten** zum Zuordnen von Funktionen zu verwenden. Wenn die Verwaltung einer Funktionalität nur über die Komponente **Verwalten** ausgeführt werden kann, wird sie in der zugehörigen Beschreibung in der folgenden Liste aufgeführt.

Adaptive Analyse

Diese geschützte Funktion steuert den Zugriff auf die Berichte, die mithilfe von Adaptive Analytics gepackt werden.

Verwaltung

Diese geschützte Funktion enthält die gesicherten Funktionen, die den Zugriff auf die Verwaltungsseiten steuern, die Sie zur Verwaltung der IBM Cognos -Software verwenden. Systemadministratoren können diese Funktion verwenden, um Verwaltungstasks an verschiedene Administratoren zu delegieren.

Dieser Funktion sind die folgenden gesicherten Funktionen zugeordnet:

- **Adaptive Analytics-Administration**

  Benutzer können auf Adaptive Analytics zugreifen, um Verwaltungstasks auszuführen.

- **Verwaltungstasks**

  Users can access **Inhaltsverwaltung** on the **Konfiguration** tab in **IBM Cognos Administration** to administer exports, imports, consistency checks, and report updates.

- **Collaboration-Verwaltung**

Benutzer können auf die Möglichkeit zugreifen, Collaboration-Plattformen zu erstellen und zu steuern.

- **System konfigurieren und verwalten**

  Users can access **System** on the **Status** tab and **Dispatcher und Services** on the **Konfiguration** tab in **IBM Cognos Administration** to configure dispatchers and services, and to manage the system.

- **Controllerverwaltung**

  Benutzer können die Verwaltungsfunktionen von IBM Cognos Controller verwenden.

- **Datenquellenverbindungen**

  Users can access **Datenquellenverbindungen** on the **Konfiguration** tab in **IBM Cognos Administration** to define data sources, connections, and signons. In IBM Cognos Analytics on Cloud können sie auch über das Menü **Verwalten** auf die Seite **Sicheres Gateway** zugreifen.

- **Verteilerlisten und Kontakte**

  Benutzer können auf der Registerkarte **Konfiguration** in **IBM Cognos Administration** auf **Verteilerlisten und Kontakte** zugreifen, um Verteilerlisten und Kontakte zu verwalten.

- **Visualisierungen verwalten**

  Diese geschützte Funktion gibt an, dass der Benutzer Zugriffsrechte auf angepasste Visualisierungen für einzelne Benutzer, Gruppen und Rollen steuern kann.

  Anmerkung: Um diese geschützte Funktion zu verwalten, müssen Sie **Verwalten** > **Personen** > **Funktionen**auswählen. Sie können diese Funktion nicht über die **Verwaltungskonsole**verwalten.

- **Mobile Administration**

  Benutzer können IBM Cognos Analytics Mobile Reports -Services und -Anwendungen verwalten.

- **Planungsverwaltung**

  Benutzer können auf IBM Cognos Planning Contributor Administration Console und IBM Cognos Planning Analyst zugreifen, um Verwaltungstasks auszuführen.

- **PowerPlay-Server**

  Der Benutzer erhält nur eingeschränkten Zugriff auf die IBM Cognos -Verwaltungsseiten. Dazu gehört der Zugriff auf die PowerPlay -Seite und die Fähigkeit zum Festlegen von PowerPlay -Eigenschaften.

- **Drucker**

  Benutzer können auf **Drucker** auf der Registerkarte **Konfiguration** in **IBM Cognos Administration** zugreifen, um Drucker zu verwalten.

- **Service 'Query Service'**

  Benutzer können auf die **Status** > **Datenspeicher** -Seite in **IBM Cognos Administration** zugreifen, um dynamische Cubes zu verwalten. Benutzer können Operationen für Würfel ausführen, wie z. B. Cubes starten und stoppen, den Datencache aktualisieren und Abfrageservicetasks erstellen und planen.

- **Aktivitäten und Zeitpläne ausführen**

  Benutzer können auf der Registerkarte **Status** in **IBM Cognos Administration** auf **Aktuelle Aktivitäten**, **Vergangene Aktivitäten**, **Anstehende Aktivitäten** und **Zeitpläne** zugreifen, um die Serveraktivitäten zu überwachen und Zeitpläne zu verwalten. Um unabhängig von der Überwachungsfunktion den Zugriff auf die Planungsfunktionalität zu erteilen, verwenden Sie die Funktion "Terminierung".

- **Funktionalität festlegen und UI-Profile verwalten**

  Benutzer können auf der Registerkarte **Sicherheit** in **IBM Cognos Administration** auf **Funktionen** und **Benutzerschnittstellenprofile** zugreifen, um die gesicherten Funktionen und Features und die Reporting -Benutzerschnittstellen-Profile zu verwalten.

- **Stile und Portlets**

  Benutzer können auf der Registerkarte **Konfiguration** in **IBM Cognos Administration** auf **Stile** und **Portlets** zugreifen, um Stile und Portlets zu verwalten.

- **Benutzer, Gruppen und Rollen**

Users can access **Benutzer, Gruppen und Rollen** on the **Sicherheit** tab in **IBM Cognos Administration** to manage namespaces, users, groups, and roles.

AI

Diese Funktion ermöglicht den designierten Benutzern den Zugriff auf die KI-Funktionalität. Die Rollen, die standardmäßig mit Ausführungsberechtigungen erteilt werden, werden im Abschnitt AI-Funktionalität aufgelistet.

Anmerkung: Zum Verwalten dieser Funktion und der zugehörigen gesicherten Funktionen müssen Sie **Verwalten** > **Personen** > **Funktionen**auswählen. Sie können diese Funktion nicht über die **Verwaltungskonsole**verwalten.

Dieser Funktion sind die folgenden gesicherten Funktionen zugeordnet:

- 11.1.6 **-Learning**

  Diese geschützte Funktion ermöglicht es dem System, von der Produktnutzung eines Zessionars zu lernen.

- 11.1.5 **-Assistent**

  Diese geschützte Funktion ermöglicht den designierten Benutzern die Verwendung des Assistenten.

Analysestudio

Diese geschützte Funktion steuert den Zugriff auf IBM Cognos Analysis Studio. Benutzer mit Zugriff auf dieses Studio untersuchen, analysieren, vergleichen dimensionale Daten, finden aussagekräftige Informationen in großen Datenquellen und beantworten Geschäftsfragen.

Ausgabe anhängen

11.1.7 Diese Funktion ermöglicht es einem Benutzer, Ausgaben in einer E-Mail anzuhängen, wenn ein Zeitplan festgelegt, ein Bericht im Hintergrund ausgeführt oder Jobschritte gesetzt werden.

Anmerkung: Um diese Funktion zu verwalten, müssen Sie **Verwalten** > **Personen** > **Funktionen**auswählen. Sie können diese Funktion nicht über die **Verwaltungskonsole**verwalten.

Cognos Analytics for Mobile

11.1.7 Diese Funktion ermöglicht Benutzern den Zugriff auf Cognos Analytics über die App "Cognos Analytics for Mobile". Die Rollen, die standardmäßig mit Ausführungsberechtigungen erteilt werden, werden im Abschnitt "Cognos Analytics for Mobile-Funktion" von Anfängliche Zugriffsberechtigungen für Funktionenaufgelistet.

Anmerkung: Um diese Funktion zu verwalten, müssen Sie **Verwalten** > **Personen** > **Funktionen**auswählen. Sie können diese Funktion nicht über die **Verwaltungskonsole**verwalten.

Cognos Insight

Diese geschützte Funktion steuert den Zugriff auf IBM Cognos Insight. Benutzer, die Zugriff auf dieses Tool haben, arbeiten mit komplizierten Datenquellen, um die Verwendung von Arbeitsbereichen zu erkennen, zu visualisieren und zu planen, um Arbeitsbereiche zu verwenden.

Cognos-Viewer

Diese geschützte Funktion steuert den Zugriff auf IBM Cognos Viewer, den Sie zum Anzeigen von Berichten verwenden.

Die mit dieser Funktion verbundenen gesicherten Funktionen sind

- **Kontextmenü**

  Benutzer können das Kontextmenü in IBM Cognos Viewer verwenden.

Hinweis: Zum Anzeigen des Kontextmenüs müssen Benutzer über Zugriff auf die gesicherten Funktionen von **Auswahl** und **Kontextmenü** verfügen.

- **Mit Optionen ausführen**

  Benutzer können die Standardlaufoptionen ändern. Wenn Benutzer über keine Ausführungsberechtigungen für diese Funktion verfügen, können sie das Symbol **Mit Optionen ausführen**  für Berichte nicht anzeigen.

- **Auswahl**

  Benutzer können Text in Listen und Kreuztabellen auswählen.

- **Symbolleiste**

  Benutzer können die Symbolleiste des IBM Cognos -Viewers anzeigen.

Zusammenarbeiten

Diese geschützte Funktion steuert den Zugriff auf IBM Connections innerhalb von IBM Cognos.

Zu dieser Funktion gehören die folgenden gesicherten Funktionen:

- **Collaboration-Tools starten**

  Die geschützte Funktion ermöglicht es Benutzern, IBM Connections über ein beliebiges Startmenü in der IBM Cognos Analytics -Umgebung zu starten, einschließlich der Seite "Erste Schritte" des Cognos -Arbeitsbereichs und des Menüs "Aktionen". Die Links werden auf der IBM Connections-Homepage des Benutzers, sofern sie konfiguriert ist, oder auf der Seite "Aktivitäten" angezeigt.

- **Kollaborationskomponenten zulassen**

  Diese geschützte Komponente steuert den Zugriff auf das Symbol **Zusammenarbeiten** und die Suchergebnisse für IBM Connections-Suchergebnisse im Arbeitsbereich von Cognos . Benutzer müssen über Zugriff zum Erstellen oder Anzeigen von Aktivitäten innerhalb von Cognos Workspace verfügen.

Controller Studio

Diese geschützte Funktion steuert den Zugriff auf IBM Cognos Controller.

Dashboard

Diese geschützte Funktion steuert den Zugriff auf die Ansicht 'Dashboards' und 'Stories'. Benutzer benötigen Ausführungsberechtigungen für die Dashboard-Funktion, um sowohl Dashboards als auch Storys anzuzeigen. Die Rollen, die standardmäßig mit Ausführungsberechtigungen erteilt werden, werden im Abschnitt „Dashboardfunktion“ auf Seite 456 aufgelistet.

Anmerkung: Zur Verwaltung dieser seecured-Funktion müssen Sie **Verwalten** > **Personen** > **Funktionen**auswählen. Sie können diese Funktion nicht über die **Verwaltungskonsole**verwalten.

Datenmanager

Diese geschützte Funktion steuert den Zugriff auf Data Manager.

Datensätze

Diese geschützte Funktion steuert den Zugriff auf das Menü **Datei erstellen** , das über die Kontextmenüs des Pakets und des Datenmoduls verfügbar ist.

Desktop-Tools

Diese geschützte Funktion steuert den Zugriff auf die Produkte von Cognos Desktop Tools. Benutzer mit dieser Funktion sind Mitglieder der Rolle "Analyseserucher". Auf diese Weise können sie auf Cognos

Analysis For Microsoft Excel, Cognos Framework Manager, Cognos Cube Designer und Dynamic Query Analyzer, Transformer und TM1 Writeback für den gebündelten FLBI TM1 Server zugreifen.

Detaillierte Fehler

Diese geschützte Funktion steuert den Zugriff auf die Anzeige detaillierter Fehlernachrichten im Web-Browser.

Visualisierungen entwickeln

Diese geschützte Funktion gibt an, dass der Benutzer angepasste Visualisierungen entwickeln kann.

Anmerkung: Um diese Funktion zu verwalten, müssen Sie **Verwalten** > **Personen** > **Funktionen**auswählen. Sie können diese Funktion nicht über die **Verwaltungskonsole**verwalten.

Drillthrough-Assistent

Diese geschützte Funktion steuert den Zugriff auf die Drillthrough-Debugging-Funktionalität in der Drillthrough- **Gehe zu** -Seite und in den Drillthrough-Definitionen. Benutzer, die über diese Funktion verfügen, sehen für jedes Drillthrough-Ziel zusätzliche Informationen auf der Seite **Gehe zu** . Diese Informationen können helfen, eine Drillthrough-Definition zu debuggen, oder sie können an den Cognos Software Services-Ansprechpartner weitergeleitet werden.

Ereignisstudio

Diese geschützte Funktion steuert den Zugriff auf Event Studio.

E-Mail

11.1.7 Diese Funktion ermöglicht es einem Benutzer, eine E-Mail zu senden, wenn Inhalte terminiert oder gemeinsam genutzt werden. Die Rollen, die standardmäßig mit Ausführungsberechtigungen erteilt werden, werden im Abschnitt "E-Mail-Funktion" von Anfängliche Zugriffsberechtigungen für Funktionenaufgelistet.

Anmerkung: Zum Verwalten dieser Funktion und der zugehörigen gesicherten Funktionen müssen Sie **Verwalten** > **Personen** > **Funktionen**auswählen. Sie können diese Funktion nicht über die **Verwaltungskonsole**verwalten.

Dieser Funktion sind die folgenden gesicherten Funktionen zugeordnet:

Optionen für E-Mail

Diese geschützte Funktion ermöglicht es einem Benutzer, bei der Festlegung eines Zeitplans die E-Mail-Zustellung auszuwählen, einen Bericht im Hintergrund auszuführen oder Jobschritte zu definieren.

Link in E-Mail einschließen

Diese geschützte Funktion ermöglicht es einem Benutzer, beim Teilen von Inhalten, beim Festlegen eines Zeitplans oder bei der Ausführung eines Berichts im Hintergrund eine Verknüpfung zum Inhalt aus einer E-Mail zu erhalten.

Mit E-Mail teilen

Diese geschützte Funktion ermöglicht es einem Benutzer, annotierte Screenshots per E-Mail von **Gemeinsam nutzen** > **Senden**zu teilen.

Typ in externer E-Mail

Diese geschützte Funktion ermöglicht es einem Benutzer, externe Empfänger in einer E-Mail einzugeben. Wenn die gesicherte Funktion nicht erteilt wird, kann der Benutzer nur Empfänger aus ihren authentifizierten Namespaces auswählen.

Indexierte Suche ausführen

Diese geschützte Funktion steuert den Zugriff auf die Suche nach indizierten Inhalten. Diese geschützte Funktion wird erst angezeigt, wenn der Indexaktualisierungsservice gestartet wurde.

Standardmäßig ermöglicht Execute Indexed Search eine erweiterte indexierte Suche. Wenn die indexierte Suche inaktiviert ist, wird eine grundlegende indexierte Suche bereitgestellt.

Executive-Dashboard

Diese geschützte Funktion steuert den Zugriff auf den Arbeitsbereich von IBM Cognos . Benutzern, die Zugriff auf diese Funktion haben, werden grundlegende Berechtigungen für die Arbeitsbereiche in Cognos Workspace erteilt. Mit diesem Typ von Berechtigungen können Benutzer die Arbeitsbereiche anzeigen, auf den Arbeitsbereichdaten ein Drilldown durchführen, Kommentare hinzufügen, die Arbeitsbereiche drucken, Schieberegler verwenden und Wertfilter auswählen, wenn diese Filter in den Arbeitsbereich eingeschlossen werden.

Die folgenden gesicherten Funktionen, die der Funktion **Executive-Dashboard** zugeordnet sind, erteilen die umfangreicheren Berechtigungen für den Arbeitsbereich:

- **Erweiterte Dashboard-Funktionen verwenden**

  Verwenden Sie diese Funktion, um den Benutzern maximale Berechtigungen für den Arbeitsbereich zu erteilen.

- **Interaktive Dashboard-Features verwenden**

  Verwenden Sie diese Funktion, um den Benutzern Berechtigungen für den Zugriff auf die Arbeitsbereichsfunktionen zu erteilen, die die Interaktion mit den Widgetdaten zulassen. Dazu gehört der Zugriff auf die On-Demand-Symbolleiste im Widget, die Optionen für die Interaktion mit den Berichtsdaten bereitstellt, wie z. B. Sortieren, Löschen, Zurücksetzen, Vertauschen von Zeilen und Spalten, und Ändern des Anzeigetyps für Berichte.

Exploration

Diese geschützte Funktion steuert den Zugriff auf die Funktion **Neu** > **Exploration** . Benutzer benötigen Ausführungsberechtigungen für die Explorationsfunktion sowohl zum Erstellen oder Anzeigen von Erkundungsangaben. Die Rolle wird standardmäßig mit Ausführungsberechtigungen erteilt, die in Abschnitt „Explorationsfähigkeit” auf Seite 463 . aufgelistet sind.

Externer Inhalt

Diese Funktion ermöglicht es dem Empfänger, Inhalte aus Quellen zu verwenden, die sich außerhalb von IBM Cognos Analytics befinden.

Anmerkung: Zum Verwalten dieser Funktion und der zugehörigen gesicherten Funktionen müssen Sie **Verwalten** > **Personen** > **Funktionen**auswählen. Sie können diese Funktion nicht über die **Verwaltungskonsole**verwalten.

Die geschützte Funktion, die der Funktion für externe Inhalte zugeordnet ist, ist **Watson Studio**. Sie ermöglicht dem Empfänger die Erstellung von Assets im Content-Store von Cognos Analytics, die auf externe Watson Studio-Notizbücher verweisen.

Externe Repositorys

Diese geschützte Funktion steuert den Zugriff auf externe Repositorys. Externe Repositorys stellen einen Langzeitspeicher für Berichtsinhalte bereit. Wenn eine Verbindung zu einem externen Repository für ein Paket oder einen Ordner angegeben wird, werden Berichtsausgabeversionen automatisch in das Repository kopiert.

Die mit dieser Funktion verbundenen gesicherten Funktionen sind

- **Repository-Verbindungen verwalten**

Benutzer können eine Repository-Verbindung für ein Paket oder einen Ordner festlegen, wenn bereits eine Datenquellenverbindung vorhanden ist.

- **Externe Dokumente anzeigen**

  Benutzer können die Berichtsausgabe, die in einem externen Repository gespeichert ist, anzeigen.

CSV-Ausgabe generieren

Mit Berechtigungen für diese geschützte Funktion können Benutzer Berichtsausgaben im CSV-Format (CSV = Begrenzte Text) generieren. Ohne diese Funktion sehen Benutzer in der Benutzerschnittstelle keine Option zum Ausführen von Berichten im CVS-Format.

PDF-Ausgabe generieren

Mit Berechtigungen für diese geschützte Funktion können Benutzer Berichtsausgaben im PDF-Format generieren. Ohne diese Funktion sehen die Benutzer in der Benutzerschnittstelle keine Option, um Berichte im PDF-Format auszuführen.

XLS-Ausgabe generieren

Mit Berechtigungen für diese geschützte Funktion können Benutzer Berichtsausgaben in den Formaten der Microsoft Excel-Tabelle (XLS) generieren. Ohne diese Funktion sehen Benutzer in der Benutzerschnittstelle keine Option für die Ausführung von Berichten in den XLS-Formaten.

XML-Ausgabe generieren

Mit Berechtigungen für diese geschützte Funktion können Benutzer Berichtsausgaben im XML-Format generieren. Ohne diese Funktion sehen Benutzer in der Benutzerschnittstelle keine Option zum Ausführen von Berichten im XML-Format.

Glossar

Diese geschützte Funktion steuert den Zugriff auf das Business-Glossar von IBM InfoSphere .

Einträge ausblenden

Diese geschützte Funktion gibt an, dass ein Benutzer Einträge ausblenden und ausgeblendete Einträge in der IBM Cognos -Software anzeigen kann.

Das Kontrollkästchen **Diesen Eintrag ausblenden** wird auf der Registerkarte **Allgemein** auf den Eigenschaftenseiten der Einträge angezeigt. Das Kontrollkästchen **Ausgeblendete Einträge anzeigen** wird auf der Registerkarte **Vorgaben** in Benutzerprofilen und auf der Registerkarte **Allgemein** in den Optionen  , **Eigene Vorgaben**, angezeigt.

Relationale Metadaten importieren

Gibt an, dass eine Gruppe relationale Metadaten unter Verwendung des dynamischen Abfragemodus in ein Framework Manager-oder Dynamic Cube Designer-Projekt importieren kann.

Standardmäßig gehören die Gruppen "Systemadministrator", "Verzeichnisadministrator" und "Berichtsadministratoren" zu dieser gesicherten Funktion.

Wenn andere Gruppen die Möglichkeit benötigen, relationale Metadaten in ein dynamisches Abfragemodusprojekt zu importieren, müssen sie der Funktion hinzugefügt werden. Wenn Sie z. B. eine Framework Manager-Benutzergruppe erstellen und Ihre Framework Manager-Benutzer zu dieser Gruppe hinzufügen, müssen Sie auch die Gruppe zur gesicherten Funktion für den Import relationaler Metadaten hinzufügen.

Job

Diese geschützte Funktion steuert, ob ein Benutzer in der Lage ist, Jobs zu erstellen.

Anmerkung: Um diese Funktion zu verwalten, müssen Sie **Verwalten** > **Personen** > **Funktionen**auswählen. Sie können diese Funktion nicht über die **Verwaltungskonsole**verwalten.

Abstammung

Diese geschützte Funktion steuert den Zugriff auf die Aktion **Abstammung** . Verwenden Sie diese Option, um Informationen zu Daten oder Metadatenelementen aus IBM Cognos Viewer oder aus der Quellenverzeichnisstruktur in Reporting, Query Studio und Analysis Studio anzuzeigen.

Inhalt verwalten

Diese gesicherten Funktionen steuern den Zugriff auf die Registerkarte **Inhalt** in **Verwalten**.

Eigene Datenquellensignonen verwalten

Diese geschützte Funktion steuert die Fähigkeit, die Berechtigungsnachweise für die Datenquelle auf der Registerkarte **Personal** in **Eigene Vorgaben**zu verwalten.

Mobil

Diese geschützte Funktion steuert den Zugriff auf IBM Cognos Analytics Mobile Reports.

Notizbuch

Diese geschützte Funktion steuert den Zugriff auf die Option **Neu** > **Notizbuch** . Benutzer benötigen Ausführungsberechtigungen für die Notebook-Funktion, um Notebooks zu erstellen.

Anmerkung: Um diese Funktion zu verwalten, müssen Sie **Verwalten** > **Personen** > **Funktionen**auswählen. Sie können diese Funktion nicht über die **Verwaltungskonsole**verwalten.

Planungsbeitragszahler

Diese geschützte Funktion steuert den Zugriff auf den Planungskontributor IBM Cognos Planning Contributor und den Planungsanalytiker IBM Cognos .

PowerPlay Studio

Diese geschützte Funktion steuert den Zugriff auf PowerPlay Studio.

Abfragestudio

Diese geschützte Funktion steuert den Zugriff auf das Query Studio, mit dem Sie einfache Ad-hoc-Berichte erstellen können.

Die dieser Funktion zugeordnete gesicherte Funktion ist

- **Erstellen**

  Erstellen Sie neue Berichte und verwenden Sie die Option Speichern als Option für neue Berichte und angepasste Ansichten.

- **Erweitert**

  Verwenden Sie erweiterte Authoring-Funktionen, wie z. B. das Erstellen von komplexen Filtern, das Formatieren von Stil und die mehrsprachige Unterstützung.

Berichtsstudio

Diese geschützte Funktion steuert den Zugriff auf die Reporting -Benutzerschnittstelle und auf die zugrunde liegende Berichtsausführungsfunktionalität. Benutzer benötigen Ausführungsberechtigungen für diese geschützte Funktion, um auf die Reporting -Benutzerschnittstelle zugreifen zu können. Traversen oder Leseberechtigungen für diese geschützte Funktion sind unter Umständen erforderlich, um die zugeordneten gesicherten Funktionen zu verwenden, z. B. um Berichte auszuführen, die mit angepasstem SQL oder eingebettetem HTML erstellt wurden.

Zu dieser Funktion gehören die folgenden gesicherten Funktionen:

- **Externe Daten zulassen**

  Benutzer können externe Daten in Berichten verwenden.

- **Platzen**

  Benutzer können Burstberichte erstellen und ausführen.

- **Erstellen/Löschen**

  Benutzer können neue Berichte erstellen, die Option Speichern als Option für neue Berichte und Berichtsansichten verwenden und Modelle ändern.

- **HTML-Elemente im Bericht**

  Benutzer können die Schaltfläche "HTMLItem" und die Hyperlinkelemente der Berichtsspezifikation verwenden, wenn sie Berichte erstellen.

- **Benutzerdefiniertes SQL**

  Benutzer können die SQL-Anweisungen direkt in der Abfragespezifikation bearbeiten und die Abfragespezifikationen ausführen, die die bearbeitete SQL-Anweisungen enthalten.

  Tipp: Einschränkungen für die Benutzer, die diese Funktion verwenden können, werden in Framework Manager nicht umgesetzt. Ein Framework-Manager-Benutzer, der keine **Benutzerdefiniertes SQL** -Rechte in **IBM Cognos Administration** hat, kann beispielsweise weiterhin ein Abfragesubjekt erstellen und manuell erstellte SQL-Abfragen für die Suche einer Datenbank verwenden.

In Cloud speichern

11.1.5 Diese Funktion ermöglicht designierten Benutzern, ihre Berichtsausgabe in der Cloud zu speichern. Benutzer benötigen Ausführungsberechtigungen für die Funktion "In Cloud speichern", um das Kontrollkästchen **In der Cloud speichern** als Zustellungsoption für gespeicherte Berichtsausgaben anzuzeigen. Die Rollen, die standardmäßig mit Ausführungsberechtigungen erteilt werden, werden im Abschnitt In Cloud-Funktion speichern aufgelistet.

Anmerkung: Zum Verwalten dieser Funktion und der zugehörigen gesicherten Funktion müssen Sie **Verwalten** > **Personen** > **Funktionen**auswählen. Sie können diese Funktion nicht über die **Verwaltungskonsole**verwalten.

Dieser Funktion ist die folgende gesicherte Funktion zugeordnet:

- **Verbindungen verwalten**

  Mit dieser geschützten Funktion können Verzeichnisadministratoren auf die **Verwalten** > **Speicher** -Seite zugreifen, um Verbindungen zu externen Cloud Object Storage-Services zu erstellen und zu verwalten. Designierte Benutzer können dann auf das Feature **In der Cloud speichern** zugreifen.

Planung

Die Funktion "Zeitplanung" ermöglicht einem Benutzer, Elemente zu planen, die ausgeführt werden können, wie z. B. Berichte. Benutzer müssen über die Funktion "Zeitplanung" verfügen, um die Option

Meine Zeitpläne und Abonnements im persönlichen Menü  anzuzeigen. Weitere Informationen finden Sie im Artikel "Meine Zeitpläne und Abonnements" in der *IBM Cognos Analytics-Erste Schritte*.

Die mit dieser Funktion verknüpften gesicherten Funktionen sind

- **Terminieren nach Tag**

  Benutzer können Einträge täglich planen.

- **Zeitplan nach Stunde**

  Benutzer können Einträge nach der Stunde planen.

- **Zeitplan für Minute**

  Benutzer können Einträge bis zu einer Minute planen.

  Wenn einem Benutzer der Zugriff auf die Funktion **Zeitplan für Minute** verweigert wird, wird auch für andere Funktionen, die die Terminierung von 'by Minute' zulassen, z. B. die Funktion **Zeitplan nach Monat** , eine 'by Minute' -Terminierung verweigert.

- **Zeitplan nach Monat**

  Benutzer können die Einträge monatlich planen.

- **Zeitplan nach Auslöser**

  Benutzer können Einträge auf der Basis eines Auslösers planen.

- **Zeitplan für Woche**

  Benutzer können Einträge wöchentlich planen.

- **Zeitplan für Jahr**

  Benutzer können die Einträge jährlich planen.

- **Terminierungspriorität**

  Benutzer können die Verarbeitungspriorität geplanter Einträge einrichten und ändern.

  Anmerkung: Ein Benutzer, der ein Element terminiert (d. h. ein Bericht, ein Ereignis, ein Job usw.), ohne dass die Funktion **Terminierungspriorität** einen Artikel mit einer anderen Priorität als 3 planen kann, kann nicht terminiert werden. Eine andere Priorität kann festgelegt werden und im Zeitplan von einem Benutzer mit dem entsprechenden Zugriff angezeigt werden. Der Bericht wird jedoch weiterhin mit einer Priorität von 3 ausgeführt, es sei denn, sein Eigentumsrecht wird auch an einen Benutzer mit dem entsprechenden Zugriff auf die **Terminierungspriorität** -Funktionalität geändert.

Self-Service-Paketassistent

Diese geschützte Funktion steuert die Möglichkeit, auszuwählen, welche Datenquellen zum Erstellen eines Pakets verwendet werden können.

Eingabe-spezifische Funktionen festlegen

Diese geschützte Funktion gibt an, dass ein Benutzer Funktionen auf einer Eingangsebene einrichten kann.

Die Registerkarte **Funktionen** wird auf den **Eigenschaften festlegen** -Seiten für Pakete und Ordner für Benutzer angezeigt, die über diese Funktion verfügen und die Richtlinienberechtigungen für den Eintrag festgelegt haben oder die Eigner des Eintrags sind.

Share Pin Board

11.1.7 Benutzer, denen diese Funktion zugeordnet ist, können eine Pinnwand gemeinsam nutzen, die sie mit Cognos Analytics for Mobile erstellt haben.

Anmerkung: Um diese Funktion zu verwalten, müssen Sie **Verwalten** > **Personen** > **Funktionen**auswählen. Sie können diese Funktion nicht über die **Verwaltungskonsole**verwalten.

Spezifikationsausführung

Diese geschützte Funktion ermöglicht es einer Benutzer-oder Software-Development-Kit-Anwendung, eine integrierte Spezifikation zu verwenden. Die gesicherte Funktion "Specification Execution" wird als Berechtigungsklasse für Analyseadministratorengezählt.

IBM Cognos Analytics -Studios und einige Services verwenden intern integrierte Spezifikationen für die Ausführung von Tasks. Der Service, der die Spezifikation ausführt, testet eine Reihe von Funktionen, um sicherzustellen, dass der Benutzer berechtigt ist, die integrierte Spezifikation zu verwenden. Weitere Informationen finden Sie in der Methode "runSpecification" in der *Entwicklerhandbuch*.

Dateien hochladen

Diese geschützte Funktion steuert den Zugriff auf die Funktion **Dateien hochladen** . Benutzer, die über diese Funktion verfügen, können Datendateien hochladen.

Visualisierungsalerts

11.1.7 Benutzer, denen diese Funktion zugeordnet ist, können einen Alert für eine Pinnwand in Cognos Analytics for Mobile erstellen.

Anmerkung: Um diese Funktion zu verwalten, müssen Sie **Verwalten** > **Personen** > **Funktionen**auswählen. Sie können diese Funktion nicht über die **Verwaltungskonsole**verwalten.

Überwachungsregeln

Diese geschützte Funktion steuert den Zugriff auf die Registerkarte **Regeln** in **Meine Überwachungselemente**. Verwenden Sie diese geschützte Funktion, um Überwachungsregeln zu erstellen und auszuführen.

Webbasierte Modellierung

Diese geschützte Funktion steuert den Zugriff auf die webbasierte Modellierungsfunktion. Benutzer, die über diese Funktion verfügen, können Datenmodule über das Menü **Neu** > **Datenmodul** erstellen.

Zugriff auf Funktionen festlegen

Sie legen den Zugriff auf die Funktionen fest, die auch als geschützte Funktionen und Features bezeichnet werden, indem Sie den angegebenen Namespaces, Benutzern, Gruppen oder Rollen die Berechtigungen "Ausführen" und "Traverse" erteilen.

Anmerkung: Ein Benutzer muss über die Berechtigungen "Execute" und "Traverse" für eine Funktion oder eine seiner Unterfunktionen verfügen, die im Menü "Personal" unter **Eigene Vorgaben** > **Personal** > **Erweitert** > **Eigene Funktionen** > **Details anzeigen**angezeigt werden soll.

Vorbereitende Schritte

Für die Verwaltung von gesicherten Funktionen und Features müssen Sie über die Richtlinienberechtigungen verfügen. In der Regel wird dies von Verzeichnisadministratoren ausgeführt.

Bevor Sie mit der Festlegung von Berechtigungen für Funktionen beginnen, müssen Sie sicherstellen, dass die ursprünglichen Sicherheitseinstellungen bereits geändert wurden.

Vorgehensweise

1. Klicken Sie in **Verwalten** > **Personen**auf **Funktionen**.

   Es wird eine Liste der verfügbaren gesicherten Funktionen angezeigt.

2. Klicken Sie für die geschützte Funktion, die Sie ändern möchten, auf das Symbol 'Mehr'  und anschließend auf **Eigenschaften**.

3. Klicken Sie auf die Registerkarte **Zugriff** .
4. Wählen Sie aus, ob die Berechtigungen des übergeordneten Eintrags verwendet werden sollen, oder geben Sie verschiedene Berechtigungen an:
   - Wenn Sie die Berechtigungen des übergeordneten Eintrags verwenden möchten, wählen Sie das Kontrollkästchen **Übergeordneter Zugriff überschreiben** ab und klicken Sie auf **Anwenden**.
   - Wenn Sie Zugriffsberechtigungen explizit für den Eintrag festlegen möchten, wählen Sie das Kontrollkästchen **Übergeordneter Zugriff überschreiben** aus und führen Sie dann die verbleibenden Schritte aus.
5. Wenn Sie einen Eintrag aus der Liste entfernen möchten, klicken Sie auf das Symbol 'Mitglied entfernen'  .
6. Wenn Sie der Liste neue Einträge hinzufügen möchten, klicken Sie auf das Symbol 'Mitglied hinzufügen'  und wählen Sie aus, wie Einträge ausgewählt werden sollen:
   - Wenn Sie aus aufgelisteten Einträgen auswählen möchten, klicken Sie auf den entsprechenden Namespace, und klicken Sie anschließend auf die gewünschten Benutzer, Gruppen oder Rollen. Klicken Sie auf **Hinzufügen** , wenn Sie fertig sind.
   - Wenn Sie mehrere Einträge gleichzeitig auswählen möchten, klicken Sie auf Ctrl-click.
   - Um nach Einträgen zu suchen, geben Sie Text in das  ein. Feld **Suchen** .

     Anmerkung: Sie können auf das Symbol "Suchmethode"  klicken, um Einträge zu suchen, die entweder enthalten, mit dem Text beginnen oder eine exakte Übereinstimmung mit dem Typ haben, den Sie eingeben.
   - Klicken Sie auf das Symbol 'Filter  ', um die Sicht der Einträge einzugrenzen.
   - Wenn Sie den Namen der Einträge eingeben möchten, die hinzugefügt werden sollen, klicken Sie auf **Typ** , und geben Sie die Namen von Gruppen, Rollen oder Benutzern ein. Verwenden Sie dabei das folgende Format, wobei ein Semikolon (;) jeden Eintrag trennt:

     namespace/group_name;*namespace/role_name*;*namespace/user_name*;

     Im Folgenden sehen Sie ein Beispiel:

     Cognos/Authors; LDAP/scarter;
7. Wählen Sie das Feld in der Spalte **Berechtigungen** neben dem Eintrag aus, für den Sie den Zugriff auf die Funktion oder Funktion festlegen möchten.
8. Wählen Sie eine der folgenden Berechtigungen aus: **Zugriff**, **Zuordnen**, **Verwalten**oder **Angepasst**.

   Weitere Informationen finden Sie unter „Berechtigungsstufen" auf Seite 443.
9. Klicken Sie auf **Anwenden**.
10. Klicken Sie auf **OK** , wenn Sie fertig sind.

Kapitel 14. Objektfunktionalität

Objektfunktionen geben die gesicherten Funktionen und Features an, die Benutzer, Gruppen oder Rollen mit verschiedenen Paketen verwenden können. Zum Beispiel definieren die Funktionen das Studio, um ein Paket zu öffnen, und die Studio-Features, die während der Arbeit mit diesem Paket verfügbar sind.

Die gesicherten Funktionen und ihre Funktionen, die auch als globale Funktionen bezeichnet werden, steuern den Zugriff auf die verschiedenen Komponenten und Funktionen in IBM Cognos -Software. Damit Objektfunktionen funktionieren können, müssen Sie sie mit den anwendbaren globalen Funktionen kombinieren. Wenn Sie beispielsweise Objektfunktionen für ein Paket einrichten, das Reporting -und Query Studio-Berichte enthält, müssen Sie sicherstellen, dass der Benutzer auch Zugriff auf die gesicherten Funktionen von **Reporting** und **Abfragestudio** und die zugehörigen gesicherten Funktionen hat.

Durch das erneute Publizieren eines vorhandenen Pakets aus einem Clienttool, wie z. B. Framework Manager, werden die zuvor angegebenen Objektfunktionen nicht überschrieben oder geändert.

Steuerungsobjektfunktionen mit der gesicherten **Eingabe-spezifische Funktionen festlegen** -Funktion „Eingabe-spezifische Funktionen festlegen” auf Seite 216.

Sie können die folgenden Objektfunktionen für einzelne Pakete „Objektfunktionen für ein Paket einrichten” auf Seite 221einrichten.

Adaptive Analyse

Diese geschützte Funktion steuert den Zugriff auf die Berichte, die mithilfe von Adaptive Analytics gepackt werden.

Verwaltung

Diese geschützte Funktion steuert den Zugriff auf die Verwaltungsseiten in der IBM Cognos -Software. Sie können Objektfunktionen für die folgenden gesicherten Features in **Verwaltung**angeben.

- **Adaptive Analytics-Administration**

  Benutzer können auf Adaptive Analytics zugreifen, um Verwaltungstasks auszuführen.
- **Planungsverwaltung**

  Benutzer können auf IBM Cognos Planning Contributor Administration Console und IBM Cognos Planning Analyst zugreifen, um Verwaltungstasks auszuführen.

Ereignisstudio

Diese geschützte Funktion steuert den Zugriff auf Event Studio.

Glossar

Diese geschützte Funktion steuert den Zugriff auf das Business-Glossar von IBM InfoSphere .

Planungsbeitragszahler

Diese geschützte Funktion steuert den Zugriff auf den Planungskontributor IBM Cognos Planning Contributor und den Planungsanalytiker IBM Cognos .

PowerPlay Studio

Diese geschützte Funktion steuert den Zugriff auf PowerPlay Studio.

Abfragestudio

Diese geschützte Funktion steuert den Zugriff auf das Query Studio, mit dem Sie einfache Ad-hoc-Berichte erstellen können.

Die dieser Funktion zugeordnete gesicherte Funktion ist

- **Erstellen**

  Erstellen Sie neue Berichte und verwenden Sie die Option Speichern als Option für neue Berichte und angepasste Ansichten.

- **Erweitert**

  Verwenden Sie erweiterte Authoring-Funktionen, wie z. B. das Erstellen von komplexen Filtern, das Formatieren von Stil und die mehrsprachige Unterstützung.

Berichtsstudio

Diese geschützte Funktion steuert den Zugriff auf die Reporting -Benutzerschnittstelle und auf die zugrunde liegende Berichtsausführungsfunktionalität. Benutzer benötigen Ausführungsberechtigungen für diese geschützte Funktion, um auf die Reporting -Benutzerschnittstelle zugreifen zu können. Traversen oder Leseberechtigungen für diese geschützte Funktion sind unter Umständen erforderlich, um die zugeordneten gesicherten Funktionen zu verwenden, z. B. um Berichte auszuführen, die mit angepasstem SQL oder eingebettetem HTML erstellt wurden.

Zu dieser Funktion gehören die folgenden gesicherten Funktionen:

- **Externe Daten zulassen**

  Benutzer können externe Daten in Berichten verwenden.

- **Platzen**

  Benutzer können Burstberichte erstellen und ausführen.

- **Erstellen/Löschen**

  Benutzer können neue Berichte erstellen, die Option Speichern als Option für neue Berichte und Berichtsansichten verwenden und Modelle ändern.

- **HTML-Elemente im Bericht**

  Benutzer können die Schaltfläche "HTMLItem" und die Hyperlinkelemente der Berichtsspezifikation verwenden, wenn sie Berichte erstellen.

- **Benutzerdefiniertes SQL**

  Benutzer können die SQL-Anweisungen direkt in der Abfragespezifikation bearbeiten und die Abfragespezifikationen ausführen, die die bearbeitete SQL-Anweisungen enthalten.

  Tipp: Einschränkungen für die Benutzer, die diese Funktion verwenden können, werden in Framework Manager nicht umgesetzt. Ein Framework-Manager-Benutzer, der keine **Benutzerdefiniertes SQL** -Rechte in **IBM Cognos Administration** hat, kann beispielsweise weiterhin ein Abfragesubjekt erstellen und manuell erstellte SQL-Abfragen für die Suche einer Datenbank verwenden.

Abstammung

Diese geschützte Funktion steuert den Zugriff auf die Aktion **Abstammung** . Verwenden Sie diese Option, um Informationen zu Daten oder Metadatenelementen aus IBM Cognos Viewer oder aus der Quellenverzeichnisstruktur in Reporting, Query Studio und Analysis Studio anzuzeigen.

Spezifikationsausführung

Diese geschützte Funktion ermöglicht es einer Benutzer-oder Software-Development-Kit-Anwendung, eine integrierte Spezifikation zu verwenden. Die gesicherte Funktion "Specification Execution" wird als Berechtigungsklasse für Analyseadministratorengezählt.

IBM Cognos Analytics -Studios und einige Services verwenden intern integrierte Spezifikationen für die Ausführung von Tasks. Der Service, der die Spezifikation ausführt, testet eine Reihe von Funktionen, um sicherzustellen, dass der Benutzer berechtigt ist, die integrierte Spezifikation zu verwenden. Weitere Informationen finden Sie in der Methode "runSpecification" in der *Entwicklerhandbuch*.

Überwachungsregeln

Diese geschützte Funktion steuert den Zugriff auf die Registerkarte **Regeln** in **Meine Überwachungselemente**. Verwenden Sie diese geschützte Funktion, um Überwachungsregeln zu erstellen und auszuführen.

Objektfunktionen für ein Paket einrichten

Verwenden Sie diese Funktion, um die gesicherten Funktionen und Features anzugeben, die Benutzer, Gruppen oder Rollen mit bestimmten Paketen verwenden können.

Sie können Objektfunktionen auf Paketebene oder, wenn das Paket in einem Ordner gespeichert ist, auf Ordnerebene angeben. Die auf Ordnerebene angegebenen Funktionen gelten nur für Pakete in diesem Ordner und in seinen Unterordnern und nicht für alle anderen Einträge, einschließlich Berichte. Wenn ein Ordner beispielsweise Pakete, Berichte und einen Unterordner enthält, der andere Pakete und Berichte enthält, sind nur die Pakete im Ordner und im Unterordner von den Leistungseinstellungen betroffen.

Die folgenden Funktionen werden global angewendet; sie können nicht nach Ordnerbasis in einem Ordner festgelegt werden:

- CSV-Ausgabe generieren
- PDF-Ausgabe generieren
- XLS-Ausgabe generieren
- XML-Ausgabe generieren

Vorbereitende Schritte

Um Objektfunktionen zu verwenden, müssen die Benutzer

- haben Zugriff auf die gesicherten Funktionen und Features, die dem Paket Kapitel 13, „Funktionen”, auf Seite 207 zugeordnet sind.
- Zugriff auf die geschützte **Objektfunktionalität** -Funktion „Eingabe-spezifische Funktionen festlegen” auf Seite 216
- Sie haben die Richtlinienberechtigungen für das Paket Kapitel 12, „Zugriffsberechtigungen und Berechtigungsnachweise”, auf Seite 193 oder das Paket für das Paket festgelegt.

Wenn Sie nach der Installation der IBM Cognos -Software zum ersten Mal Objektfunktionen einrichten, empfehlen wir Ihnen, mit **Öffentliche Ordner**zu beginnen und die Funktionen für **Öffentliche Ordner** zu spiegeln, die die globalen Funktionen widerspiegeln. Dadurch wird eine genaue Referenzversion bereitgestellt, auf der die Objektfunktionen weiter verfeinert werden können.

Vorgehensweise

1. Öffnen Sie die Seite "Paket" oder "Ordner".

   Tipp: Wenn Sie Objektfunktionen für **Öffentliche Ordner**einrichten, klicken Sie auf die Schaltfläche 'Eigenschaften'  in der Produktsymbolleiste. **Öffentliche Ordner** werden in Cognos Analytics Version 11.0.x durch **Teaminhalt** ersetzt.
2. Klicken Sie auf die Registerkarte **Funktionen** .
3. Wählen Sie das Markierungsfeld **Über den übergeordneten Eintrag erworbene Funktionen außer Kraft setzen** aus.

4. Wählen Sie in der Liste **Name** und **Funktionen** das Kontrollkästchen neben dem Benutzer, der Gruppe oder dem Aufgabenbereich aus, für den Sie Objektfunktionen angeben möchten.

   Wenn der Benutzer, die Gruppe oder die Rolle nicht in der Liste enthalten ist, klicken Sie auf **Hinzufügen**. Wenn Sie den Benutzer, die Gruppe oder die Rolle aus der Liste entfernen möchten, wählen Sie das entsprechende Kontrollkästchen aus, und klicken Sie auf **Entfernen**.

   Weitere Informationen zum Hinzufügen oder Entfernen von Einträgen aus dieser Liste finden Sie in den Schritten in „Zugriffsberechtigungen für einen Eintrag festlegen" auf Seite 200.
5. Wählen Sie in der Liste **Erteilen** und **Verweigern** die zutreffenden Markierungsfelder aus, um die erforderlichen Objektfunktionen für Benutzer, Gruppen oder Rollen zu erteilen oder zu verweigern.

   Ein Symbol, das eine erteilte oder verweigerte Funktion darstellt, wird neben dem Namen des Benutzers, der Gruppe oder der Rolle angezeigt. Wenn Sie den Zugriff auf eine geschützte Funktion verweigern, verweigern Sie automatisch den Zugriff auf alle seine gesicherten Funktionen.
6. Falls zutreffend, wählen Sie das Kontrollkästchen **Die Funktionalität aller untergeordneten Einträge löschen** aus.

   Verwenden Sie diese Option, um Objektfunktionen für eine Hierarchie von Einträgen anzugeben, z. B. für alle Pakete in einem Ordner.
7. Klicken Sie auf **OK**.

Kapitel 15. Anfangssicherheit

Wenn ein Content-Store initialisiert wird, wird eine Gruppe von Sicherheitsobjekten erstellt und im Namespace von Cognos gespeichert. Diese Objekte sind für die Vereinfachung der Verwaltung von IBM Cognos konzipiert.

Die anfänglichen Sicherheitsrichtlinien gewähren allen Benutzern uneingeschränkten Zugriff auf alle Objekte im Content-Store. Der Sicherheitsadministrator muss die Anfangssicherheitseinstellungen ändern, um den Content Store zu sichern. Weitere Informationen finden Sie unter „Sicherheitseinstellungen nach der Installation" auf Seite 238.

Eine Zusammenfassung der Erstzugriffsberechtigungen für die Content Manager-Objekte finden Sie unter Anhang C, „Anfangszugriffsberechtigungen", auf Seite 441.

Integrierte Einträge

Zu den integrierten Einträgen gehören das Benutzerkonto "Anonym", die Gruppen "Alle authentifizierten Benutzer" und "Jeder" sowie die Rollen "Systemadministratoren" und "Tenantadministratoren". Die integrierten Einträge können nicht gelöscht werden. Sie erscheinen sowohl in gesicherten als auch in nicht gesicherten Umgebungen.

Anonym

Dieser Eintrag stellt einen Benutzeraccount dar, der von Mitgliedern der allgemeinen Öffentlichkeit gemeinsam genutzt wird, die auf die IBM Cognos -Software zugreifen können, ohne dass sie zur Authentifizierung aufgefordert werden. Diese Art des Zugriffs ist zum Beispiel bei der Verteilung eines Onlinekatalogs nützlich.

Anonyme Benutzer können nur die Einträge sehen, für die keine Zugriffsberechtigungen festgelegt sind, oder sie werden speziell für dieses Konto oder für die Gruppe "Jeder" festgelegt.

Sie können das Konto des anonymen Benutzers inaktivieren, indem Sie die Konfigurationsparameter im Konfigurationstool ändern.

Alle authentifizierten Benutzer

Diese Gruppe stellt Benutzer dar, die von Authentifizierungsprovidern authentifiziert werden. Die Zugehörigkeit zu dieser Gruppe wird durch das Produkt verwaltet und kann nicht angezeigt oder geändert werden.

Diese Gruppe kann nicht implementiert werden. Weitere Informationen finden Sie unter „Einschließlich Cognos Gruppen und Rollen" auf Seite 306.

Jeder

Diese Gruppe stellt alle authentifizierten Benutzer und das Konto des anonymen Benutzers dar. Die Zugehörigkeit zu dieser Gruppe wird durch das Produkt verwaltet und kann nicht angezeigt oder geändert werden.

Sie können die Gruppe "Jeder" verwenden, um die Standardsicherheit schnell festzulegen. Um beispielsweise einen Bericht zu sichern, erteilen Sie dem Bericht für die Gruppe "Jeder" Lese-, Schreib- oder Ausführungsberechtigungen. Nachdem diese Sicherheit vorhanden ist, können Sie anderen Benutzern, Gruppen oder Rollen den Zugriff auf den Bericht erteilen und die Gruppe "Jeder" aus der Sicherheitsrichtlinie für diesen Bericht entfernen. Dann haben nur Benutzer, Gruppen und Rollen, die Sie angegeben haben, Zugriff auf den Bericht erteilt.

Sie können die Gruppe "Jeder" verwenden, um die Sicherheit während der Implementierung anzuwenden, siehe „Sicherheit und Implementierung" auf Seite 300, aber die Gruppe selbst kann nicht

implementiert werden. Weitere Informationen finden Sie unter „Einschließlich Cognos Gruppen und Rollen“ auf Seite 306.

Systemadministratoren

Dies ist eine besondere Rolle in der IBM Cognos -Software. Mitglieder dieser Rolle gelten als Root-Benutzer oder Superuser. Sie können unabhängig von den Sicherheitsrichtlinien, die für das Objekt festgelegt sind, auf ein beliebiges Objekt im Content-Store zugreifen und diese ändern. Nur Mitglieder der Rolle "Systemadministratoren" können die Zugehörigkeit zu dieser Rolle ändern.

Die Rolle "Systemadministratoren" darf nicht leer sein. Wenn Sie Systemadministratoren nicht verwenden möchten, können Sie eine leere Gruppe im Cognos -Namespace oder in Ihrem Authentifizierungsprovider erstellen und diese Gruppe zur Mitgliedschaft in der Rolle "Systemadministratoren" hinzufügen.

Wenn diese Rolle während der Initialisierung des Content Store erstellt wird, wird die Gruppe "Jeder" in die Mitgliedschaft einbezogen. Dies bedeutet, dass alle Benutzer uneingeschränkten Zugriff auf den Content Store haben. Unmittelbar nach der Installation und Konfiguration von IBM Cognos -Software müssen Sie die Anfangssicherheitseinstellungen für diese Rolle ändern und die Gruppe "Jeder" aus der Mitgliedschaft entfernen. Weitere Informationen finden Sie unter „Sicherheitseinstellungen nach der Installation“ auf Seite 238.

Sie können diese Rolle, einschließlich Cognos Gruppen und Rollen, implementieren. Weitere Informationen finden Sie unter „Einschließlich Cognos Gruppen und Rollen“ auf Seite 306.

Mieteradministratoren

Diese Rolle wird in einer Multi-Tenant- IBM Cognos -Umgebung verwendet. Mitglieder dieser Rolle können mehrere Tenants verwalten.

Wenn diese Rolle während der Initialisierung des Content Store erstellt wird, verfügt sie über keine Mitglieder und Funktionen. Nur Systemadministratoren können Mitglieder hinzufügen und Zugriffsberechtigungen und Funktionen für diese Rolle zuweisen.

Vordefinierte Rollen

Zu den vordefinierten Rollen gehören mehrere IBM Cognos -Rollen. Jede Rolle verfügt über eine bestimmte Gruppe von Zugriffsberechtigungen und kann für die Sicherung unterschiedlicher Komponenten und Funktionen in IBM Cognos -Software verwendet werden. Sie können die vordefinierten Rollen verwenden oder löschen.

Wenn die vordefinierten Rollen während der Initialisierung des Content Store erstellt werden, ist die Gruppe "Jeder" Mitglied der Rolle "Systemadministrator". Einige dieser Rollen sind Konsumenten, Abfragebenutzer, Analysebenutzer und Autoren. Wenn Sie die vordefinierten Rollen verwenden möchten, sollten Sie die ursprüngliche Mitgliedschaft unmittelbar nach der Installation und Konfiguration von IBM Cognos -Software ändern. Weitere Informationen finden Sie unter „Sicherheitseinstellungen nach der Installation“ auf Seite 238.

Es gibt zwei Typen von vordefinierten Cognos-Rollen: Standardrollen und Lizenzrollen.

Standardrollen

In der Tabelle in diesem Abschnitt werden die vordefinierten Standard Cognos -Rollen aufgelistet. Standardrollen verfügen jeweils über spezifische Funktionen, die es Benutzern ermöglichen, verschiedene Tasks in IBM Cognos Analyticsauszuführen.

Referenzen:

- Eine Liste der Standardfunktionen, die jeder Standardrolle zugeordnet sind, finden Sie unter „Anfängliche Zugriffsberechtigungen für Funktionen“ auf Seite 443.
- Informationen zum Ändern der Zugehörigkeit zu Standardrollen finden Sie im Artikel „Systemadministratoren und vordefinierte Rollen sichern“ auf Seite 239.

· Ein anderer Typ von Rolle ist eine Lizenzrolle. Basierend auf Lizenzberechtigungen gibt es vier Lizenznamen: **Analyseadministrator**; **Analyseexplorer**; **Analysebenutzer**; und **Analyseviewer**. Weitere Informationen finden Sie unter „Lizenzrollen" auf Seite 226.

Tabelle 57. Vordefinierte Cognos -Standardrollen

Standardrolle	**Beschreibung**
Analysebenutzer	Die Mitglieder verfügen über dieselben Zugriffsberechtigungen wie die Konsumenten. Sie können auch das IBM Cognos Analysis Studio verwenden.
Verfasser	Mitglieder verfügen über dieselben Zugriffsberechtigungen wie Abfragebenutzer und Analysebenutzer. Sie können Reporting, Query Studio und Analysis Studio verwenden und öffentliche Inhalte, wie z. B. Berichte und Berichtsausgaben, speichern.
Verbraucher	Mitglieder können öffentliche Inhalte, wie z. B. Berichte, lesen und ausführen.
Verzeichnisadministratoren	Mitglieder können den Inhalt von Namensbereichen verwalten. Im Namespace von Cognos verwalten sie Gruppen, Accounts, Kontakte, Verteilerlisten, Datenquellen und Drucker.
Bibliotheksadministratoren	Die Mitglieder können den Inhalt der Registerkarte **Bibliothek** in der IBM Cognos Administration aufrufen, importieren und verwalten.
Mobile Benutzer	Mitglieder können auf IBM Cognos -Inhalte, z. B. Berichte, über IBM Cognos Analytics Mobile Reportszugreifen.
Mobile Administratoren	Mitglieder können IBM Cognos Analytics Mobile Reportsverwalten.
Modellierungsprogramme	Mitglieder können die Modellierungsbenutzeroberfläche verwenden, um Datenmodule zu erstellen und zu verwalten.
Portaladministratoren	Mitglieder können die Cognos -Portlets und andere Portlets verwalten. Dazu gehören das Anpassen von Portlets, das Definieren von Portletdarstellungen und das Festlegen von Zugriffsberechtigungen für Portlets. Portaladministratoren können auch Erweiterungen hochladen, die es Benutzern ermöglichen, zum Beispiel Bilder zu Berichten oder Dashboards hinzuzufügen.
Entwickler von Planungsbeitragsern	Mitglieder können auf den Contributor-Web-Client, den Contributor-Add-in für Microsoft Excel oder Analyst zugreifen.
Administratoren für Planungsberechtigungen	Mitglieder können in der Anwendung auf Contributor Administration Console, Analyst und alle zugeordneten Objekte zugreifen.
Benutzer abfragen	Die Mitglieder verfügen über dieselben Zugriffsberechtigungen wie die Konsumenten. Sie können auch IBM Cognos Query Studio verwenden.

Tabelle 57. Vordefinierte Cognos -Standardrollen (Forts.)	
Standardrolle	**Beschreibung**
Leser	Mitglieder haben Lesezugriff auf IBM Cognos -Software. Sie können in einigen Abschnitten des Content Store navigieren, gespeicherte Berichtsausgaben im Portal anzeigen, Zellen in gespeicherten Berichtsausgaben in Cognos Viewer auswählen und das Kontextmenü von Cognos Viewer verwenden, um Aktionen durchzuführen, z. B. Drillthrough.
Berichtsadministratoren	Mitglieder können den öffentlichen Inhalt verwalten, für den sie vollen Zugriff haben. They can also use IBM Cognos Analytics - Reporting and IBM Cognos Query Studio.
Serveradministratoren	Mitglieder können Server, Disponenten und Jobs verwalten.
Systemadministratoren	Mitglieder können unabhängig von den Sicherheitsrichtlinien, die für das Objekt festgelegt sind, auf jedes Objekt im Content-Store zugreifen und diese ändern. Nur Mitglieder der Rolle "Systemadministratoren" können die Zugehörigkeit zu dieser Rolle ändern.

Lizenzrollen

Um Ihnen die Zuordnung von Funktionen zu Lizenzierungsanforderungen zu erleichtern, stellt Cognos Analytics auch vordefinierte Rollen bereit, die auf Lizenzberechtigungen basieren.

Anmerkung: Eine andere Art von Rolle ist eine Standardrolle. Standardrollen verfügen über spezifische Funktionen, die es Benutzern ermöglichen, verschiedene Tasks auszuführen. Weitere Informationen finden Sie unter „Standardrollen” auf Seite 224.

In der folgenden Tabelle werden die vordefinierten Lizenzrollen aufgelistet.

Tabelle 58. Vordefinierte Lizenzrollen für Cognos	
Lizenzrolle	**Beschreibung**
Analyseadministrator	Mitglieder haben dieselben Zugriffsberechtigungen wie Analytics Explorers. Sie können auch auf IBM Software Development Kit; und Komponenten im Menü **Verwalten** zugreifen, einschließlich IBM Cognos Administration.
Analyseexplorer	Mitglieder verfügen über dieselben Zugriffsberechtigungen wie Analytics-Benutzer. Sie können auch auf Exploration, Planning Analytics for Microsoft Excel, Cognos Framework Manager, Cognos Cube Designer und Dynamic Query Analyzer, Jupyter Notebook und Transformer zugreifen.
Analysebenutzer	Mitglieder können neue Berichte, Dashboards, Erkundungen, Storys, neue Jobs, Daten-Server-/Quellenverbindungen oder Datenmodule erstellen. Sie können Berichte ausführen, auf Eingabeaufforderungen reagieren und Dateien hochladen. Sie können auch auf Cognos for Microsoft Office, Cognos Workspace, Cognos Event Studio, Cognos Query Studio und Cognos Analysis Studio zugreifen.

Tabelle 58. Vordefinierte Lizenzrollen für Cognos (Forts.)	
Lizenzrolle	**Beschreibung**
Analyseviewer	Mitglieder können öffentliche Inhalte lesen. Sie können z. B. Berichte abonnieren und Dashboards und Storys anzeigen. Mitglieder können jedoch keine öffentlichen Inhalte ausführen. Daher können sie keine Berichte planen.

Standardberechtigungen auf der Basis von Lizenzen

In IBM Cognos Analyticswird der Lizenzzähler in **Verwalten** > **Lizenzen** von den Funktionen gesteuert, die einem Benutzer, einer Gruppe oder einer Rolle erteilt werden.

Anmerkung: Wenn Sie Änderungen an den Standardberechtigungen vornehmen, kann ein Benutzer bis zu einer anderen Lizenz als der, den sie standardmäßig erteilt haben, wechseln.

Informationen dazu, wie Benutzer auf der Basis ihrer Lizenzberechtigungen eingeschränkt werden können, finden Sie unter „Funktionalität basierend auf Lizenzrollen zuordnen" auf Seite 234.

In der folgenden Tabelle werden die Funktionen zugeordnet, die für jede Lizenz erteilt werden. Funktionen werden in gesicherte Features unterteilt. Ein Häkchen (✓) gibt an, dass eine Berechtigung für ein bestimmtes gesichertes Feature erteilt wird. Funktionen, die als "Nicht zutreffend" -Lizenzen als Lizenz für Viewer-Lizenzen markiert sind.

Tabelle 59. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen

Funktion	Gesicherte Funktion	Analyseviewer	Analysebenutzer	Analyseexplorer	Analyseadministrator	Kommentare
Adaptive Analyse		✓	✓	✓	✓	Nicht zutreffend
Verwaltung			✓	✓	✓	
	Adaptive Analytics-Administration				✓	Nicht zutreffend
	Verwaltungstasks				✓	
	Collaboration-Verwaltung				✓	
	System konfigurieren und verwalten				✓	
	Controllerverwaltung				✓	Sie benötigen eine separate IBM Controller-Lizenz.

Tabelle 59. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)

Funktion	Gesicherte Funktion	Analyseviewer	Analysebenutzer	Analyseexplorer	Analyseadministrator	Kommentare
	Datenquellenverbindungen		✓	✓	✓	
	Verteilerlisten und Kontakte				✓	
	Visualisierungen verwalten				✓	
	Metrische Studio-Verwaltung				✓	Sie benötigen eine separate Metriklizenz
	Mobile Administration				✓	
	Planungsverwaltung				✓	Sie benötigen einen separaten IBM Planning Contributor Licence
	PowerPlay-Server				✓	Sie benötigen eine separate PowerPlay-Lizenz
	Drucker				✓	
	Service 'Query Service'				✓	
	Aktivitäten und Zeitpläne ausführen				✓	
	Funktionalität festlegen und UI-Profile verwalten				✓	
	Stile und Portlets				✓	

Tabelle 59. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)

Funktion	Gesicherte Funktion	Analyseviewer	Analysebenutzer	Analyseexplorer	Analyseadministrator	Kommentare
	Benutzer, Gruppen und Rollen				✓	
AI			✓	✓	✓	
	Lernen	✓	✓	✓	✓	
	Assistent verwenden		✓	✓	✓	
Analysestudio			✓	✓	✓	
11.1.7 -Ausgaben anhängen			✓	✓	✓	
Cognos Analytics for Mobile		✓	✓	✓	✓	
Cognos Insight			✓	✓	✓	Nicht zutreffend
Cognos-Viewer		✓	✓	✓	✓	
	Kontextmenü	✓	✓	✓	✓	
	Mit Optionen ausführen		✓	✓	✓	
	Auswahl	✓	✓	✓	✓	
	Symbolleiste	✓	✓	✓	✓	
Zusammenarbeiten		✓	✓	✓	✓	Sie benötigen eine separate Berechtigung von IBM Connections
	Collaboration-Funktionen zulassen	✓	✓	✓	✓	Sie benötigen eine separate Berechtigung von IBM Connections

Tabelle 59. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)

Funktion	Gesicherte Funktion	Analyseviewer	Analysebenutzer	Analyseexplorer	Analyseadministrator	Kommentare
	Collaboration-Tools starten	✓	✓	✓	✓	Sie benötigen eine separate Berechtigung von IBM Connections
Controller Studio			✓	✓	✓	Sie benötigen eine separate IBM Controller-Lizenz.
Dashboard		✓	✓	✓	✓	
	Erstellen/ Bearbeiten		✓	✓	✓	
Datenmanager		✓	✓	✓	✓	Nicht zutreffend
Datensätze			✓	✓	✓	
Desktop-Tools				✓	✓	
Detaillierte Fehler		✓	✓	✓	✓	
Visualisierungen entwickeln			✓	✓	✓	
Drillthrough-Assistent			✓	✓	✓	
11.1.7 E-Mail		✓	✓	✓	✓	
	Optionen für E-Mail		✓	✓	✓	
	Link in E-Mail einschließen	✓	✓	✓	✓	
	Mit E-Mail teilen	✓	✓	✓	✓	
	Typ in externer E-Mail	✓	✓	✓	✓	
Ereignisstudio			✓	✓	✓	

Tabelle 59. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)

Funktion	Gesicherte Funktion	Analyseviewer	Analysebenutzer	Analyseexplorer	Analyseadministrator	Kommentare
Indexierte Suche ausführen		✓	✓	✓	✓	
Executive-Dashboard			✓	✓	✓	
	Erweiterte Dashboard-Funktionen verwenden		✓	✓	✓	
	Interaktive Dashboard-Features verwenden		✓	✓	✓	
Exploration			✓	✓	✓	
Externe Repositorys		✓	✓	✓	✓	
	Repository-Verbindungen verwalten		✓	✓	✓	
	Externe Dokumente anzeigen	✓	✓	✓	✓	
CSV-Ausgabe generieren			✓	✓	✓	
PDF-Ausgabe generieren			✓	✓	✓	
XLS-Ausgabe generieren			✓	✓	✓	
XML-Ausgabe generieren			✓	✓	✓	
Glossar		✓	✓	✓	✓	Integration in IBM InfoSphere Business Glossary. Kann direkt über Viewer verwendet werden

Tabelle 59. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)

Funktion	Gesicherte Funktion	Analyseviewer	Analysebenutzer	Analyseexplorer	Analyseadministrator	Kommentare
Einträge ausblenden		✓	✓	✓	✓	
Relationale Metadaten importieren				✓	✓	
Job			✓	✓	✓	
Abstammung		✓	✓	✓	✓	
Inhalt verwalten					✓	
Eigene Datenquellensignonen verwalten			✓	✓	✓	
Metrikstudio			✓	✓	✓	Sie benötigen eine separate Metriklizenz
	Ansicht bearbeiten		✓	✓	✓	Sie benötigen eine separate Metriklizenz
Mobil		✓	✓	✓	✓	
Notizbuch				✓	✓	IBM Cognos Analytics for Jupyter Notebook Server muss installiert sein, damit die Notebook-Funktionen verfügbar sind.
Planungsbeitragszahler		✓	✓	✓	✓	Sie benötigen eine separate Berechtigung von IBM Planning Contributor

Tabelle 59. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)

Funktion	Gesicherte Funktion	Analyseviewer	Analysebenutzer	Analyseexplorer	Analyseadministrator	Kommentare
PowerPlay Studio			✓	✓	✓	Sie benötigen eine separate PowerPlay-Lizenz
Abfragestudio			✓	✓	✓	
	Erweitert		✓	✓	✓	
	Erstellen		✓	✓	✓	
Berichtsstudio			✓	✓	✓	
	Externe Daten zulassen		✓	✓	✓	
	Platzen		✓	✓	✓	
	Erstellen/ Löschen		✓	✓	✓	
	HTML-Elemente im Bericht		✓	✓	✓	
	Benutzerdefiniertes SQL		✓	✓	✓	
In Cloud speichern			✓	✓	✓	
	Verbindungen verwalten				✓	
Planung			✓	✓	✓	
	Plantage nach Tag		✓	✓	✓	
	Zeitplan nach Stunde		✓	✓	✓	
	Zeitplan für Minute		✓	✓	✓	
	Zeitplan nach Monat		✓	✓	✓	
	Zeitplan nach Auslöser		✓	✓	✓	

Tabelle 59. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)						
Funktion	**Gesicherte Funktion**	**Analyseviewer**	**Analysebenutzer**	**Analyseexplorer**	**Analyseadministrator**	**Kommentare**
	Zeitplan für Woche		✓	✓	✓	
	Zeitplan für Jahr		✓	✓	✓	
	Nach Priorität planen		✓	✓	✓	
Self-Service-Paketassistent				✓	✓	
Eingabe-spezifische Funktionen festlegen			✓	✓	✓	
Share Pin Board			✓	✓	✓	
Momentaufnahmen			✓	✓	✓	
Spezifikationsausführung					✓	
Dateien hochladen			✓	✓	✓	
Visualisierungsalerts			✓	✓	✓	
Überwachungsregeln			✓	✓	✓	
Webbasierte Modellierung			✓	✓	✓	

Funktionalität basierend auf Lizenzrollen zuordnen

Sie können Funktionen basierend auf Lizenzrollenberechtigungen zuordnen. Auf diese Weise können Sie Benutzer darauf beschränken, nur die Funktionen auszuführen, auf die sie Anspruch haben.

Sie müssen die Tasks in dieser Reihenfolge ausführen:

1. ☐ Ordnen Sie sich der Rolle "Systemadministratoren" zu.
2. ☐ Zugriff auf Mitglieder des Cognos-Namespace beschränken
3. ☐ Entfernen der Gruppe "Jeder" aus der Rolle "Systemadministratoren"
4. ☐ Benutzer ihren vordefinierten Rollen zuordnen
5. ☐ Funktionen zur Analyse von Analysefunktionen entfernen, um die Lizenzvoraussetzungen
6. ☐ Dashboard-Funktionen für bestimmte Rollen und Benutzer erteilen (nur 11.1.4)

Informationen zu Nutzungseinschränkungen finden Sie in der Veröffentlichung Lizenzinformationsdokumente (http://www-03.ibm.com/software/sla/sladb.nsf/searchlis/?searchview & searchorder=4 & searchmax=0 & query = (IBM + Cognos + Analytics + 11.1) für Ihr Programm.

1. Ordnen Sie sich der Systemadministratorrolle zu.:

Als Administrator müssen Sie zunächst sicherstellen, dass Ihre persönliche Benutzer-ID und alle zutreffenden Verwaltungsgruppen Mitglieder der Rolle "Systemadministratoren" sind.

Erst nachdem Sie diese Task ausgeführt haben, können Sie Gruppe "Jeder" aus der Rolle "Systemadministratoren" entfernen.

Verfahren

1. Melden Sie sich mit der Benutzer-ID und dem Kennwort des Administrators bei Cognos Analytics an.
2. Klicken Sie auf **Verwalten** > **Personen** > **Konten**.
3. Wählen Sie den **Cognos** -Namespace aus.
4. Klicken Sie auf das Symbol 'Mehr'  neben der Rolle **Systemadministratoren** und klicken Sie dann auf **Mitglieder anzeigen**.
5. Klicken Sie auf **Auswählen**.
6. Fügen Sie Ihre persönliche Benutzer-ID und alle zutreffenden Verwaltungsgruppen zur Rolle **Systemadministratoren** hinzu.

2. Zugriff auf Mitglieder des Cognos-Namespace zurücknehmen:

Sie oder das Installationsprogramm können den Zugriff auf Cognos Analytics so konfigurieren, dass nur Benutzer, die Mitglieder einer Gruppe oder einer Rolle im Namespace von **Cognos** sind, auf die Anwendung zugreifen können.

Verfahren

1. Starten Sie IBM Cognos Configuration auf jedem Content Manager-Computer.
2. Klicken Sie im **Explorer** -Fenster unter **Sicherheit**auf **Authentifizierung**.
3. Ändern Sie im Fenster **Eigenschaften** den Wert von **Zugriff auf Mitglieder des integrierten Namespace beschränken** in **Wahr**.
4. Klicken Sie im Menü **Datei** auf **Speichern**.

3. Die Gruppe "Jeder" aus der Rolle "Systemadministratoren" entfernen:

Wichtig: Stellen Sie sicher, dass Sie Ihre Benutzer-ID der Rolle **Systemadministratoren** zugeordnet haben, bevor Sie die Gruppe "Jeder" aus der Rolle "Systemadministratoren" entfernen. Andernfalls wird diese Rolle gesperrt, und niemand kann weitere administrative Änderungen vornehmen.

Bei der Gruppe **Jeder** handelt es sich um eine Cognos-Gruppe, die jede Benutzer-ID im Cognos-Namespace enthält. Nach der Installation wird die Gruppe "Jeder" standardmäßig der Rolle "Systemadministratoren" zugeordnet. Diese Erstkonfiguration gibt jedem Benutzer, auch solchen, die nicht als Administratoren gedacht sind, uneingeschränkten Zugriff auf alle Funktionen.

Zweck

Diese Task entfernt von allen Benutzern alle Funktionen, die sie ursprünglich von einer Standardinstallation zugeordnet wurden. Nach der Ausführung dieser Task wird der nächste Schritt in Benutzer und Gruppen ihren vordefinierten Rollen zuordnensein. Die Benutzer haben dann nur Zugriff auf die Funktionen, die sie für ihre eigene Rolle benötigen.

Verfahren

1. Melden Sie sich mit Ihrer persönlichen Benutzer-ID an, die Sie zuvor der Rolle "Systemadministratoren" zugeordnet haben.
2. Klicken Sie auf **Verwalten** > **Personen** > **Konten**.
3. Wählen Sie den **Cognos** -Namespace aus.

4. Klicken Sie auf das Symbol 'Mehr'  neben der Rolle **Systemadministratoren** und klicken Sie dann auf  **Mitglieder anzeigen**.
5. Klicken Sie auf das Symbol 'Member entfernen'  neben der Gruppe ' **Jeder** ' und klicken Sie dann auf **OK**.

4. Zuweisen von Benutzern zu ihren vordefinierten Rollen:

Sie können nun Benutzern und Gruppen ihre vordefinierten Rollen zuordnen. Diese Rollen sind wie folgt:

· **Analyse-Explorers**

· **Analysebenutzer**

· **Analyseanzeigefunktionen**

Informationen zu dieser Task

Durch die Zuordnung der einzelnen Benutzer zu ihrer vordefinierten Rolle gewähren Sie ihnen effektiv die Funktionen, die ihrer Rolle zugeordnet sind. Eine Matrix der Standardfunktionen, die für jede vordefinierte Rolle verfügbar sind, finden Sie unter „Standardberechtigungen auf der Basis von Lizenzen” auf Seite 227.

Verfahren

1. Melden Sie sich als Systemadministrator an.
2. Klicken Sie auf **Verwalten** > **Personen** > **Konten**.
3. Wählen Sie den **Cognos** -Namespace aus.
4. Klicken Sie auf das Symbol 'Mehr'  neben der Rolle **Analyse-Explorers** und klicken Sie dann auf  **Mitglieder anzeigen**.
5. Klicken Sie auf **Auswählen**.
6. Fügen Sie die zutreffenden Benutzer und Gruppen als Mitglieder der Rolle **Analyse-Explorers** hinzu.
7. Wiederholen Sie die Schritte **4-6** für diese Rollen:
   · **Analysebenutzer**
   · **Analyseviewer**

5. Analyse-Viewer-Funktionen entfernen, um die Lizenzvoraussetzungen zu erfüllen:

Informationen zu dieser Task

Bestimmte Funktionen zählen zu einer Analytics-Benutzer-Lizenz, die nicht für die Lizenznehmer von Analytics Viewer bestimmt sind. Standardmäßig werden diese Funktionen jedoch der Gruppe **Jeder** gewährt. In dieser Aufgabe beschränken Sie die Liste der Benutzer, die diese Funktionen erteilt haben, nur für die Benutzer, die entsprechend lizenziert sind. Der Nettoeffekt ist, dass die Funktionen von den Lizenznehmern von Analytics Viewer entfernt werden und sich entsprechend ihren Lizenzberechtigungen bewegen.

Diese Aufgabe besteht aus zwei Teilen:

1. Fügen Sie für jede dieser Funktionen bestimmte Rollen hinzu:
   · **CSV-Ausgabe generieren**
   · **PDF-Ausgabe generieren**
   · **XLS-Ausgabe generieren**
   · **XML-Ausgabe generieren**
   · **Datensätze**
2. Entfernen Sie die Gruppe "Jeder" aus den oben aufgeführten Funktionen. Als Ergebnis behalten nur die Rollen, die in Teil 1 hinzugefügt wurden, die Funktionen.

Verfahren

1. Melden Sie sich als Systemadministrator an.
2. Klicken Sie auf **Verwalten** > **Personen** > **Funktionen**.
3. Klicken Sie auf das Symbol Weitere  neben der Funktion **CSV-Ausgabe generieren** , und klicken Sie dann auf **Zugriff anpassen**.
4. Klicken Sie auf das Symbol 'Mitglied hinzufügen'  .
5. Klicken Sie auf den **Cognos** -Namespace.
6. Drücken Sie die Steuertaste (Strg), um die Mehrfachauswahl **Analysebenutzer**, **Analyse-Explorers**, **Verfasser**, **Modellierungsprogramme**und **Berichtsadministratoren**zu aktivieren.
7. Klicken Sie auf **Hinzufügen** und anschließend auf **Schließen**.
8. Wählen Sie in der Spalte **Berechtigungen** für jede von Ihnen hinzugefügte Rolle **Zugriff**aus.
9. Klicken Sie auf das Symbol 'Member entfernen'  neben der Gruppe **Jeder** und klicken Sie dann auf **OK**.
10. Wiederholen Sie die Schritte **3**-**9** für die verbleibenden Funktionen:
    - **PDF-Ausgabe generieren**
    - **XLS-Ausgabe generieren**
    - **XML-Ausgabe generieren**
    - **Datensätze**
11. Blättern Sie zur Funktion **Externe Repositorys** .
    a. Klicken Sie auf das Symbol Weitere  .
    b. Klicken Sie auf **Zugriff anpassen**.
    c. Klicken Sie auf das Symbol 'Member entfernen'  neben der Gruppe ' **Jeder** '.
    d. Klicken Sie auf **OK**.
12. Blättern Sie zur Funktion **Momentaufnahmen** .
    a. Klicken Sie auf das Symbol Weitere  .
    b. Klicken Sie auf **Zugriff anpassen**.
    c. Klicken Sie auf das Symbol 'Member entfernen'  neben der Gruppe ' **Jeder** '.
    d. Klicken Sie auf **OK**.

6. Dashboardfunktionen für bestimmte Rollen und Benutzer erteilen (nur 11.1.4):

11.1.4 Nur in Cognos Analytics 11.1.4 müssen Sie die Funktionalität von **Dashboard** und die gesicherte Funktion von **Dashboard** > **Erstellen/Bearbeiten** anpassen.

Verfahren

1. Melden Sie sich als Systemadministrator an.
2. Klicken Sie auf **Verwalten** > **Personen** > **Funktionen**.
3. Blättern Sie zur Funktion **Dashboard** .
    a. Klicken Sie auf das Symbol Weitere  .
    b. Klicken Sie auf **Zugriff anpassen**.
    c. Klicken Sie auf das Symbol 'Mitglied hinzufügen'  .
    d. Klicken Sie auf den **Cognos** -Namespace.
    e. Wählen Sie **Analyseviewer**aus.
    f. Klicken Sie auf **Hinzufügen** und anschließend auf **Schließen**.
    g. Wählen Sie in der Spalte **Berechtigungen** für **Analyseviewer**die Option **Zugriff**aus.

4. Erweitern Sie die Funktion **Dashboard** und klicken Sie anschließend auf das Symbol Weitere  neben **Erstellen/Bearbeiten**.
   a. Klicken Sie auf **Zugriff anpassen**.
   b. Klicken Sie auf das Symbol 'Member entfernen'  neben der Rolle **Analyseviewer** .
   c. Klicken Sie auf das Symbol 'Mitglied hinzufügen'  .
   d. Navigieren Sie zu Ihrem Namespace, wählen Sie die entsprechenden Gruppen oder Benutzer aus, und klicken Sie dann auf **Hinzufügen**.
   e. Klicken Sie auf das Symbol 'Mitglied hinzufügen'  .
   f. Navigieren Sie zum Namespace von **Cognos** .
   g. Drücken Sie die Steuertaste (Strg), um die Mehrfachauswahl **Analysebenutzer**, **Analyse-Explorers**, **Verfasser**, **Modellierungsprogramme**und **Berichtsadministratoren**zu aktivieren.
   h. Klicken Sie auf **Hinzufügen** und anschließend auf **Schließen**.
   i. Wählen Sie in der Spalte **Berechtigungen** für jeden Benutzer, jede Gruppe und jede Rolle, die Sie hinzugefügt haben, **Zugriff**aus.

Upgrade-Szenario: Haben Ihre angepassten Rollen dieselben Namen wie die neueren Cognos-Lizenzrollen

Wenn Sie zuvor Rollen mit denselben Namen erstellt haben wie die neueren Cognos-Lizenzrollen und Sie ein Upgrade planen, sollten Sie sich überlegen, welche Funktionen Sie nach dem Upgrade auf die Rollen anwenden möchten.

Weitere Informationen finden Sie unter „Lizenzrollen” auf Seite 226 .

- Wenn Sie weiterhin Funktionen verwenden möchten, die Sie zuvor diesen Rollen zugeordnet haben, können Sie das Upgrade durchführen, ohne diese Funktionen zu verlieren.
- However, if you want to adopt the capabilities of the new license roles, you must first delete or rename your existing roles **vor dem Upgrade**.

Sicherheitseinstellungen nach der Installation

Ihre IBM Cognos -Softwareinstallation muss bereits für die Verwendung eines Authentifizierungsproviders konfiguriert sein, der im IBM Cognos Analytics Installations-und Konfigurationshandbuch dokumentiert ist.

Wenn die vordefinierten Rollen während der Initialisierung des Content Store erstellt werden, ist die Gruppe **Jeder** ein Mitglied der Rolle **Systemadministratoren** . Dies bedeutet, dass alle Benutzer vollen Zugriff auf den Content Store haben. Um diesen Zugriff zu begrenzen, müssen Sie vertrauenswürdige Benutzer als Mitglieder dieser Rolle hinzufügen und anschließend die Gruppe "Jeder" aus der Mitgliedschaft entfernen.

Außerdem müssen Sie die Zugehörigkeit zu den vordefinierten Rollen ändern, die die Gruppe **Jeder**enthalten, z. B. **Verbraucher**, **Benutzer abfragen**und **Verfasser**. Nehmen Sie ähnliche Änderungen wie für die Rolle **Systemadministratoren** für sie vor. Diese Änderungen sollten auch die Lizenzbedingungen berücksichtigen.

Wenn Sie die vordefinierten Rollen nicht verwenden möchten, können Sie sie löschen.

Um den Namespace von **Cognos** zu sichern, ändern Sie die ursprünglichen Zugriffsberechtigungen, indem Sie den erforderlichen Benutzern den Zugriff erteilen.

Wenn Sie Zugriffsberechtigungen festlegen, sollten Sie den Zugriff auf Einträge für die Gruppe "Everyone" nicht explizit verweigern. Wenn Sie den Zugriff verweigern, werden alle anderen Sicherheitsrichtlinien für den Eintrag außer Kraft gesetzt. Wenn Sie den Zugriff auf den Eintrag für "Jeder" verweigert haben, wird der Eintrag unbrauchbar.

Um eine sichere Installation zu gewährleisten, sollten Benutzer nur die Berechtigungen und Funktionen erhalten, die erforderlich sind, damit sie ihre zugewiesenen Aufgaben ausführen können. Beispiel: **Leser** wäre normalerweise auf Lese-und Transitberechtigungen für **Öffentliche Ordner** beschränkt und darf keine Berichte erstellen, die ein Studio verwenden. Die Verbraucher würden in der Regel auf Lese-, Traversen-und Ausführungsberechtigungen beschränkt.

Bestimmte Funktionen, wie z. B. **HTML-Element im Bericht** und **Benutzerdefiniertes SQL** , sollten fest verwaltet werden. Diese Funktionen werden sowohl während des Authoring-Prozesses als auch beim Ausführen von Berichten überprüft. Wenn ein Konsument einen Bericht ausführen muss, der diese Funktionen erfordert, können Sie möglicherweise die **Als Eigner ausführen** -Funktion verwenden, um die Anzahl der Systembenutzer zu begrenzen, für die diese Funktionen erforderlich sind. Das Feature **Als Eigner ausführen** verwendet die Berechtigungsnachweise des Berichtsinhabers, um Funktionsprüfungen durchzuführen und auf Daten zuzugreifen.

Informationen zum Erteilen von Funktionen für Pakete finden Sie unter Objektfunktionalität.

Systemadministratoren und vordefinierte Rollen sichern

Ändern Sie als einer der ersten Schritte bei der Konfiguration der Sicherheit für die IBM Cognos -Umgebung die Anfangsmitgliedschaft der Rolle "Systemadministratoren" und andere vordefinierte Rollen.

Wenn die Gruppe **Jeder** Mitglied einer vordefinierten Rolle ist, entfernen Sie die Gruppe aus der Rollenzugehörigkeit.

Vorgehensweise

1. Öffnen Sie **IBM Cognos Administration**von **Verwalten** > **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Sicherheit** auf **Benutzer, Gruppen und Rollen**.
3. Klicken Sie auf den **Cognos** -Namespace.
4. Klicken Sie für die Rolle, die Sie ändern möchten, in der Spalte **Aktionen** auf die Schaltfläche Eigenschaften festlegen.
5. Ändern Sie auf der Registerkarte **Mitglieder** die Rollenzugehörigkeit:
   - Stellen Sie sicher, dass ein oder mehrere Benutzer, die in Ihrem Authentifizierungsprovider definiert sind, Mitglieder sind
   - Entfernen Sie die Gruppe **Jeder** , wenn diese Gruppe Mitglied der Rolle ist.
   - Klicken Sie auf **OK**.
6. Legen Sie auf der Registerkarte **Berechtigungen** Zugriffsberechtigungen für diese Rolle fest, um zu verhindern, dass nicht berechtigte Benutzer den Inhalt erstellen, aktualisieren oder löschen, und klicken Sie anschließend auf **OK**.
7. Wiederholen Sie für jede Rolle, die Sie ändern möchten, die Schritte 3 bis 6.

Cognos-Namespace sichern

Sie können den Cognos -Namespace wie folgt einrichten.

Vorgehensweise

1. Öffnen Sie **IBM Cognos Administration**von **Verwalten** > **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Sicherheit** auf **Benutzer, Gruppen und Rollen**.
3. Klicken Sie in der Spalte **Aktionen** neben dem Cognos -Namespace auf die Schaltfläche Eigenschaften festlegen.
4. Legen Sie auf der Registerkarte **Berechtigungen** Zugriffsberechtigungen für den **Cognos** -Namespace fest, um zu verhindern, dass nicht berechtigte Benutzer den Inhalt erstellen, aktualisieren oder löschen.

Es wird empfohlen, die Gruppe "Jeder" zu entfernen. Sie können es jedoch verlassen, je nach Ihren Anforderungen.

5. Wenn Sie möchten, wählen Sie das Markierungsfeld **Zugriffsberechtigungen für alle untergeordneten Einträge löschen** aus.
6. Klicken Sie auf **OK**.

Content-Store sichern

Zur Gewährleistung seiner Sicherheit und Integrität wird der Content-Manager-Service auf den Content-Manager-Service zugreifen, indem er die Single-Datenbank-Anmeldung verwendet, die in IBM Cognos Configuration angegeben ist. Die Datenbankanmeldung wird gemäß Ihren Verschlüsselungsstandards verschlüsselt. Die Content-Store-Sicherheit basiert jedoch nicht nur auf der IBM Cognos Analytics -Sicherheit, sondern auch auf der nativen Datenbanksicherheit, der Betriebssystemsicherheit und der Netzsicherheit.

Führen Sie für die Sicherung Ihrer Datenbank die folgenden Richtlinien aus:

- Sichern Sie die Datenbank und die Datenbank-API mithilfe der Mechanismen, die von der Datenbank, dem Netz und dem Betriebssystem bereitgestellt werden.
- Ordnen Sie eine begrenzte Anzahl von Benutzern zu, um die Datenbank zu verwalten.
- Verwenden Sie die native Sicherheitsfunktion Ihrer Datenbank, um den Benutzerkonten, die auf die Datenbank zugreifen, wie folgt nur die Mindestberechtigungen zu erteilen:
  - Microsoft SQL Server

    Benutzer müssen über die Berechtigung zum Erstellen und Löschen von Tabellenberechtigungen für die Datenbank verfügen. Stellen Sie sicher, dass das Benutzerkonto ein Mitglied der Rollen "db_ddladmin", "db_datareader" und "db_datawriter" und der Eigner des zugehörigen Standardschemas ist.
  - ORACLE

    Benutzer müssen über die Berechtigung zum Herstellen einer Verbindung zur Datenbank verfügen. Darüber hinaus müssen sie in der Lage sein, Tabellen, Trigger, Sichten, Prozeduren und Sequenzen zu erstellen, zu ändern und zu löschen sowie Daten in den Datenbanktabellen einzufügen, zu aktualisieren und zu löschen. Die Berechtigungen müssen dem Benutzeraccount direkt und nicht über eine Gruppe oder eine Rollenzugehörigkeit erteilt werden.
  - IBM Db2

    Benutzer müssen die Berechtigungen "create", "drop table", "CREATETAB", "CONNECT" und "IMPLICITSCHEMA" für die Datenbank haben. Außerdem müssen sie über USE-Berechtigungen für den Tabellenbereich USER TEMPORARY und andere geeignete Tabellenbereiche verfügen, die der Datenbank zugeordnet sind.
  - Sybase Adaptive Server Enterprise

    Benutzer müssen über die Erstellung, die Falltabelle, die Standardeinstellung, die Erstellung von Prozeduren, die Erstellung von Regeln, die Erstellung von Tabellen und die Erstellung von Anzeigeberechtigungen für die Datenbank verfügen.
- Begrenzen Sie die Anzahl der Benutzer, die über Lese-oder Schreibzugriff für die Content Manager-Tabellen verfügen.
- Folgen Sie anderen Empfehlungen zur Sicherung der Datenbank. Weitere Informationen finden Sie in der Datenbankdokumentation.

Kapitel 16. Eingabeeigenschaften

Sie können steuern, wie ein Eintrag angezeigt wird und sich verhält, indem Sie seine Eigenschaften ändern. Die Eigenschaften für Einträge variieren abhängig von der Art des Eintrags und Ihren Berechtigungen. Beispielsweise verfügen Berichte über Eigenschaften zur Steuerung von Ausführungsoptionen, während Ordner nicht ausgeführt werden. Wenn eine Eigenschaft für den Typ des Eintrags, den Sie anpassen, nicht anwendbar ist, wird er nicht auf der **Eigenschaften festlegen** -Seite angezeigt.

Allgemeine Eigenschaften

Allgemeine Eigenschaften werden auf der Registerkarte **Allgemein** der Seite **Eigenschaften festlegen** angezeigt.

In der folgenden Tabelle werden die allgemeinen Eigenschaften beschrieben, die verfügbar sind.

Tabelle 60. Allgemeine Eingabeeigenschaften

Eigenschaft	**Beschreibung**
Typ	Die Art des Eintrags.
Eigner	Der Eigner des Eintrags. Der Eigner ist standardmäßig die Person, die den Eintrag erstellt hat. Wenn der Eigner nicht mehr im Namespace vorhanden ist oder sich aus einem anderen Namespace als der aktuelle Benutzer befindet, wird der Eigner als `Nicht verfügbar`angezeigt. Wenn Sie Richtlinienberechtigungen festgelegt haben, klicken Sie auf **Machen Sie mich zum Eigentümer** , um der Eigner des Eintrags zu werden.
Kontakt	Die Person, die für den Eintrag verantwortlich ist. Klicken Sie auf **Setzen Sie den Kontakt** , und klicken Sie dann auf **Den Kontakt auswählen** , um den Kontakt für den Eintrag festzulegen, oder klicken Sie auf **Geben Sie eine E-Mail-Adresse ein.** , um die E-Mail-Adresse des Kontakts einzugeben.
Position	Die Position des Eintrags in dem Portal und dessen ID. Klicken Sie auf **Suchpfad, ID und URL anzeigen** , um die vollständig qualifizierte Position und die ID des Eintrags im Content-Store anzuzeigen. Den Einträgen wird eine eindeutige Kennung (ID) zugeordnet.
Erstellt	Das Datum, an dem der Eintrag erstellt wurde.
Geändert	Das letzte Datum, an dem der Eintrag geändert wurde.
Symbol	Das Symbol für den Eintrag. Klicken Sie auf **Bearbeiten** , um ein alternatives Symbol anzugeben.
Indexiert	Die Zeitmarke, die angibt, wann der Eintrag zuletzt indexiert wurde. Die Eigenschaft wird nicht angezeigt, wenn der Eintrag nicht indexiert wurde.

Tabelle 60. Allgemeine Eingabeeigenschaften (Forts.)	
Eigenschaft	**Beschreibung**
Diesen Eintrag inaktivieren	Wenn diese Option ausgewählt ist, können Benutzer, die keine Schreibberechtigung für diesen Eintrag haben, nicht auf sie zugreifen. Der Eintrag ist im Portal nicht mehr sichtbar. Wenn ein Eintrag inaktiviert ist und Sie Schreibzugriff auf ihn haben, wird neben dem Eintrag das Symbol für inaktiviert angezeigt.
Diesen Eintrag ausblenden	Wählen Sie diese Eigenschaft aus, um Berichte, Pakete, Seiten, Ordner, Jobs und andere Einträge auszublenden. Blenden Sie einen Eintrag aus, um zu verhindern, dass er nicht mehr verwendet wird, oder um Ihre Ansicht zu organisieren. Der ausgeblendete Eintrag ist noch für andere Einträge zugänglich. Zum Beispiel ist ein verdeckter Bericht als Drillthrough-Ziel zugänglich. Ein verdeckter Eintrag bleibt sichtbar, aber sein Symbol ist ausgeblendet. Wenn Sie das Markierungsfeld **Ausgeblendete Einträge anzeigen** in den Bereichsoptionen  , **Eigene Vorgaben**, löschen, wird der Eintrag aus Ihrer Sicht nicht mehr angezeigt. Sie müssen Zugriff auf die Funktionalität von **Einträge ausblenden** haben, die Ihr Administrator erteilt hat, um diese Eigenschaft anzuzeigen.
Sprache	Eine Liste der Sprachen, die für den Eintragsnamen, die Anzeigenspitze und die Beschreibung verfügbar sind, entsprechend der Konfiguration, die Ihr Administrator eingerichtet hat. Klicken Sie auf **Werte für diese Sprache entfernen** , um den Eintragsnamen, die Anzeigenspitze und die Beschreibung für eine bestimmte Sprache zu entfernen.
Name	Der Name des Eintrags für die ausgewählte Sprache.
Bildschirmspitze	Eine optionale Beschreibung des Eintrags. Der Anzeigentipp wird angezeigt, wenn Sie den Zeiger über das Symbol für den Eintrag im Portal anhalten. Es können bis zu 100 Zeichen für eine Bildschirmspitze verwendet werden.
Beschreibung	Eine optionale Beschreibung des Eintrags. Sie wird im Portal angezeigt, wenn Sie Ihre Vorgaben für die Verwendung der Detailsicht festlegen. Die Detailansicht wird nur in 'Öffentliche Ordner' und 'Eigene Ordner' angezeigt.
Protokoll ausführen	Die Anzahl der Vorkommen oder der Zeitraum, in denen die Ausführungshistorien für den Eintrag aufbewahrt werden sollen.
Berichtsausgabeversionen	Die Anzahl der Vorkommen oder der Zeitraum, in denen die Berichtsausgaben aufbewahrt werden. Wenn Sie diesen Wert auf null (0) setzen, wird eine unbegrenzte Anzahl von Versionen gespeichert.

Tabelle 60. Allgemeine Eingabeeigenschaften (Forts.)	
Eigenschaft	**Beschreibung**
Paket	Das Paket, das dem Eintrag zugeordnet ist. Wenn das Quellenpaket verschoben oder gelöscht wurde, liest der Text `Nicht verfügbar`. Klicken Sie auf **Link zu einem Paket** , um den Eintrag mit einem anderen Paket zu verknüpfen.
URL	Eine URL für eine Datei oder eine Website-Adresse. Dieses Feld ist nur sichtbar, wenn Sie über Leseberechtigungen für den Eintrag verfügen. Wenn Sie über Schreibberechtigungen ohne Leseberechtigungen verfügen, ist diese Eigenschaft nicht sichtbar.
Quellenbericht	Ein Pfad zum Quelleneintrag für eine Berichtsansicht. Wenn der Quelleneintrag verschoben oder gelöscht wurde, liest der Text `Nicht verfügbar`. Klicken Sie auf **Berichtseigenschaften** , um die Eigenschaften des Quellenberichts anzuzeigen. Klicken Sie auf **Link zu einem Bericht** , um den Eintrag mit einem anderen Paket zu verknüpfen.
Quellenagent	Ein Pfad zum Quelleneintrag für eine Agentenansicht. Wenn der Quelleneintrag verschoben oder gelöscht wurde, liest der Text `Nicht verfügbar`. Klicken Sie auf **Agenteneigenschaften** , um die Eigenschaften des Quellenberichts anzuzeigen. Klicken Sie auf **Link zu einem Agenten** , um den Eintrag mit einem anderen Paket zu verknüpfen.
Erweiterte Weiterleitung	Routing-Tags können auf Datenobjekte, wie z. B. Pakete, Datenmodule und hochgeladene Dateien, sowie auf Benutzergruppen und Rollen angewendet werden. Diese Tags werden in Kombination mit Servergruppen verwendet, um Routing-Regeln für Dispatcher anzugeben.
Gateway	Die Position des Web-Servers, auf dem sich das ursprüngliche IBM Cognos -Produkt befindet. Gilt nur für Berichte der Series 7 PowerPlay .

Bericht-, Abfrage-, Analyse-und PowerPlay -Berichtseigenschaften

Die Berichtseigenschaften werden auf den folgenden Registerkarten auf der **Eigenschaften festlegen** -Seite angezeigt:

- Registerkarte **Bericht** für Reporting -Berichte
- Registerkarte **Abfrage** für Query Studio-Berichte
- Registerkarte **Analyse** für Analysis Studio-Berichte
- Registerkarte **PowerPlay-Bericht** für Berichte der Serie 7 PowerPlay

Sie können die verfügbaren Papierformate auswählen. Klicken Sie in **IBM Cognos Administration** auf **Konfiguration** > **Dispatcher und Services**. Klicken Sie auf die Schaltfläche zum Definieren der Papierformate  . Um neue Papierformate hinzuzufügen, klicken Sie auf **Neu**. Um Papierformate zu löschen, klicken Sie auf **Löschen**.

In der folgenden Tabelle werden die verfügbaren Berichtseigenschaften beschrieben.

Tabelle 61. Bericht-, Abfrage-, Analyse-und PowerPlay -Berichtseigenschaften	
Eigenschaft	**Beschreibung**
Standardaktion	Die Standardaktion, wenn der Bericht ausgeführt wird.
Formate	Das Ausgabeformat, das verwendet werden soll, wenn der Bericht ausgeführt wird.
PDF-Optionen	Die Optionen, z. B. Ausrichtung, Papiergröße und Kennwort, um den Bericht zu öffnen, werden bei der Erstellung von PDF-Ausgabe verwendet.
Unterstützung für Eingabehilfen aktivieren	Gibt an, ob Berichtsausgaben erstellt werden sollen, die die behindertengerechte Durch die Aktivierung der Unterstützung wird die Berichtsausgabe erstellt, die von einem Sprachausgabeprogramm gelesen werden kann.
Sprachen	Die Standardsprache, die für die Berichtsdaten verwendet werden soll, wenn der Bericht ausgeführt wird.
Eingabeaufforderungswerte	Wenn das Kontrollkästchen ausgewählt ist, werden Benutzer aufgefordert, Werte zum Filtern von Daten auszuwählen, wenn der Bericht ausgeführt wird.
Aktuelle Werte	Die Werte, die zum Filtern von Daten verwendet werden, wenn ein Bericht ausgeführt wird. Weitere Informationen finden Sie unter „Geben Sie die Standardaufforderungswerte für einen Bericht an.” auf Seite 369.
Protokoll ausführen	Gibt an, wie lange Laufhistorien aufbewahrt werden sollen. Sie können die Laufhistorien für eine bestimmte Anzahl von Ausführungen oder für eine bestimmte Anzahl von Tagen oder Monaten beibehalten.
Berichtsausgabeversionen	Gibt an, wie lange Berichtsausgabehistorien aufbewahrt werden sollen. Sie können die Berichtsausgabe für eine bestimmte Anzahl von Ausführungen oder für eine bestimmte Anzahl von Tagen oder Monaten beibehalten.
Zeilen pro Seite in HTML-Berichten	Die Anzahl der Zeilen, die pro Webseite in HTML-Berichten angezeigt werden sollen.
Als Eigner ausführen	Gibt an, ob bei der Ausführung des Berichts die Berechtigungsnachweise des Eigners verwendet werden sollen. Weitere Informationen finden Sie unter „Vertrauenswürdige Berechtigungsnachweise” auf Seite 202.
Als Eigner ausführen: Nur Funktionen	Gibt an, ob nur die Eignerfunktionen und nicht die Berechtigungsnachweise des Eigners verwendet werden sollen, wenn der Bericht ausgeführt wird.
HTML-Optionen: Öffnen im Entwurfsmodus	Gibt an, ob ein PowerPlay-Bericht der Serie 7 im HTML-Format im Entwurfsmodus geöffnet werden soll.

Jobeigenschaften

Die Jobmerkmale werden auf der Registerkarte **Job** der Seite **Eigenschaften festlegen** angezeigt.

In der folgenden Tabelle werden die verfügbaren Jobmerkmale beschrieben.

Tabelle 62. Jobeigenschaften

Eigenschaft	Beschreibung
Schritte	Eine Liste der Schritte im Job.
Unterbreitung von Schritten	Gibt an, ob Job-Tasks alle gleichzeitig oder nacheinander ausgeführt werden sollen.
Standardwerte für alle Schritte	Legen Sie die Standardwerte auf der Jobebene fest. Klicken Sie auf **Festlegen**und geben Sie anschließend die Standardwerte für alle Schritte des Jobs an. Wenn keine Standardwerte festgelegt sind, werden die Standardwerte für die einzelnen Schritte verwendet.
Details der Verlaufsprotokolldetails	Klicken Sie auf **Alle** , um die vollständigen Verlaufsdetails für die Jobschritte zu speichern, wenn die Ausführungsaktivität erfolgreich abgeschlossen wird. Die vollständigen Verlaufsdetails für die Jobschritte umfassen **Name**, **Anforderungszeit**, **Startzeit**, **Fertigstellungszeit**, **Status**. Klicken Sie auf **Begrenzt** , um die Details der begrenzten Ausführungsprotokoll für den Job zu speichern. Zu den Details der begrenzten Ausführungshistorie gehören die Startzeit des Jobs, die Beendigungszeit, der Status und die Nachrichten. Wenn die Jobausführung fehlschlägt, werden die vollständigen Verlaufsdetails gespeichert. Der Standardwert ist **Alle**. Die Einstellung für die Ausführungsprotokolldetailstufe für den Job überschreibt die Einstellungen für die Jobschritte.

Agenteneigenschaften

Agenteneigenschaften werden auf der Registerkarte **Agent** der Seite **Eigenschaften festlegen** angezeigt.

In der folgenden Tabelle werden die verfügbaren Agenteneigenschaften beschrieben.

Tabelle 63. Agenteneigenschaften

Eigenschaft	Beschreibung
Aufgaben	Eine Liste der Tasks in dem Agenten.
Standardaktion	Die Standardaktion, wenn der Agent ausgeführt wird.
Eingabeaufforderungswerte	Die Werte, die zum Filtern von Daten verwendet werden, wenn ein Agent ausgeführt wird.
Als Eigner ausführen	Gibt an, ob bei der Ausführung des Agenten die Berechtigungsnachweise des Eigners verwendet werden sollen. Weitere Informationen finden Sie im Artikel „Vertrauenswürdige Berechtigungsnachweise” auf Seite 202.

Tabelle 63. Agenteneigenschaften (Forts.)	
Eigenschaft	**Beschreibung**
Als Eigner ausführen: Nur Funktionen	Gibt an, ob nur die Eignerfunktionen und nicht die Berechtigungsnachweise des Eigners verwendet werden sollen, wenn der Bericht ausgeführt wird.
Alertliste	Gibt an, ob Benutzer die Möglichkeit haben, sich der Alertliste für einen Agenten hinzuzufügen.

Regeleigenschaften

Verwenden Sie die Regeleigenschaften, um eine Überwachungsregel zu definieren oder zu ändern. Über die Registerkarte **Meine Überwachungselemente**, **Regeln** können Sie auf die Regeleigenschaften zugreifen, indem Sie auf das Symbol "Eigenschaften festlegen" für einen Überwachungsregeleintrag klicken. Die Eigenschaften befinden sich auf der Registerkarte **Regel** der Seite **Eigenschaften festlegen** .

Die Regeleigenschaften geben Bedingungen in der gespeicherten HTML-Berichtsausgabe an, so dass Sie beim Speichern des Berichts und der Bedingungen, die erfüllt werden, benachrichtigt werden.

In der folgenden Tabelle werden die verfügbaren Regeleigenschaften beschrieben.

Tabelle 64. Regeleigenschaften	
Eigenschaft	**Beschreibung**
Regel inaktivieren	Gibt an, ob die Überwachungsregel inaktiviert werden soll. Wenn diese Option inaktiviert ist, wird die Überwachungsregel nicht angewendet, wenn die Berichtsausgabe generiert wird.
Senden Sie einen Alert, wenn der Bericht *Berichtsname* enthält:	Der Name des Berichts und die Regel, die für die Uhrenregel definiert ist. Um die Definition zu bearbeiten, klicken Sie auf die vorhandene Filterbedingung, z. B. größer als (>), und klicken Sie in der angezeigten Liste auf eine andere Bedingung. Geben Sie einen anderen Wert in der Box an.
Für den ausgewählten Kontext	Die Objekte in dem Bericht, für den die Regel gilt.
Alerttyp	Der Typ des Alerts, den Sie erhalten, wenn die Regel erfüllt ist. Sie können per E-Mail oder News benachrichtigt werden.

Kapitel 17. Zeitpläne und Aktivitäten

Sie können eine Liste der geplanten Aktivitäten der Benutzer anzeigen, die an einem bestimmten Tag aktuell, an der Vergangenheit oder an einem bestimmten Tag angezeigt werden.

Sie können die Liste so filtern, dass nur die Einträge angezeigt werden, die angezeigt werden sollen. Ein Balkendiagramm zeigt Ihnen einen Überblick über die täglichen Aktivitäten nach Stunden. Sie können das Diagramm verwenden, um das optimale Datum für die Neuplanung von Aktivitäten zu wählen. Sie können die Ausführungspriorität für Einträge festlegen. Sie können auch das Ausführungsprotokoll für Einträge anzeigen, angeben, wie lange die Ausführungsprotokolle aufbewahrt werden sollen, und fehlgeschlagene Einträge erneut ausführen.

Sie können sehen, wer jeden Eintrag ausgeführt hat, und je nach Bedarf Aktionen für Einträge ausführen. Sie können z. B. den großen Job eines Benutzers abbrechen oder aussetzen, wenn er wichtige Einträge in der Warteschlange einhält. Sie können die Priorität einer Eintragsinstanz auch überschreiben, oder Sie können sie für einen Eintrag selbst dauerhaft ändern.

Wenn Sie Ansichten wechseln, müssen Sie die aktuellen Daten aktualisieren. Wenn Sie beispielsweise von **Vergangene Aktivitäten** auf **Anstehende Aktivitäten**wechseln, müssen Sie die aktuellen Daten in den Teilfenstern aktualisieren.

Administratoren können die Verwaltungsfunktion von **Verwalten** > **Aktivitäten** verwenden oder **IBM Cognos Administration** , um Aktivitäten für alle Benutzereinträge zu verwalten.

Bericht planen

11.1.7 Sie planen einen Bericht, um ihn zu einem späteren Zeitpunkt oder zu einem wiederkehrenden Datum und zu einem wiederkehrenden Zeitpunkt auszuführen.

Wenn Sie einen Zeitplan nicht mehr benötigen, können Sie ihn löschen. Sie können sie auch inaktivieren, ohne die Planungsdetails zu verlieren. Anschließend können Sie den Zeitplan zu einem späteren Zeitpunkt aktivieren.

Wenn Sie möchten, können Sie den aktuellen Zeitplaneigner ändern, indem Sie die Berechtigungsnachweise für einen geplanten Eintrag ändern. Weitere Informationen finden Sie im Artikel "Eigentumsrecht an einem Zeitplan übernehmen" in der *Benutzerhandbuch verwalten*.

Vorbereitende Schritte

Um diese Funktionalität zu verwenden, müssen Sie über die erforderlichen Berechtigungen für die Funktionalität von **Planung** verfügen. Sie können sehen, welche Funktionen mit der zugeordneten Lizenzrolle im Thema "Standardberechtigungen auf der Basis von Lizenzen" in der *Benutzerhandbuch verwalten*verfügbar sind.

Um einen Bericht zu planen, benötigen Sie außerdem die folgenden Zugriffsberechtigungen für alle Datenquellen, die im Bericht verwendet werden:

- dataSource-Ausführen und Traverse
- dataSourceConnection-Ausführen und Traverse

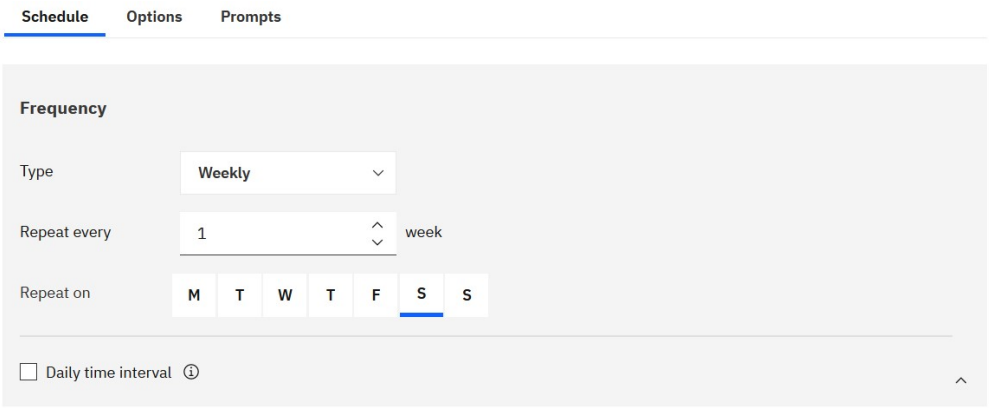
  Wenn Sie nur den Zugriff ausführen, werden Sie aufgefordert, sich bei der Datenbank anzumelden.
- dataSourceSignon-Ausführen

Zum Planen von Berichten, die in den eingeschränkten CVS-, PDF-, XLS-oder XML-Ausgabeformaten ausgeführt werden sollen, benötigen Sie die Generierung der Ausgabefunktion für das bestimmte Format. Weitere Informationen finden Sie im Artikel *Berichtsformate* in der *Verwaltung und Sicherheit*.

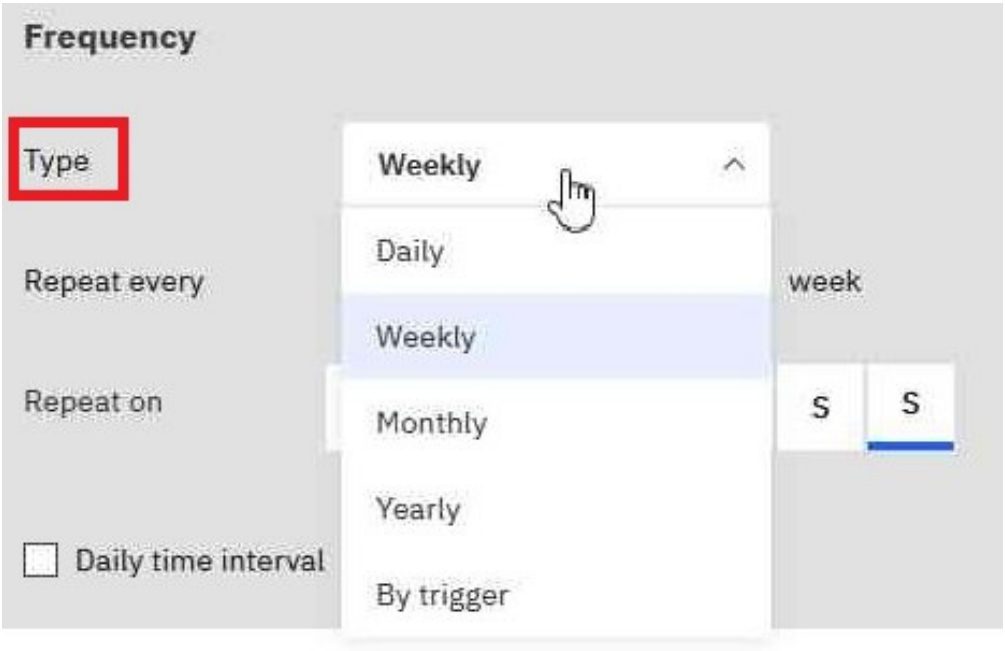
Um die Priorität für einen Eintrag festlegen zu können, müssen Sie über die erforderlichen Berechtigungen für das gesicherte Feature **Terminierungspriorität** verfügen. Weitere Informationen finden Sie unter Funktionen ..

Vorgehensweise

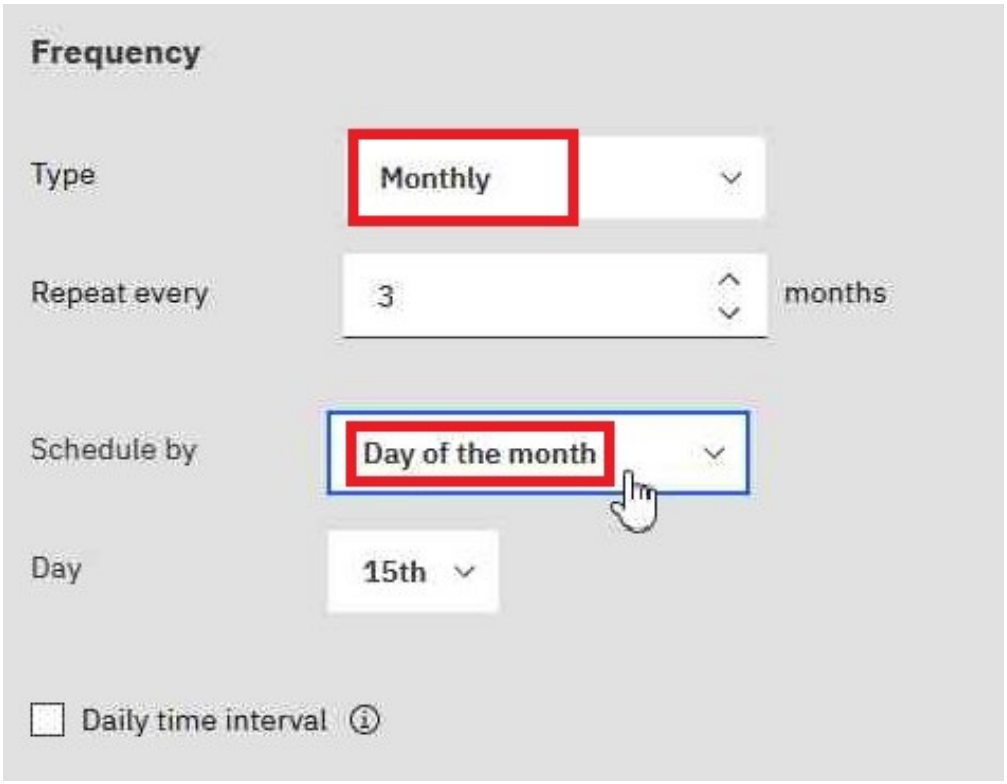
1. Klicken Sie auf das Symbol 'Mehr' ··· , und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie im Teilfenster **Eigenschaften** auf die Registerkarte **Zeitplan** und anschließend:
   · Klicken Sie auf **Zeitplan erstellen**.



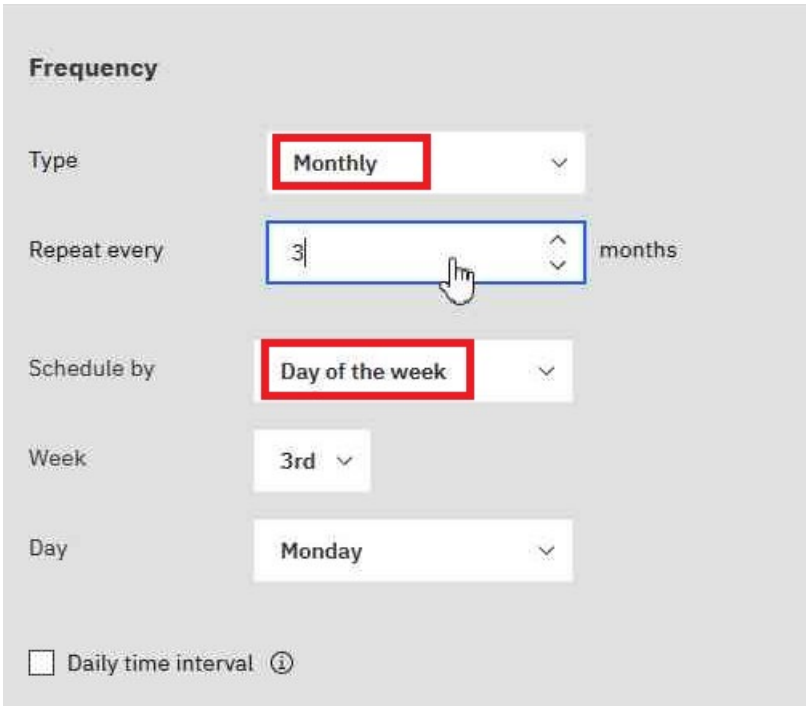
   Tipp: Die verfügbaren Optionen ändern sich bei jeder Auswahl. Warten Sie, bis das Teilfenster aktualisiert wird, bevor Sie weitere Einstellungen auswählen.
3. Geben Sie im Abschnitt **Häufigkeit** an, wann und wie häufig der Bericht ausgeführt wird:
   · Wählen Sie das **Typ** der Zeiteinheit aus, um das Intervall zwischen Besprechungen zu messen.



   Tipp: Versuchen Sie, verschiedene **Typ** -Werte auszuwählen, und beobachten Sie dann, wie sich die anderen Felder ändern. Wenn Sie beispielsweise **Täglich**, **Wöchentlich**oder **Monatlich** auswählen, können Sie eine **Wiederholen Sie alle** *Ganze Zahl*auswählen. Sie können daher ein Intervall auswählen, bei dem es sich um ein Vielfaches der von Ihnen ausgewählten Zeiteinheit handelt, z. B. "alle 3 Wochen".
   · Wenn Sie einen **Typ** -Wert von **Monatlich**auswählen,

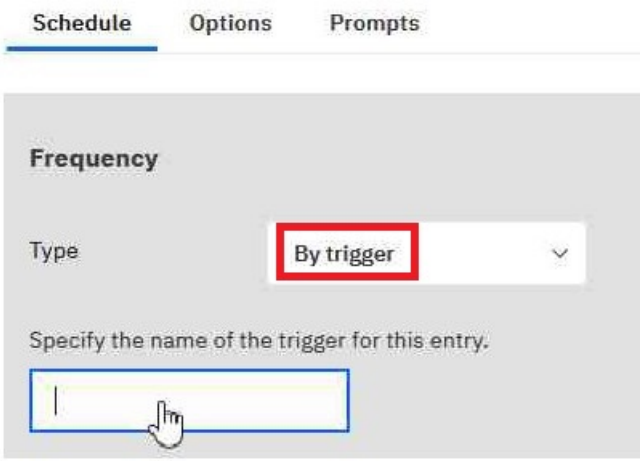


– Wählen Sie **Tag des Monats** im Feld **Planen nach** aus, damit Sie z. B. "Wiederholung alle 3 Monate am 15. des Monats" auswählen können (siehe Abbildung oben).



– Wählen Sie **Tag der Woche** im Feld **Planen nach** aus, damit Sie z. B. "Wiederholung alle 3 Monate am 3. Montag des Monats" auswählen können (siehe Abbildung oben).

· Wenn Sie einen **Typ** -Wert von **Nach Auslöser**auswählen,

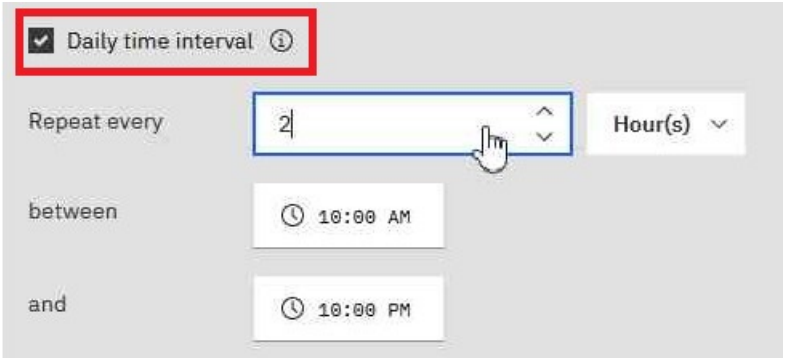


Tipp: Wenn ein Bericht von einem Auslöser geplant wird, kann er nur ausgeführt werden, wenn Sie bereits ein Auslöserereignis eingerichtet haben. Weitere Informationen finden Sie unter "Trigger-Vorkommen auf einem Server einrichten" in der *Verwaltung und Sicherheit* ..

Geben Sie in dem oben dargestellten Feld den Namen des Auslöservorkommens ein, z. B. `trigger.bat`.

4. Wenn Sie eine tägliche Frequenz für Ihre geplanten Einträge auswählen möchten, gehen Sie wie folgt vor:

   · Wählen Sie das Markierungsfeld **Tägliches Zeitintervall** aus.

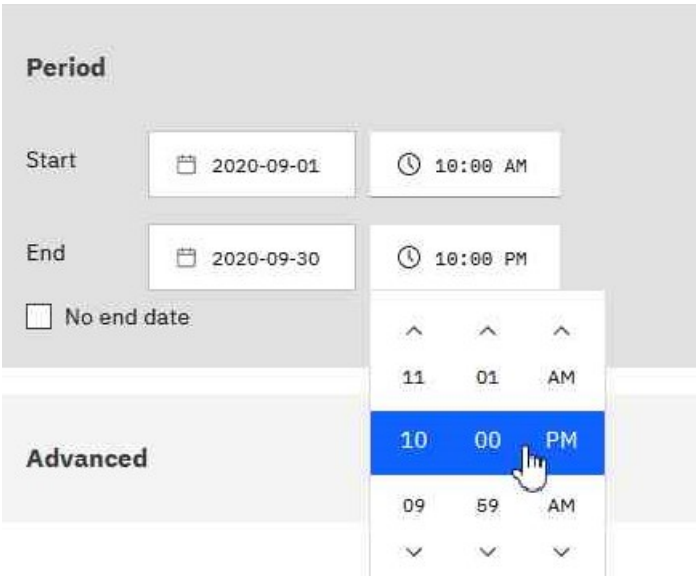


Tipp: Geben Sie die Häufigkeit und den Zeitraum während des Tages an, in dem der Bericht ausgeführt wird. Beispiel: "alle 2 Stunden zwischen 10:00 und 22:00 Uhr" (siehe Abbildung oben).

Es wird empfohlen, eine stündliche Frequenz auszuwählen, die gleichmäßig in die 24-Stunden-Uhr unterteilt wird. Auf diese Weise wird sichergestellt, dass Ihr Bericht jeden Tag zur selben Zeit ausgeführt wird. Wenn Sie eine stündliche Frequenz auswählen, die nicht gleichmäßig in die 24-Stunden-Uhr aufgeteilt wird, wird Ihr Bericht in den folgenden Tagen zu verschiedenen Zeiten ausgeführt.

5. Wenn Sie den Zeitraum festlegen möchten, innerhalb dessen die ersten und letzten Ausführungen des Berichts ausgeführt werden sollen, gehen Sie wie folgt vor:

   · Blättern Sie zum Abschnitt **Zeitraum** .



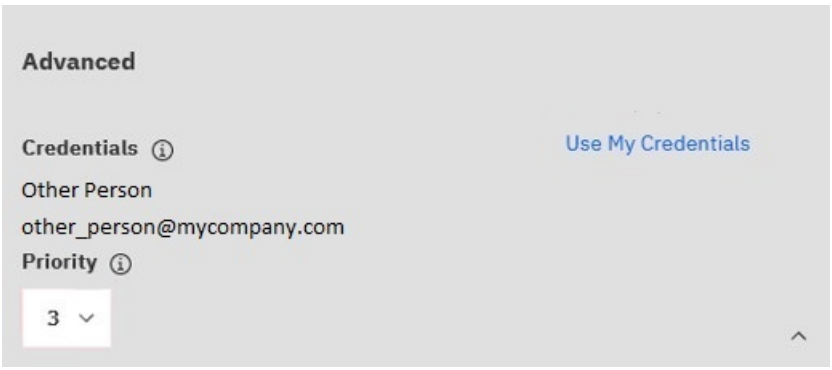
Tipp: Im obigen Beispiel wird der erste Berichtslauf am 1. September um 10:00 Uhr stattfinden, und der letzte Berichtslauf endet am 30. September um 22:00 Uhr.

Legen Sie das Datum und die Uhrzeit für den Beginn und das Ende der Periode fest.

Wenn Sie im Abschnitt **Zeitraum** nichts eingeben, beginnt der Zeitraum standardmäßig, sobald Sie den Zeitplan speichern, und es ist kein Enddatum vorhanden.

6. Gehen Sie wie folgt vor, wenn Sie die Berechtigungsnachweise oder die Priorität des Zeitplans ändern möchten:

   · Klicken Sie auf den Abschnitt **Erweitert** .



Tipp:

Informationen zum Feld 'Berechtigungsnachweise'

Die Berechtigungsnachweise zeigen den aktuellen Zeitplaneigner an. Wenn Sie nicht bereits der Zeitplaneigner sind, können Sie auf **Eigene Berechtigungsnachweise verwenden** klicken und temporäre Änderungen an dem Zeitplan vornehmen.

Weitere Informationen finden Sie im Artikel " Eigentumsrecht an einem Zeitplan übernehmen" in der *Benutzerhandbuch verwalten*.

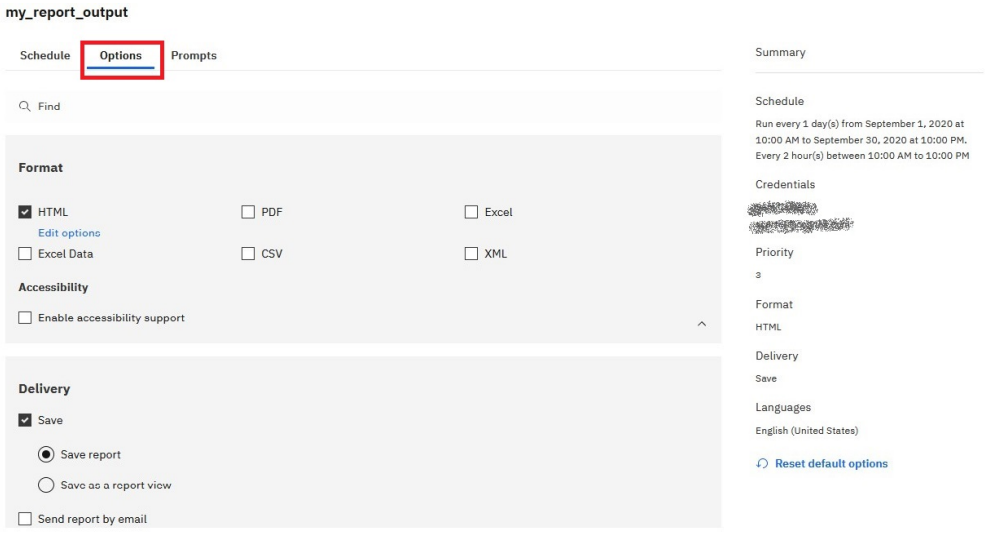
Informationen zum Feld "Priorität"

Wenn Sie die Funktion "Terminierungspriorität" zugeordnet haben, können Sie für den geplanten Eintrag eine Priorität von 1 bis 5 auswählen. Priorität 1 wird zuerst ausgeführt.

Weitere Informationen finden Sie im Artikel " Priorität für die Eintragsausführung ändern" in der *Benutzerhandbuch verwalten*.

7. Gehen Sie wie folgt vor, um das Standardformat, die Bereitstellungsmethode und die Sprache Ihres Berichts anzuzeigen:

· Klicken Sie auf die Registerkarte **Optionen** .

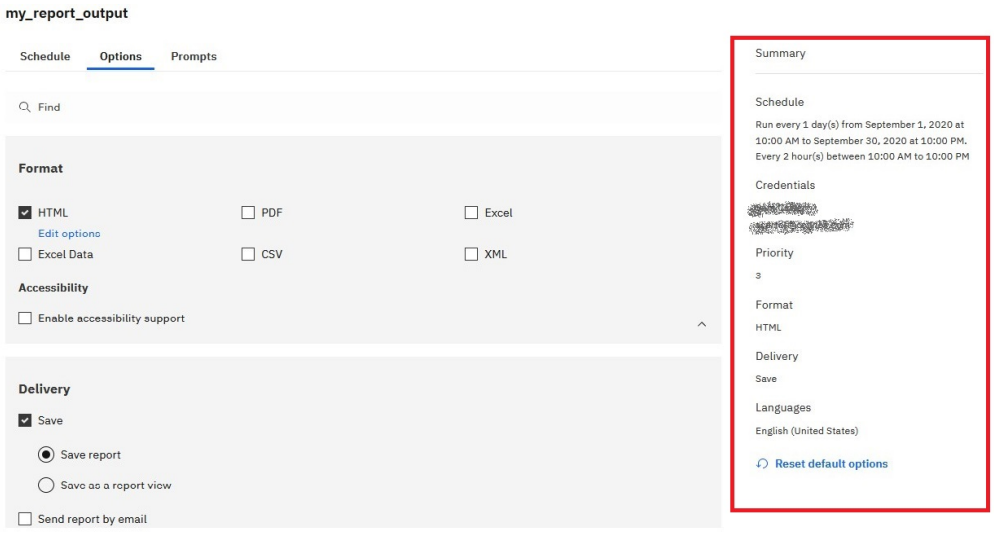


Tipp:

Die Standardoptionen werden angezeigt:

– **Format**: Nur HTML, behindertengerechte behindertengerechte Bedienung
– **Zustellung**: Nur Bericht speichern
– **Sprachen**: Nur Englisch

· Haben Sie das Teilfenster **Zusammenfassung** bemerkt?



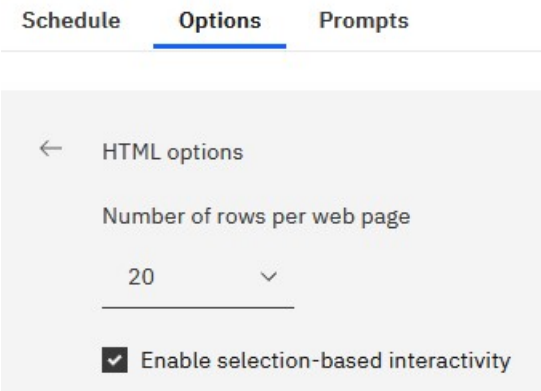
Tipp:

Wenn Sie Ihren Zeitplan erstellen, verwendet das Teilfenster **Zusammenfassung** auf der rechten Seite Ihres Fensters die natürliche Sprache, um alle Ihre Auswahl in Echtzeit zu beschreiben.

Sie können jederzeit auf **Standardoptionen zurücksetzen** klicken, um die Optionen zu löschen, die Sie auf jeder Registerkarte festgelegt haben.

8. Wenn Sie möchten, ändern Sie die **Format** -Optionen:

· Wenn Sie das HTML-Format auswählen, können Sie auf **Optionen bearbeiten**klicken.



Tipp:

Wenn Sie in einem Bericht eine Drilloperation durchführen oder einen Drillthrough zu anderen Berichten durchführen möchten, müssen Sie das Kontrollkästchen **Auswahlbasierte Interaktivität aktivieren** auswählen. Wenn Ihr Bericht jedoch sehr groß ist, können Sie das Kontrollkästchen abwählen, um die Zeit zu verkürzen, die für die Ausführung des Berichts erforderlich ist.

- Wenn Sie das PDF-Format auswählen, können Sie auf **Optionen bearbeiten**klicken.

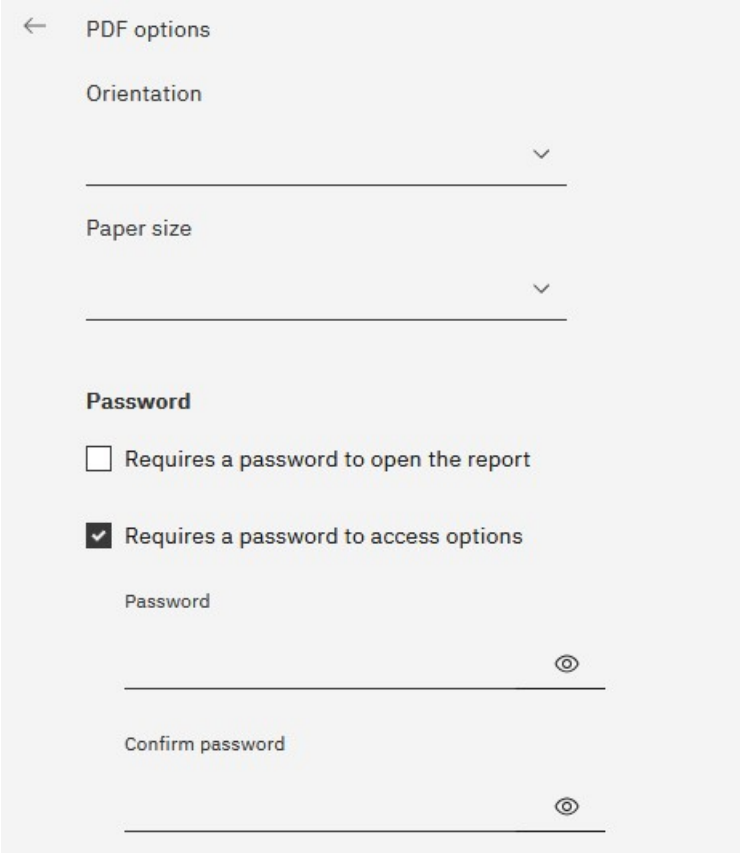


Abbildung 5. PDF-Optionen-Teil 1

Tipp: Sie können ein Kennwort erstellen, um zusätzliche Sicherheit zu Ihrem Bericht hinzuzufügen. Dies ist zusätzlich zu den Berechtigungen, die Benutzer durch ihre Funktionalität erhalten.

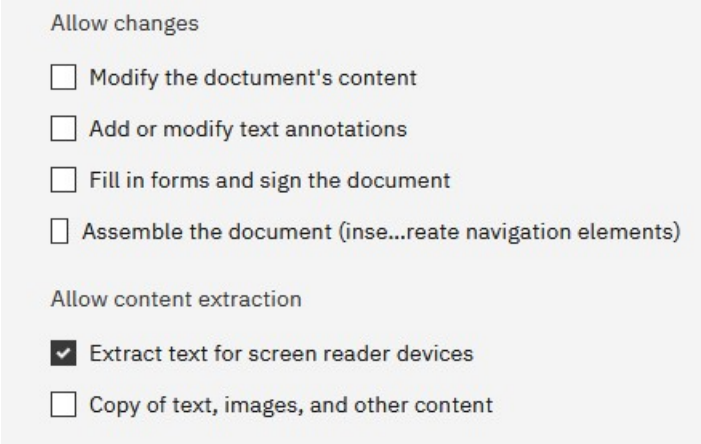


Abbildung 6. PDF-Optionen-Teil 2

Tipp: Sie können die Arten von Änderungen, die andere Benutzer an dem Bericht vornehmen können, begrenzen.

· Wenn Sie das Markierungsfeld **Unterstützung für Eingabehilfen aktivieren** auswählen.

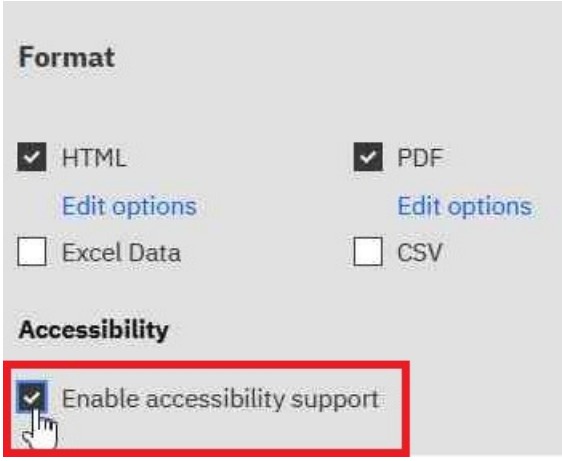


Abbildung 7. PDF-Optionen-Teil 1

Tipp: Sie können die Berichtsausgabe zugänglich machen. Zugängliche Berichte enthalten Features, wie z. B. Alternativtext, die Benutzern mit Behinderungen den Zugriff auf Berichtsinhalte mit Hilfe von unterstützenden Technologien ermöglichen, wie z. B. Sprachausgabeprogrammen.

In IBM ® Cognos ® -Anwendungen können Sie eine zugängliche Ausgabe für Berichte, Jobs, Schritte innerhalb von Jobs und geplante Einträge in PDF und HTML erstellen.

Für barrierefreie Berichte ist mehr Berichtsverarbeitung erforderlich und eine größere Dateigröße als nicht zugängliche Berichte. Folglich kann die Zugänglichkeit von Berichten negative Auswirkungen auf die Leistung haben.

9. Sie können die **Zustellung** -Optionen ändern:

· Wenn Sie den Bericht in Cognos Analytics speichern möchten, haben Sie zwei Optionen.

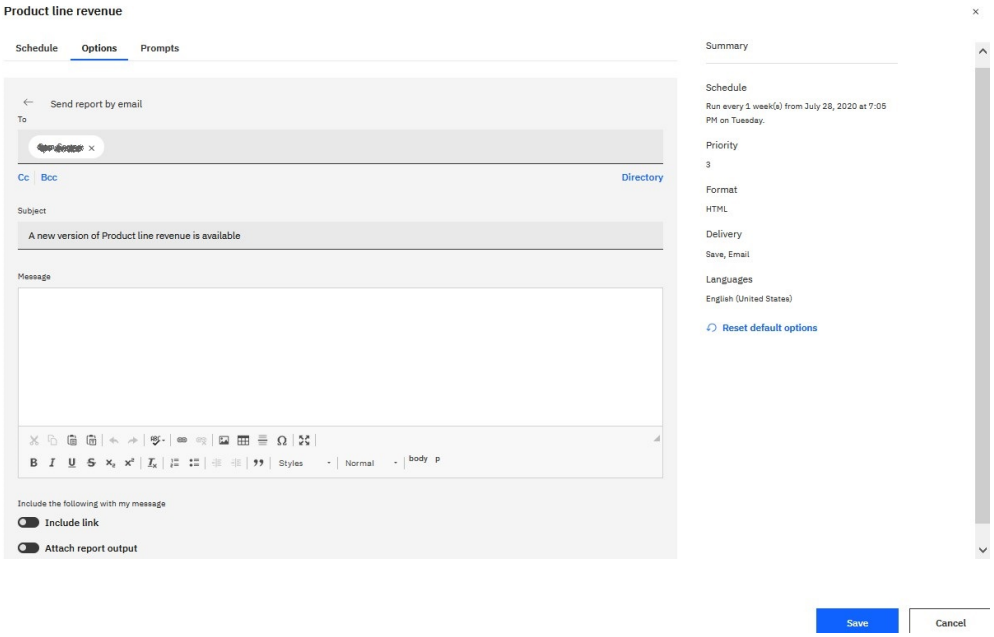
Abbildung 8. PDF-Optionen-Teil 1

Tipp:

- **Bericht speichern**. Diese Option ist standardmäßig ausgewählt.
- **Als Berichtsansicht speichern**. Anders als beim Speichern des Berichts können Sie den Namen oder Zielordner in der Berichtsansicht ändern. Eine Berichtsansicht verwendet dieselbe Berichtsspezifikation wie der Quellenbericht, weist jedoch unterschiedliche Eigenschaften auf, z. B. Eingabeaufforderungswerte, Zeitpläne, Bereitstellungsmethoden, Ausführungsoptionen, Sprachen und Ausgabeformate.

  Beim Erstellen einer Berichtsansicht wird der ursprüngliche Bericht nicht geändert. Sie können den Quellenbericht für eine Berichtsansicht ermitteln, indem Sie die zugehörigen Eigenschaften anzeigen. Die Eigenschaften der Berichtsansicht geben auch einen Link zu den Eigenschaften des Quellenberichts an.

· Wenn Sie **Bericht per E-Mail senden** auswählen und anschließend auf **Details bearbeiten**klicken.

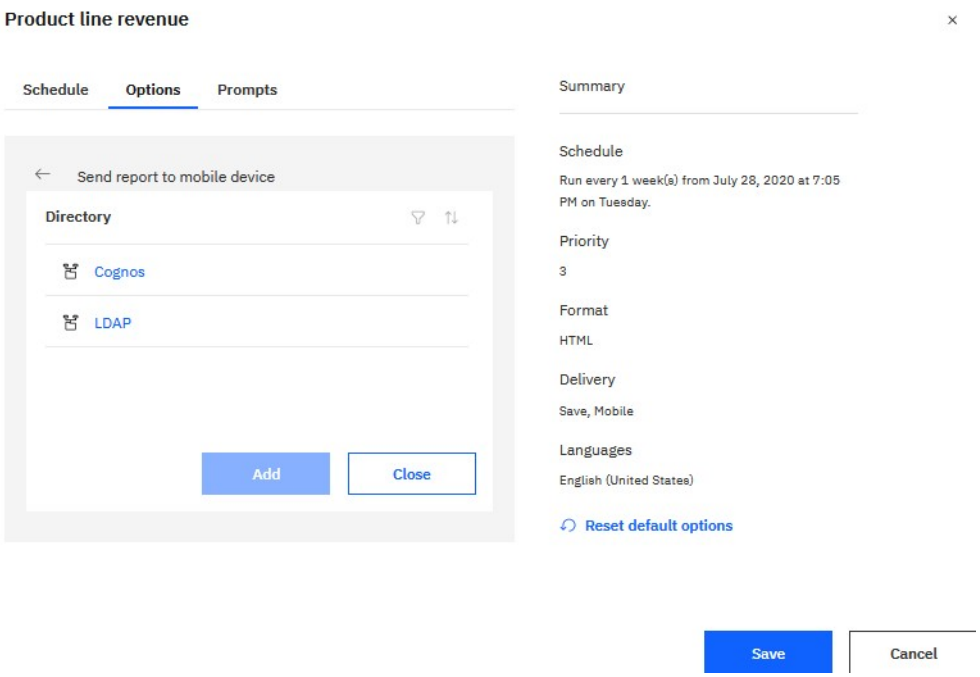


Tipp:

Es wird ein E-Mail-Fenster angezeigt, in dem Sie die Namen der Empfänger eingeben können, wenn Sie über die Berechtigung verfügen. Andernfalls können Sie Ihre E-Mail-Empfänger aus Ihrem lokalen LDAP-Verzeichnis auswählen. Wenn Ihr Verzeichnis sehr groß ist, können Sie Such-, Filter- und Sortierfunktionen verwenden, um Ihre Empfänger schnell zu finden.

Nachdem Sie Ihre Nachricht eingegeben haben und über die korrekten Berechtigungen verfügen, können Sie die Berichtsausgabe an die E-Mail anhängen. Oder Sie können einen Link hinzufügen, auf den Ihr Empfänger klicken kann, um den Bericht zu sehen.

· Wenn Sie **Bericht an mobiles Gerät senden**auswählen.

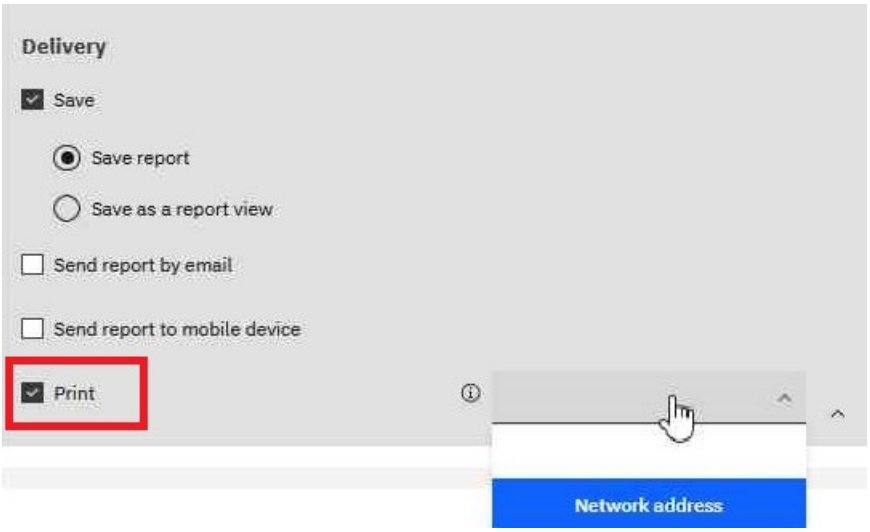


Tipp:

Diese Option ist nur für Benutzer von Cognos Analytics on Demand oder Cognos Analytics on Cloud Hosted verfügbar.

Ähnlich wie bei der E-Mail-Option, können Sie Ihren Empfänger im Verzeichnis finden. Wenn der Bericht ausgeführt wird, wird er über Cognos Analytics for Mobile an das mobile Gerät des Empfängers gesendet.

- Wenn Sie **Drucken**auswählen.



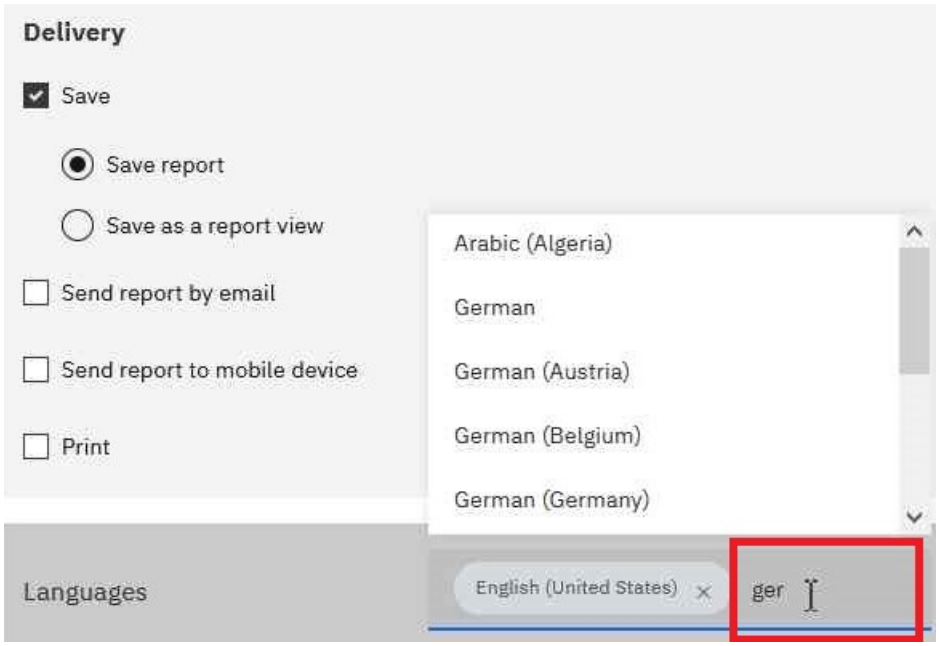
Tipp: Es kann bequem sein, dass Sie eine gedruckte Kopie eines Berichts haben.

Möglicherweise müssen Sie einen Bericht prüfen, wenn Ihr Computer nicht verfügbar ist, oder Sie benötigen möglicherweise eine Kopie eines Berichts an eine Besprechung.

Um Berichte zu drucken, müssen Sie die Funktion 'PDF-Ausgabe generieren' haben.

Wählen Sie einen Drucker aus der Liste aus oder geben Sie einen gültigen Druckernamen, einen gültigen Standort oder eine gültige Adresse ein, und klicken Sie anschließend auf **Hinzufügen**.

- Wenn Sie Ihre Ausgabe in anderen Sprachen als Englisch wünschen (Standardeinstellung).



Tipp: Beginnen Sie mit der Eingabe des Namens der Sprache in das Feld **Sprachen** . Es wird eine dynamische Liste der Sprachen angezeigt, aus der Sie die gewünschte Sprache auswählen können.

10. Wenn in Ihrem Bericht Eingabeaufforderungen angezeigt werden:

   · Klicken Sie auf die Registerkarte **Eingabeaufforderungen** , und klicken Sie dann auf **Werte festlegen**.

Tipp: In dem oben gezeigten Beispiel **Eingabeaufforderung** wird der Wert für den Parameter **`p_Date`** für einen Datumswert angezeigt.

11. Klicken Sie auf **Speichern**.

Ergebnisse

Es wird ein Zeitplan erstellt, und der Bericht wird zum nächsten geplanten Zeitpunkt ausgeführt.

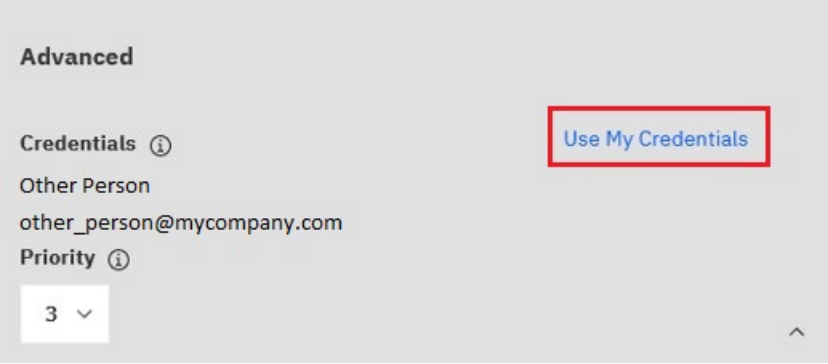
Eigentumsrecht an einem Zeitplan übernehmen

Wenn Sie einen Zeitplan bearbeiten, der von einem anderen Benutzer gehört, können Sie den Zeitplan während der aktuellen Cognos Analytics-Sitzung übernehmen.

Beispiel: Ein Zeitplaneigner befindet sich im Urlaub, aber Sie haben keine Zugriffsberechtigungen, um den Zeitplan zu ändern. Sie können das temporäre Eigentumsrecht an dem Zeitplan übernehmen und einige Planungsoptionen ändern, während sie weg sind. Sobald Sie die Sitzung verlassen, ändern sich die Berechtigungsnachweise des Zeitplans jedoch wieder an den ursprünglichen Eigner.

Vorgehensweise

1. Klicken Sie auf das Symbol 'Mehr' ··· , und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Zeitplan** , und klicken Sie dann auf **Bearbeiten**.
3. Blättern Sie auf der Registerkarte **Zeitplan** nach unten, und klicken Sie auf den Abschnitt **Erweitert** .



   Wenn der Zeitplan einem anderen Eigner zugeordnet ist, wird ein **Eigene Berechtigungsnachweise verwenden** -Link angezeigt.
4. Klicken Sie auf **Eigene Berechtigungsnachweise verwenden**.

   Ihr Name wird im Feld **Berechtigungsnachweise** angezeigt.
5. Nehmen Sie Änderungen am Zeitplan vor.
6. Klicken Sie auf **Speichern** , um den Zeitplan zu speichern.

Ergebnisse

Der Zeitplan wird mit den Änderungen aktualisiert, die Sie vorgenommen haben. Sobald Sie die Sitzung verlassen, werden die Berechtigungsnachweise des Zeitplans an den ursprünglichen Eigner zurückgeändert.

Priorität für die Eintragsausführung ändern

Sie können den geplanten Einträgen eine Priorität von 1 bis 5 zuordnen.

Zum Beispiel wird ein Eintrag mit Priorität 1 vor einem Eintrag mit Priorität 5 ausgeführt. Wenn mehr als ein Eintrag mit derselben Priorität vorhanden ist, wird zuerst die erste, die in der Warteschlange eintraf, ausgeführt. Die Standardpriorität ist 3.

Vorbereitende Schritte

Sie müssen über die Funktion "Planungspriorität" verfügen, um die Ausführungspriorität zu ändern.

Informationen zu diesem Vorgang

Interaktive Einträge werden immer sofort ausgeführt, und die Priorität kann nicht geändert werden, wenn sie ausgeführt werden.

Sie legen die Priorität für einen Eintrag fest, wenn Sie ihn terminieren. Wenn sich ein Eintrag in der aktuellen, anstehenden oder geplanten Warteschlange befindet, können Sie die Priorität ändern.

Möglicherweise möchten Sie eine niedrige Priorität für Einträge festlegen, die eine lange Zeit benötigen, damit andere Einträge in der Warteschlange nicht verzögert werden.

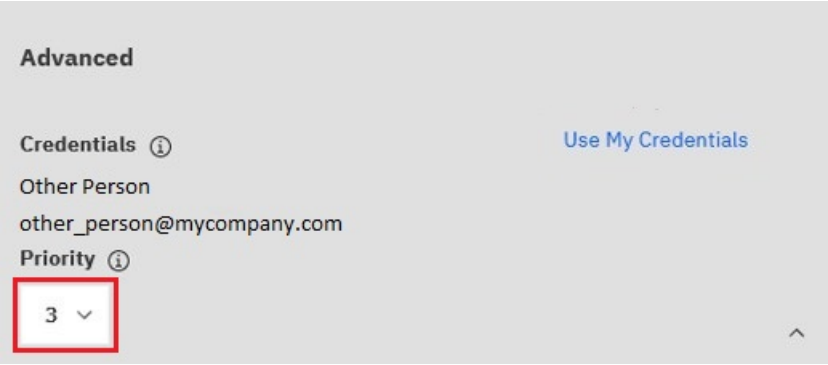
Wenn Sie einen Job terminieren, legen Sie die Priorität für den gesamten Job fest, nicht für einzelne Einträge innerhalb des Jobs. Möglicherweise möchten Sie eine niedrige Priorität für einen Job mit vielen Einträgen festlegen, damit andere Einträge in der Warteschlange nicht verzögert werden.

Sie planen die Priorität für den übergeordneten Job. Wenn der Job ausgeführt wird, übernehmen alle untergeordneten Einträge die Priorität des übergeordneten Jobs. Wenn sich der Job in der Warteschlange befindet und noch nicht aktiv ist, können Sie die Priorität aktualisieren. Sie können dies nicht für die einzelnen Einträge im Job ausführen. Durch Ändern der Priorität des Jobs wird die Priorität aller untergeordneten Einträge geändert. Sie können den Ausführungsverlauf eines Jobs anzeigen, während er ausgeführt wird, und sehen, welche der zugehörigen Einträge ausgeführt wurden, ausgeführt werden oder bis zum Abschluss stehen.

Die Priorität der Einträge in der Warteschlange wirkt sich nicht auf einen bereits aktiven Eintrag aus. Dieser Eintrag wird abgeschlossen, und anschließend wird die Warteschlangenpriorität auf den nächsten zu laufenden Eintrag überprüft.

Vorgehensweise

1. Klicken Sie auf das Symbol 'Mehr' ⋯ , und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Zeitplan** , und klicken Sie dann auf **Bearbeiten**.
3. Blättern Sie auf der Registerkarte **Zeitplan** nach unten, und klicken Sie auf den Abschnitt **Erweitert** .



4. Klicken Sie im Feld Priorität auf das Unterchevron, und wählen Sie dann eine Zahl von 1 bis 5 aus.
5. Klicken Sie auf **Speichern** , um den Zeitplan zu speichern.

Anstehende Aktivitäten für einen bestimmten Tag verwalten

Sie können auswählen, ob eine Liste aller anstehenden Aktivitäten angezeigt werden soll, die für einen bestimmten Tag geplant sind.

Jeder Eintrag wird nach Namen aufgelistet und zeigt die Anforderungszeit und die Priorität an. Ein Balkendiagramm zeigt die Gesamtzahl der geplanten und abgebrochenen Einträge für jede Stunde des Tages an. Die Diagrammlegende zeigt die Gesamtzahl der geplanten und abgebrochenen Einträge für den Tag an.

Sie können die Spalten " **Anforderungszeit**", " **Status**" und " **Priorität** " sortieren. Sie können auswählen, ob eine Liste mit Hintergrundaktivitäten oder interaktiven Aktivitäten angezeigt werden soll.

Jeder Eintrag zeigt den Benutzer an, der ihn terminiert hat. Sie können nach Benutzer sortieren.

Sie können geplante Ausführungen von Einträgen stornieren, die abgebrochenen Eintragsläufe neu planen und Prioritäten setzen. Sie können Einträge auf unbestimmte Zeit aussetzen oder bis zu einem

bestimmten Datum aussetzen. Weitere Informationen finden Sie unter „Ausgesetzte Aktivitäten“ auf Seite 264

Sie können auf das Symbol **Details anzeigen**  klicken, um weitere Informationen anzuzeigen. Für jeden Eintrag werden **Antwortzeit der letzten Ausführung** und **Pfad**angezeigt.

Sie können die Einträge so filtern, dass nur diejenigen angezeigt werden, die Sie möchten. Sie können das Datum und die Uhrzeit auswählen, für die Sie anstehende Aktivitäten anzeigen möchten. Sie können nach Status, Priorität, Typ und Geltungsbereich filtern.

Sie können auch nach dem Benutzer, der den Eintrag terminiert hat, und dem Eintragseigner filtern.

Sie können filtern, um festzustellen, wie viele geplante Einträge derzeit ausgesetzt sind. Weitere Informationen finden Sie unter „Ausgesetzte Aktivitäten“ auf Seite 264 .

Sie können die Priorität eines Eintrags in der Warteschlange „Priorität für die Eintragsausführung ändern“ auf Seite 258ändern.

Vorgehensweise

1. Klicken Sie im Menü **Verwalten** auf **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Status** auf **Anstehende Aktivitäten**.
3. Klicken Sie im Abschnitt **Filter** auf die Filteroptionen, die Sie verwenden möchten.

   Tipp: Wenn Sie erweiterte Filteroptionen verwenden möchten, klicken Sie auf **Erweiterte Optionen**. Wenn Sie alle Auswahlen auf die Standardeinstellungen zurücksetzen möchten, klicken Sie auf **Auf Standardwert zurücksetzen**.
4. Klicken Sie auf **Anwenden**.

   · In der Liste werden die von Ihnen ausgewählten Einträge angezeigt.

   · Die Filterstatuszeile zeigt die Kriterien an, die zum Generieren der Liste verwendet werden.

   · Das Balkendiagramm zeigt die geplanten und abgebrochenen Einträge nach Stunde für den angegebenen Tag an.

   Die Liste der Einträge, die Filterstatuszeile und das Diagramm werden immer dann aktualisiert, wenn Sie den Filter neu definieren und auf **Anwenden**klicken. Die Liste der Einträge und der Filterstatuszeile ändert sich nicht, wenn Sie das Diagramm zu einem anderen Datum durchsuchen.
5. Wenn Sie eine Aktion für einen einzelnen Eintrag ausführen möchten, klicken Sie auf den **Aktionen** -Pfeil für den Eintrag und wählen Sie die Aktion aus. Wenn Sie eine Aktion für mehrere Einträge ausführen möchten, wählen Sie das Kontrollkästchen für die gewünschten Einträge aus, und klicken Sie anschließend auf eine der folgenden Schaltflächen in der Symbolleiste.

   In der folgenden Tabelle sind die Aktionen angegeben, die für Einträge und die zugehörigen Symbole verfügbar sind:

Tabelle 65. Anstehende Aktivitäten für bestimmte Tagesaktionen und Symbole verwalten

Aktion	**Symbol**
Details anzeigen (rechte obere Ecke)	
Details ausblenden (rechte obere Ecke)	
Ausführung abbrechen (Menü**Aktionen** neben Eintrag)	
Einträge aussetzen (Menü**Aktionen** neben dem Eintrag)	

Tabelle 65. Anstehende Aktivitäten für bestimmte Tagesaktionen und Symbole verwalten (Forts.)	
Aktion	**Symbol**
Ausgesetzte Einträge ausführen (Menü**Aktionen** neben Eintrag)	
Eine Ausführung erneut terminieren, die abgebrochen wurde (Menü**Aktionen** neben dem Eintrag)	
Priorität festlegen (Menü**Aktionen** neben dem Eintrag)	

Tipp: Wenn Sie alle Einträge in der Liste auswählen möchten, wählen Sie das Kontrollkästchen für die Liste aus.

Frühere Aktivitäten verwalten über die Administrationskonsole

Bei den vergangenen Aktivitäten handelt es sich um Einträge, die die Verarbeitung in IBM Cognos abgeschlossen haben.

Jeder Eintrag wird nach Namen aufgelistet und zeigt die Anforderungszeit und den Status an. Sie können die Spalten **Anforderungszeit** und **Status** sortieren. Das Balkendiagramm zeigt die Gesamtzahl der Einträge, aufgeschlüsselt nach Status, an. Wenn ein Eintrag fehlgeschlagen ist, wird eine Schaltfläche angezeigt, in der die Wertigkeit des Fehlers angezeigt wird. Der Benutzer, der den Eintrag ausgeführt hat, wird ebenfalls aufgelistet.

Sie können die Einträge so filtern, dass nur diejenigen angezeigt werden, die Sie möchten. Sie können eine Liste der Aktivitäten anzeigen, die innerhalb einer bestimmten Zeitdauer aufgetreten sind, z. B. die letzten vier Stunden oder den letzten Tag, oder Sie können einen Datums-oder Zeitbereich angeben. Sie können nach Status, Typ und Geltungsbereich filtern. Sie können auch nach dem Benutzer, der den Eintrag ausgeführt hat, dem Benutzer, der Eigner des Eintrags ist, und dem Dispatcher, auf dem die Aktivität ausgeführt wurde, filtern.

Sie können das Ausführungsprotokoll „Anzeigen des Ausführungsprotokolls von Einträgen" auf Seite 266anzeigen.

Vorgehensweise

1. Klicken Sie im Menü **Verwalten** auf **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Status** auf **Vergangene Aktivitäten**.

   Es wird ein Diagramm angezeigt, das zeigt, wann vergangene Aktivitäten ausgeführt wurden und ob sie erfolgreich waren, fehlgeschlagen sind oder abgebrochen wurden. Unterhalb des Diagramms werden Details zu den Aktivitäten aufgelistet.
3. Zum Filtern der Aktivitäten, die im Diagramm und in der Liste angezeigt werden, rufen Sie die Anzeige **Filter** auf und wählen Sie die gewünschten Attribute aus.

   Tipp: Sie können nach den folgenden Attributen filtern:

   · Zeitraum, innerhalb dessen die Tätigkeiten ausgeführt wurden

   · Der Benutzer, der die Aktivität ausgeführt hat

   · Aktivitätseigner

   · Aktivitätsstatus

   · Aktivitätstyp

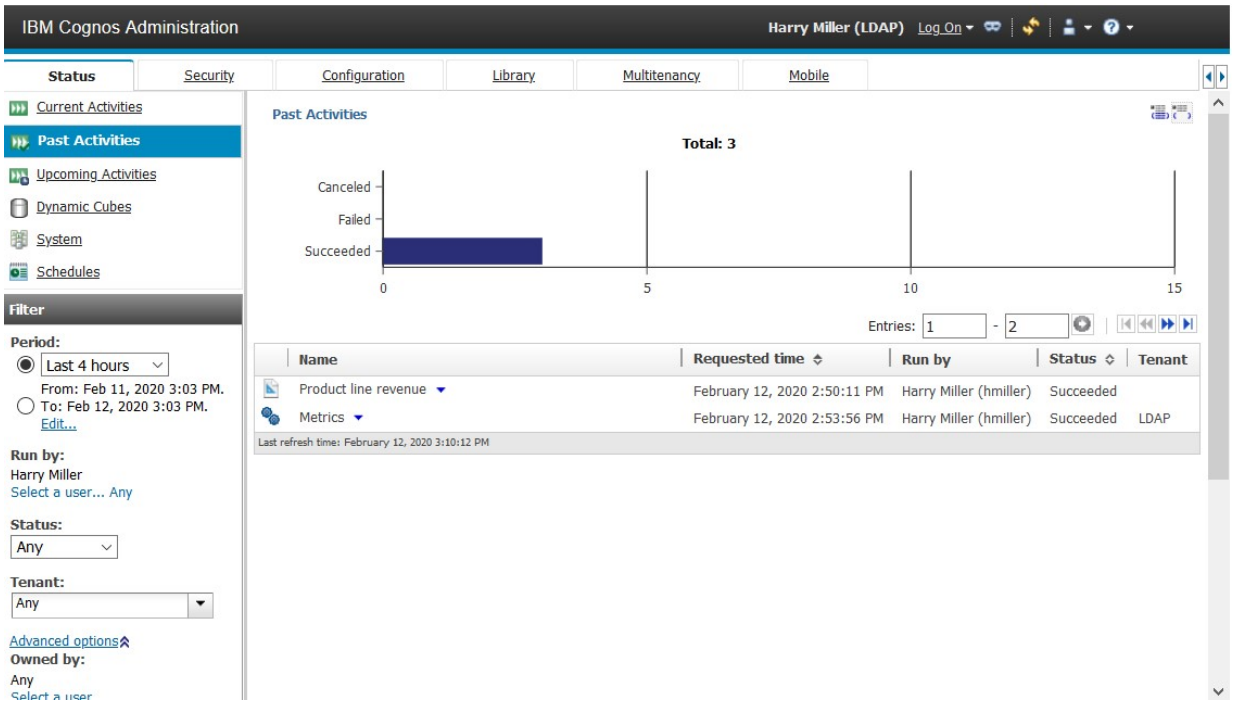
   · Der Dispatcher, der die Aktivität ausgeführt hat

· Bereich von Ordnern in **Teaminhalt** , in dem sich das Element befindet

Das folgende Diagramm zeigt ein Beispiel dafür, wie vergangene Aktivitäten in der Administrationskonsole angezeigt werden. Beachten Sie in diesem Beispiel Folgendes:

· Die Liste wird gefiltert, um nur Berichte anzuzeigen, die von Harry Miller ausgeführt werden.

· Der Job "Kennzahlen" enthält zwei Berichte, die als Jobschritte ausgeführt werden. Diese beiden Berichtsausführungen werden jedoch nicht in der Liste der Aktivitäten angezeigt.



4. Wenn eine Aktivität fehlgeschlagen ist, können Sie über die Fehlerschaltfläche neben dem Status eine Pause einlegen, um die Wertigkeit des Fehlers anzuzeigen.
5. Wenn Sie eine Aktion für einen einzelnen Eintrag ausführen möchten, klicken Sie auf den **Aktionen** -Pfeil für den Eintrag und wählen Sie die Aktion aus.

   Um eine Aktion für mehrere Einträge auszuführen, klicken Sie entweder auf das Symbol **Details anzeigen** oder auf das Symbol **Details ausblenden** in der Symbolleiste.

Aktuelle Aktivitäten verwalten

Aktuelle Aktivitäten sind Einträge, die derzeit in IBM Cognos -Software verarbeitet werden.

Jeder Eintrag wird nach Namen aufgelistet und zeigt die Anforderungszeit, den Status und die Priorität für Hintergrundaktivitäten an. Das Balkendiagramm zeigt die Gesamtzahl der Einträge an, aufgeschlüsselt nach der Anzahl der anstehenden, ausgeführten, wartenden und ausgesetzten Einträge. Wenn die Aktivität verarbeitet wird, wird die Prozessnummer angezeigt.

Sie können die Spalten " **Anforderungszeit**", " **Status**" und " **Priorität** " sortieren. Sie können auswählen, ob eine Liste mit Hintergrundaktivitäten oder interaktiven Aktivitäten angezeigt werden soll. Der Benutzer, der den Eintrag ausgeführt hat, wird ebenfalls aufgelistet. Sie können nach Benutzer sortieren.

Sie können Hintergrundeinträge aussetzen und sie später freigeben, wenn Sie möchten, dass sie ausgeführt werden. Sie können die Ausführung für Einträge, die einen der folgenden Status aufweisen, dauerhaft abbrechen:

· Anstehend in der Warteschlange

· Ausführung

· Ausgesetzt

· Warten auf die Ausführung einer externen Instanz von IBM Cognos

Sie können die Einträge so filtern, dass nur diejenigen angezeigt werden, die Sie möchten. Sie können auswählen, dass nur die Einträge mit einem bestimmten Status oder einer bestimmten Priorität angezeigt werden sollen, oder Sie können Einträge eines bestimmten Typs oder Bereichs anzeigen.

Für interaktive aktuelle Einträge können Sie den Status und den Dispatcher filtern, in dem die Aktivität ausgeführt wird. Für aktuelle Hintergrundeinträge können Sie nach Status, Priorität, Typ, Geltungsbereich, Benutzer, der den Eintrag ausgeführt hat, -Benutzer filtern, der Eigner des Eintrags, und Dispatcherist.

Wenn derzeit ein Eintrag ausgeführt wird, wird der Dispatcher, die Prozess-ID und die Startzeit angezeigt. Beachten Sie, dass die Prozess-ID und der Dispatcher für aktuelle Hintergrundeinträge möglicherweise nicht verfügbar sind, wenn die Aktivität zum ersten Mal angezeigt wird. Aktualisieren Sie die Seite, um die aktualisierte Prozess-ID und den aktualisierten Dispatcher anzuzeigen.

Wenn Sie einen Eintrag abbrechen, der andere Einträge enthält, wie z. B. einen Job oder einen Agenten, werden Schritte oder Tasks abgebrochen, die noch nicht abgeschlossen wurden. Schritte oder Tasks, die bereits abgeschlossen wurden, bleiben jedoch abgeschlossen.

Sie können die Priorität von Einträgen „Anzeigen des Ausführungsprotokolls von Einträgen“ auf Seite 266,„Priorität für die Eintragsausführung ändern“ auf Seite 258 ändern und die Ausführungsprotokoll anzeigen.

Vorgehensweise

1. Klicken Sie im Menü **Verwalten** auf **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Status** auf **Aktuelle Aktivitäten**.
3. klicken Sie auf **Hintergrundaktivitäten** oder **Interaktive Aktivitäten**, und Sie im Abschnitt **Filter** die Filteroptionen an, die Sie verwenden möchten.

   Tipp: Wenn Sie erweiterte Filteroptionen verwenden möchten, klicken Sie auf **Erweiterte Optionen**. Wenn Sie alle Auswahlen auf die Standardeinstellungen zurücksetzen möchten, klicken Sie auf **Auf Standardwert zurücksetzen**.
4. Klicken Sie auf **Anwenden**.

   In der Liste werden die von Ihnen ausgewählten Einträge angezeigt.
5. Wenn Sie eine Aktion für einen einzelnen Eintrag ausführen möchten, klicken Sie auf den **Aktionen** -Pfeil für den Eintrag und wählen Sie die Aktion aus. Wenn Sie eine Aktion für mehrere Einträge ausführen möchten, wählen Sie das Kontrollkästchen für die gewünschten Einträge aus, und klicken Sie anschließend auf eine der folgenden Schaltflächen in der Symbolleiste.

   In der folgenden Tabelle sind die Aktionen angegeben, die für Einträge und die zugehörigen Symbole verfügbar sind:

Tabelle 66. Aktionen und Symbole für aktuelle Aktivitäten verwalten

Aktion	**Symbol**
Details anzeigen (rechte obere Ecke)	
Details ausblenden (rechte obere Ecke)	
Ausführung abbrechen (Menü**Aktionen** neben Eintrag)	
Ausführung aussetzen (Menü**Aktionen** neben Eintrag)	
Ausgesetzte Einträge ausführen (Menü**Aktionen** neben Eintrag)	

Tabelle 66. Aktionen und Symbole für aktuelle Aktivitäten verwalten (Forts.)	
Aktion	**Symbol**
Priorität festlegen (Menü**Aktionen** neben dem Eintrag)	

Tipp: Wenn Sie alle Einträge in der Liste auswählen möchten, wählen Sie das Kontrollkästchen für die Liste aus.

Ausgesetzte Aktivitäten

Sie können Einträge aussetzen, um auf Systemanforderungen zu reagieren und sie später wieder aufnehmen zu können.

Nach der Aussetzung von Einträgen können Sie eine Liste mit Einträgen anzeigen, die auf unbestimmte Zeit ausgesetzt sind.

Sie können die ausgesetzten Einträge auch dann wieder aufnehmen, wenn die ursprüngliche Ausführungszeit abgelaufen ist. Wenn Sie beispielsweise einen Bericht für 9:00 Uhr terminieren und ihn dann aussetzen, können Sie den Bericht um 9:30 Uhr erneut starten.

Das anstehende Aktivitätenbardiagramm hilft Ihnen bei der Festlegung, wann Einträge neu geplant werden sollen. Wenn Sie die nächsten Termine im Diagramm anzeigen, können Sie die Anzahl der Einträge für einen bestimmten Tag anzeigen. Wenn Sie den Zeiger über eine bestimmte Stunde am Tag anhalten, können Sie die Anzahl der Einträge für diese Stunde finden. Verwenden Sie diese Option, um ein Datum zu ermitteln, an dem die Nachfrage niedrig ist, und den Eintrag zu diesem Datum neu planen. In den Diagrammspalten wird die Gesamtzahl der geplanten und abgebrochenen Einträge für jede Stunde des Tages angezeigt. Die Diagrammlegende zeigt die Gesamtzahl der geplanten, abgebrochenen und ausgesetzten Einträge für den Tag an.

Einträge aussetzen

Sie können Aktivitäten aussetzen.

Wenn Ihr System z. B. zu bestimmten Zeiten überlastet ist, können Sie die Workload reduzieren und Engpässe während dieser Spitzenzeiten vermeiden, indem Sie Einträge auf unbestimmte Zeit aussetzen oder sie für einen späteren Zeitpunkt neu planen.

Vorgehensweise

1. Klicken Sie im Menü **Verwalten** auf **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Status** auf **Anstehende Aktivitäten**.
3. Wählen Sie im Abschnitt **Filter** für **Tag** ein Datum aus, und klicken Sie für **Status** auf **Geplant**.
4. Klicken Sie auf **Anwenden**.

   In der Liste werden die geplanten Einträge für das ausgewählte Datum angezeigt. Da Einträge an diesem Datum zurückgemeldet werden, möchten Sie bestimmte Einträge auf unbestimmte Zeit aussetzen und andere Einträge neu planen. Sie möchten die anstehenden Termine im Diagramm durchsuchen und ein anderes Datum für die ausgesetzten Einträge auswählen.
5. Klicken Sie im Diagramm auf die nächsten und vorherigen Symbole, um die nächsten Datumsangaben zu durchsuchen. Das Diagramm zeigt sowohl geplante als auch abgebrochene Einträge für jeden Tag nach Stunde an.

   Wichtig: Die Liste der Einträge, die angezeigt werden, ändert sich nicht, um das in der Tabelle ausgewählte Datum zu erfüllen. Die Liste der Einträge stimmt mit Ihren angegebenen Filterkriterien überein und ändert sich erst, wenn Sie einen neuen Filter angeben und anwenden.

6. Wählen Sie in der Liste der geplanten Einträge das Kontrollkästchen für die Einträge aus, die ausgesetzt werden sollen, und klicken Sie auf die Schaltfläche zum Aussetzen in der Symbolleiste. Im Dialogfenster **Aktivität aussetzen**

   · Wenn Sie die Einträge unbegrenzt sperren, klicken Sie auf **Unendlich**.

   · Zum erneuten Planen von Einträgen auf ein anderes Datum klicken Sie auf **Bis**, und wählen Sie ein Datum und eine Uhrzeit aus.

   Beachten Sie, dass sowohl das Diagramm als auch die Liste der Einträge aktualisiert werden, und die ausgesetzten Einträge werden nicht mehr in der Liste der Einträge angezeigt.

   Tipp: Wenn Sie einen einzelnen Eintrag aussetzen möchten, klicken Sie auf den **Aktionen** -Menüpfeil für den Eintrag und klicken Sie auf **Aussetzen**.

Ausgesetzte Einträge für einen bestimmten Tag anzeigen

Sie können eine Liste der ausgesetzten Einträge für einen bestimmten Tag anzeigen.

Vorgehensweise

1. Klicken Sie im Menü **Verwalten** auf **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Status** auf **Anstehende Aktivitäten**.
3. Wählen Sie im Abschnitt **Filter** unter **Tag** ein Datum aus, und klicken Sie unter **Status** auf **Ausgesetzt**.
4. Klicken Sie auf **Anwenden**.

   In der Liste werden die ausgesetzten Einträge für diesen Tag angezeigt.

   Sie können ausgesetzte Einträge ausführen, abbrechen oder neu planen. Wenn Sie eine Aktion für einen einzelnen Eintrag ausführen möchten, klicken Sie auf den Pfeil rechts neben dem Eintrag und wählen Sie die gewünschte Aktion aus. Um eine Aktion für mehrere Einträge auszuführen, wählen Sie das Kontrollkästchen für die gewünschten Einträge aus, und klicken Sie anschließend auf die entsprechende Schaltfläche in der Symbolleiste.

   In der folgenden Tabelle sind die Aktionen angegeben, die für Einträge und die zugehörigen Symbole verfügbar sind:

Tabelle 67. Liste der ausgesetzten Einträge für bestimmte Tagesaktionen und Symbole anzeigen

Aktion	**Symbol**
Details anzeigen (rechte obere Ecke)	
Details ausblenden (rechte obere Ecke)	
Ausführung abbrechen (Menü**Aktionen** neben Eintrag)	
Einträge aussetzen (Menü**Aktionen** neben dem Eintrag)	
Ausgesetzte Einträge ausführen (Menü**Aktionen** neben Eintrag)	
Eine Ausführung erneut terminieren, die abgebrochen wurde (Menü**Aktionen** neben dem Eintrag)	

Tabelle 67. Liste der ausgesetzten Einträge für bestimmte Tagesaktionen und Symbole anzeigen (Forts.)	
Aktion	**Symbol**
Priorität festlegen (Menü**Aktionen** neben dem Eintrag)	

Tipp: Wenn Sie alle Einträge in der Liste auswählen möchten, wählen Sie das Kontrollkästchen für die Liste aus.

Anzeigen des Ausführungsprotokolls von Einträgen

Sie können die Ausführungshistorie von Einträgen anzeigen, die im Hintergrund ausgeführt werden sollen, ohne darauf zu warten, dass sie angezeigt werden.

Dazu gehören geplante Einträge, die einmal ausgeführt und gespeichert werden, sowie interaktive Einträge, die gespeichert oder per E-Mail gesendet werden. Interaktive Einträge haben keine Laufhistorien.

IBM Cognos software keeps history information each time an entry runs in the background. Das Ausführungsprotokoll für einen Eintrag enthält Informationen, wie z. B. die Anforderungszeit, die Startzeit, die Beendigungszeit und die erfolgreiche Ausführung des Berichts.

Sie können einen ausführlicheren Ausführungsverlauf für den Eintrag anzeigen, der allgemeine, Fehler- und Warnnachrichten enthält, die sich auf den Eintrag und alle Aktionen beziehen, die Sie ausführen können. Wenn eine E-Mail mit dem Eintrag verknüpft ist, wird der Status der E-Mail-Zustellung eingeschlossen.

Einige Arten von Einträgen zeigen zusätzliche Informationen auf der Seite mit dem detaillierten Ausführungsverlauf an:

- Für Berichte wird eine Berichtsausgabeversion jedes Mal beibehalten, wenn ein Bericht gemäß einem Zeitplan ausgeführt wird. Sie können die Berichtsausgabeversion aus der detaillierten Ausführungshistorie anzeigen.
- Für Jobs und Agenten können Sie eine Liste der Schritte anzeigen und eine detaillierte Ausführungshistorie für jede einzelne Schritte anzeigen. Sie können auch die Teile des Jobs oder des Agenten anzeigen, die noch nicht abgeschlossen sind. Wenn der Eintrag Teil eines übergeordneten Eintrags ist, können Sie den übergeordneten Eintrag anzeigen, der die Ausführung eingeleitet hat.
- Für Benutzertasks, die in einem Agenten enthalten sind, können Sie eine Liste der Schritte anzeigen und eine detaillierte Ausführungshistorie für jede einzelne Schritte anzeigen.
- Für Implementierungs-und Importeinträge können Sie den öffentlichen Inhalt in **IBM Cognos Administration**anzeigen.

  Die folgende Nachricht wird angezeigt: *Nur die Fortschrittsinformationen sind derzeit verfügbar. Die Informationen werden im Anschluss an die Beendigung der übergeordneten Aktivität*aktualisiert.

  Dies bedeutet, dass die Implementierung abgeschlossen ist, die übergeordnete Aktivität jedoch noch aktiv ist. Sobald die endgültigen Beendigungs-Informationen von Content Manager abgerufen werden, wird die Nachricht nicht mehr angezeigt.

Sie können fehlgeschlagene Einträge „Fehler beim erneuten Ausführen einer Task erneut ausführen” auf Seite 268 aus der detaillierten Ausführungsverlaufsseite erneut ausführen. Sie können eine Liste der zugehörigen Ausführungen anzeigen, die Teil der Wiederholungsserie sind, und eine detaillierte Ausführungshistorie für jede einzelne Ausführung anzeigen. You can specify how many run history occurrences to keep or for how long to keep them „Festlegen, wie lange Laufhistorien aufbewahrt werden sollen” auf Seite 267.

Vorgehensweise

1. Klicken Sie im Menü **Verwalten** auf **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Status** auf **Zeitpläne** oder **Vergangene Aktivitäten**.
3. Klicken Sie neben dem Eintrag auf den Pfeil, und klicken Sie dann auf **Laufprotokoll anzeigen**  .
4. Wenn Sie möchten, wählen Sie die **Status** von Einträgen aus, die Sie anzeigen möchten.

   Es wird eine Liste der ausgewählten Einträge angezeigt.
5. Wenn Sie die Ausführungsverlaufsdetails anzeigen möchten, klicken Sie in der Spalte **Aktionen** neben dem gewünschten Eintrag auf die Schaltfläche für die Detailansicht des Ausführungsprotokolls  . Wählen Sie dann, wenn Sie möchten, aus der Liste **Schweregrad** die Wertigkeit der Einträge aus.

   In den Jobschritten werden die Details zum vollständigen Ausführungsverlauf angezeigt. Wenn die Detailstufe für das Joblaufprotokoll auf **Begrenzt**gesetzt wurde, werden keine Verlaufsdetails für die Jobschritte aufgezeichnet.
6. Wenn es eine Berichtsausgabeversion gibt, klicken Sie in der Spalte **Aktionen** auf die Schaltfläche 'Ausgaben anzeigen'  , um den gewünschten Eintrag zu erhalten. Klicken Sie anschließend in der Liste **Versionen** auf die gewünschte Version. Um eine Version zu löschen, klicken Sie auf **Versionen verwalten** , und klicken Sie dann auf das Kontrollkästchen für die Version. Klicken Sie dann auf **Löschen**.
7. Wenn Sie Nachrichten anzeigen möchten, klicken Sie auf ein Element mit einem Link in der Spalte **Nachrichten** .

   Nachrichten werden verschachtelt. Untergeordnete Nachrichten können in untergeordneten Nachrichten angezeigt werden. Wenn eine Nachricht als Link angezeigt wird, können Sie über die untergeordneten Nachrichten weiterhin einen Drilldown durchführen.

Festlegen, wie lange Laufhistorien aufbewahrt werden sollen

Sie können die Laufhistorien für eine bestimmte Anzahl von Ausführungen oder für eine bestimmte Anzahl von Tagen oder Monaten beibehalten.

Sie können beispielsweise die Laufhistorien für die zehn letzten Ausführungen (Vorkommen) oder für die letzten zwei Tage oder sechs Monate beibehalten. Sie können auch auswählen, dass alle Laufhistorien beibehalten werden sollen.

Vorbereitende Schritte

Sie müssen Lese-und Schreibberechtigungen für den Eintrag und die Lese-oder Transitberechtigungen für den Ordner, der den Eintrag enthält, haben.

Vorgehensweise

1. Klicken Sie im Menü **Verwalten** auf **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Status** auf **Aktuelle Aktivitäten**, **Anstehende Aktivitäten**oder **Zeitpläne**.
3. Klicken Sie neben dem Eintrag auf den Pfeil, und klicken Sie dann auf **Eigenschaften festlegen** .

   Die Seite mit den Eintragseigenschaften wird angezeigt.
4. Wählen Sie auf der Registerkarte **Allgemein** unter **Protokoll ausführen**die Aufbewahrungsmethode aus, und geben Sie den Wert ein:
   - Um die Ausführungsprotokolle für eine bestimmte Anzahl von Vorkommen beizubehalten, klicken Sie auf **Anzahl Vorkommen** , und geben Sie die Nummer ein. Setzen Sie diesen Wert auf 0, um eine unbegrenzte Anzahl an Laufhistorien zu speichern.
   - Klicken Sie auf **Dauer** , und klicken Sie entweder auf **Tage** oder auf **Monate**, um die Laufhistorien für eine bestimmte Zeit zu halten. Geben Sie den entsprechenden Wert in das Feld ein.

5. Klicken Sie auf **OK**.

Fehler beim erneuten Ausführen einer Task erneut ausführen

Sie können einen fehlgeschlagenen Eintrag erneut übergeben.

Wenn ein Eintrag, wie z. B. ein Bericht, eine Agententask oder ein Job, gemäß einem Zeitplan ausgeführt wird oder im Hintergrund ausgeführt wird und der Fehler fehlschlägt, können Sie den fehlgeschlagenen Eintrag erneut mit denselben Optionen übergeben, die im ursprünglichen Testlauf angegeben wurden.

Für einen Job, der Schritte enthält, die erfolgreich ausgeführt wurden, und Schritte, die nicht erfolgreich ausgeführt wurden, müssen Sie den gesamten Job nicht erneut ausführen, sondern nur die einzelnen Jobschritte ausführen. Wenn die Jobschritte nacheinander ausgeführt werden, können Sie den Job, der mit dem fehlgeschlagenen Jobschritt beginnt, erneut ausführen. Wenn Sie möchten, können Sie auswählen, welche Schritte ausgeführt werden sollen, und die fehlgeschlagenen Schritte überspringen. Die ausgewählten Jobschritte werden jedoch nacheinander ausgeführt, und wenn ein Schritt fehlschlägt, werden die Schritte, die nach dem fehlgeschlagenen Schritt ausgeführt werden, nicht ausgeführt.

Wenn Sie einen Jobabschnitt einzeln erneut ausführen, wird für den übergeordneten Job ein neues Ausführungsprotokoll erstellt, das nur den einzelnen Jobabschnitt enthält. Weitere Informationen zu Laufhistorien finden Sie unter „Anzeigen des Ausführungsprotokolls von Einträgen” auf Seite 266.

Wenn Sie einen Agenteneintrag erneut ausführen, werden auch zugeordnete Tasks, z. B. eine E-Mail, die die Berichtsausgabe an eine Liste von E-Mail-Empfängern sendet, erneut ausgeführt, wenn sie zunächst fehlgeschlagen sind. Wenn zwei zugeordnete Tasks parallel ausgeführt werden und eine Task fehlschlägt und eine Task erfolgreich ausgeführt werden kann, führt die erneute Ausführung des Agenten nur die fehlgeschlagene Task erneut aus. Wenn jedoch Tasks zum Ausführen des Fehlers ausgewählt werden, werden sie erneut ausgeführt, wenn die erneute Ausführung fehlschlägt.

Obwohl das Ausführungsprotokoll Einträge zeigt, die erfolgreich ausgeführt wurden, können Sie einen erfolgreichen Eintrag nicht erneut ausführen. Die Ausführungsoptionen werden für diese Einträge nicht gespeichert.

Eine erneute Ausführung kann fehlschlagen, wenn eine Task, die einem fehlgeschlagenen Eintrag zugeordnet ist, gelöscht oder aktualisiert wird.

Vorbereitende Schritte

Sie müssen über Ausführungsberechtigungen verfügen, um eine fehlgeschlagene Task erneut ausführen zu können.

Vorgehensweise

1. Klicken Sie im Menü **Verwalten** auf **Verwaltungskonsole**.
2. Klicken Sie auf der Registerkarte **Status** auf **Vergangene Aktivitäten**.
3. Klicken Sie neben dem Eintrag auf den Pfeil, und klicken Sie dann auf **Details zum Ausführungsverlauf anzeigen**  .

   Auf der Seite **Details zum Ausführungsverlauf anzeigen** werden Ausführungsdetails angezeigt, wie z. B. Startzeit und Abschlusszeit, Ausführungsstatus und Fehlernachrichten für eine fehlgeschlagene Ausführung. Weitere Informationen, die auf der Seite angezeigt werden, hängen davon ab, ob der Eintrag für eine einzelne Aufgabe, einen Job mit mehreren Schritten oder für einen Agenten mit Aufgaben bestimmt ist. Wenn es sich beispielsweise um eine einzelne Aufgabe handelt, werden die Berichtsoptionen und die Berichtsausgaben angezeigt. Wenn es sich um einen Job mit mehreren Schritten handelt, wird ein Abschnitt **Job** mit den Ausführungsdetails zu den Jobschritten angezeigt.
4. Klicken Sie unter **Status**neben **Fehlgeschlagen**auf **Erneut ausführen**.

   · Wenn es sich bei der erneuten Ausführung um eine einzelne Task handelt, erhalten Sie eine Nachricht, in der Sie aufgefordert werden, die erneute Ausführung zu bestätigen.

- Wenn es sich bei der Wiederholungsaufgabe um einen Job mit mehreren Jobschritten oder um einen Agenten mit Tasks handelt, wird die Seite **Erneut ausführen** angezeigt. Wählen Sie das Kontrollkästchen neben den Einträgen aus, die erneut ausgeführt werden sollen.

Tipp: Sie können fehlgeschlagene Einträge auch erneut ausführen, indem Sie im Bereich "Ausstehend" auf **Erneut ausführen** klicken, um den Abschnitt zu beenden. Wenn Sie einen einzelnen Jobabschnitt erneut ausführen möchten, klicken Sie im Abschnitt 'Job' in der Spalte 'Aktionen' auf die Schaltfläche 'Ausführungsverlaufsdetails der Sicht'  für den fehlgeschlagenen Schritt.

Job zum Planen mehrerer Einträge erstellen

Sie können für mehrere Einträge denselben Zeitplan festlegen, indem Sie einen Job erstellen. Ein Job umfasst eine Sammlung von Berichten, Berichtsansichten und anderen Jobs, für die ein gemeinsamer Zeitplan mit denselben Zeitplaneinstellungen erstellt wird. Wenn ein geplanter Job ausgeführt wird, werden sämtliche Einträge in diesem Job ausgeführt.

Wenn ein Jobelement nicht verfügbar ist, können Sie eine andere Verknüpfung auswählen, indem Sie auf **Mit einem Eintrag verknüpfen** klicken.

Jobs bestehen aus Einzelschritten, die sich auf einzelne Berichte, Jobs und Berichtsansichten beziehen. Sie können angeben, ob die Einzelschritte gleichzeitig oder nacheinander ausgeführt werden sollen.

- Wenn Schritte gleichzeitig ausgeführt werden, bedeutet das, dass sie alle auf einmal übergeben werden. Der Job gilt als erfolgreich ausgeführt, wenn alle Schritte ausgeführt wurden. Wenn bei einem Schritt ein Fehler auftritt, werden die anderen Schritte dennoch ausgeführt, aber der Job erhält den Status **Fehlgeschlagen**.
- Werden die Schritte nacheinander ausgeführt, können Sie die Ausführungsreihenfolge angeben. Ein Schritt wird erst dann übermittelt, wenn der vorherige Schritt erfolgreich ausgeführt wurde. Wenn bei einem Schritt ein Fehler auftritt, können Sie auswählen, ob der Job abgebrochen werden soll oder ob die anderen Schritte fortgesetzt werden.

Sie können die Ausführung eines Jobs planen, indem Sie einen einmaligen Termin, einen regelmäßigen Termin oder ein auslösendes Ereignis wie eine Datenbankaktualisierung oder eine E-Mail festlegen. Weitere Informationen finden Sie im Abschnitt „Trigger-basierte Eintragsplanung“ auf Seite 272.

Den einzelnen Berichten, Jobs und Berichtsansichten in den jeweiligen Schritten können auch individuelle Zeitpläne zugeordnet sein. Ausführungsoptionen für einzelne Schritteinträge überschreiben die für den Job festgelegten Ausführungsoptionen. Sie können Ausführungsoptionen für den Job angeben, die als Standardeinstellung für die Schritteinträge verwendet werden, die über keine eigenen Ausführungsoptionen verfügen.

Sie können Berichte ausführen, um Ausgaben basierend auf den von Ihnen definierten Optionen, z. B. Format, Sprache und Eingabehilfen, zu erstellen.

Die Berechtigungen, die zum Hinzufügen eines Eintrags zu einem Job erforderlich sind, variieren in Abhängigkeit vom Eintragstyp. Die Berechtigungen entsprechen den Berechtigungen für das zeitliche Planen eines Eintrags. Weitere Informationen finden Sie unter „Bericht planen“ auf Seite 247.

Vorgehensweise

1. Klicken Sie in der Anwendungsleiste auf das + und dann auf .

   Die Seite **Schritte** wird angezeigt.

2. Klicken Sie auf das Symbol **Jobschritt hinzufügen**,  .
3. Wählen Sie Berichte aus, die im Job enthalten sein sollen.
   a) Navigieren Sie zu einem Ordner, der die gewünschten Berichte enthält.
   b) Wählen Sie Kontrollkästchen für einen oder mehrere Berichte aus.

      Tipps:

- Klicken Sie mit gedrückter Strg-Taste, um mehrere Kontrollkästchen auszuwählen.
- Verwenden Sie die Links **Alle in Ordner auswählen** und **Alle in Ordner abwählen**, und klicken Sie dann bei gedrückter Strg-Taste auf Kontrollkästchen, um die Auswahl in einem Ordner schnell abzuschließen.
- Klicken Sie auf **Jobschritte hinzufügen**.

c) Wiederholen Sie die Schritte „3.a" auf Seite 269 und „3.b" auf Seite 269, um Berichte in anderen Ordnern auszuwählen.

Im Fenster **Schritte** werden die Schritte aufgeführt, die für Ihren Job definiert sind. Jeder Schritteintrag zeigt Folgendes an:

- Der Name eines Berichts, den Sie ausgewählt haben.

  Tipp: Bewegen Sie den Mauszeiger über den Berichtsnamen, um den Navigationspfad zur Berichtsposition anzuzeigen.
- Ob die Schrittoptionen durch den Bericht definiert werden oder angepasst sind

4. So ändern Sie die aktuellen Schrittoptionen für einen beliebigen Schritt in Ihrem Job:
   a) Klicken Sie für den Schritt, den Sie ändern möchten, auf das Symbol "Optionen bearbeiten"  .
   b) Bearbeiten Sie die Option **Format**, **Barrierefreiheit**, **Zielgruppenverteilung**, **Zustellung**, **Sprachen** oder **Eingabeaufforderung**.
   c) Klicken Sie auf **Schließen**.
5. So ändern Sie die Standardlaufoptionen für zukünftige Schritte:
   a) Wählen Sie **Standardschrittoptionen ändern** aus.
   b) Bearbeiten Sie die Option für **Format**, **Barrierefreiheit**, Zielgruppenverteilung, **Zustellung**, Eingabeaufforderungen oder **Sprachen**.
   c) Klicken Sie auf **Schließen**.
6. Wenn Sie einen Schritt entfernen möchten, bewegen Sie den Mauszeiger über den Schritt, und klicken Sie dann auf das Symbol "Jobschritt entfernen"  .
7. Wählen Sie unter **Ausführungsreihenfolge** die Option **Alle auf einmal ausführen** oder **Nacheinander ausführen** für die Ausführung der Schritte aus.
   - Wenn Sie die Option **Nacheinander ausführen** auswählen, werden die Schritte in der Reihenfolge ausgeführt, in der sie in der Liste **Schritte** angezeigt werden.
   - Wenn die Option **Alle auf einmal ausführen** abgeblendet ist, hat Ihr Administrator diese Option inaktiviert.

     Weitere Informationen hierzu finden Sie im Abschnitt zum "Inaktivieren der Option 'Alle auf einmal ausführen' in Jobs" im Handbuch 'Cognos Analytics - Verwaltung'.
   - Wenn die Ausführung eines Jobs auch dann fortgesetzt werden soll, wenn einer der Schritte fehlschlägt, aktivieren Sie das Kontrollkästchen **Bei Fehler fortsetzen**.

   Tipp: Sie können zum Ändern der Reihenfolge der Schritte auf einen Schritt klicken und ihn an die gewünschte Position ziehen.
8. Klicken Sie in der Anwendungsleiste auf das Symbol zum Speichern  .
9. Navigieren Sie zu einem Ordner, in dem der Job gespeichert werden soll, geben Sie einen Jobnamen im Feld **Speichern unter** an und klicken Sie anschließend auf **Speichern**.

   Im Abschnitt **Ausführungsoptionen** werden die Links **Jetzt ausführen** und **Zeitplan** angezeigt.
10. Wenn der Bericht sofort ausgeführt werden soll, klicken Sie auf **Jetzt ausführen** und anschließend auf **Fertigstellen**.
11. Wenn Sie die wiederholte Ausführung planen möchten, führen Sie die folgenden Schritte aus:
    a) Klicken Sie auf **Zeitplan**.
    b) Klicken Sie auf **Neu**.

c) Geben Sie die Details zum Zeitpunkt der gewünschten Jobausführung ein.

d) Klicken Sie auf **Erstellen**.

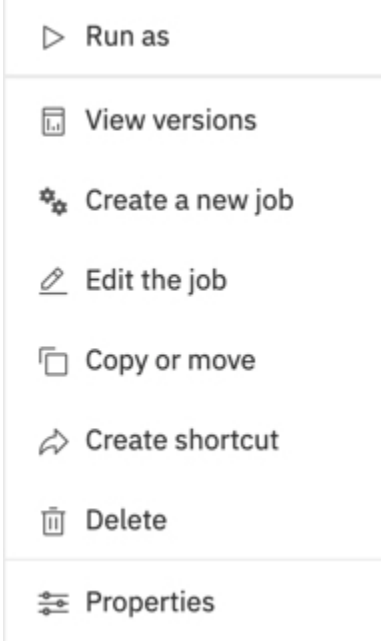
Tipp: Falls die Nachricht "Für die Ausführung dieser Operation sind Ihre Berechtigungsnachweise erforderlich" angezeigt wird, klicken Sie auf **Erneuern** und geben Sie anschließend Ihre Cognos Analytics-Benutzer-ID und das zugehörige Kennwort ein.

Ergebnisse

In dem von Ihnen ausgewählten Ordner wird ein Job erstellt, mit dem Jobsymbol gekennzeichnet und zum nächsten geplanten Zeitpunkt ausgeführt.

Nächste Schritte

Wenn Sie für den von Ihnen erstellten Job auf das Symbol 'Mehr' klicken, können Sie Operationen aus dem nachfolgenden Menü auswählen:



Zwischengespeicherte Eingabeaufforderungsdaten

Für Berichte, bei denen jedes Mal, wenn der Bericht ausgeführt wird, für Werte angezeigt wird, können Sie zwischengespeicherte Eingabeaufforderungsdaten verwenden. Berichte werden schneller ausgeführt, da Daten aus dem Cache und nicht aus der Datenbank abgerufen werden.

Der Cache wird nur verwendet, wenn eine angeforderte Sprache die gleiche wie eine im Cache ist. Der Cache enthält beispielsweise Daten für Englisch, Englisch (Vereinigte Staaten) und Deutsch (Deutschland). Wenn Sie dazu aufgefordert werden, fordern Sie Englisch (Vereinigte Staaten) für den Bericht an. Es gibt eine exakte Übereinstimmung, und die zwischengespeicherten Daten werden verwendet. Die zwischengespeicherten Daten werden auch verwendet, wenn eine Teilübereinstimmung vorhanden ist. Wenn Sie Englisch (Kanada) anfordern, werden die zwischengespeicherten Daten für Englisch verwendet. Wenn Sie Deutsch (Österreich) anfordern, gibt es keine Übereinstimmung, und die zwischengespeicherten Daten werden nicht verwendet.

Sie können Caches für Berichte oder Berichtsansichten verwenden. Für Berichtsansichten wird zuerst der Cache für die Berichtsansicht verwendet. Wenn kein Cache für Berichtsansichten gefunden wird, wird der Cache für den zugehörigen Bericht verwendet.

Sie müssen einen Job verwenden, um einen Cache zu erstellen oder zu aktualisieren. Sie können den Cache automatisch aktualisieren, indem Sie den Job so planen, dass er regelmäßig ausgeführt wird. Wenn

Sie die Live-Daten beim nächsten Ausführen des Berichts verwenden möchten, können Sie den Cache löschen.

Trigger-basierte Eintragsplanung

Sie können Einträge, die auf einem Vorkommen basieren, wie z. B. eine Datenbankaktualisierung oder eine E-Mail, planen. Das Vorkommen wirkt als Auslöser und führt dazu, dass der Eintrag ausgeführt wird. Sie können beispielsweise jedes Mal, wenn eine Datenbank aktualisiert wird, einen Bericht ausführen.

Die Trigger-basierte Terminierung kann verwendet werden, um Einträge automatisch basierend auf einem Vorkommen auszuführen. Es kann auch verwendet werden, um zu begrenzen, wenn Benutzer Einträge ausführen können. Beispiel: In einer Data-Warehouse-Umgebung, in der die Datenbank nur einmal pro Woche aktualisiert wird, ist es nicht mehr erforderlich, Berichte häufiger auszuführen.

Sie können den Bericht basierend auf der Datenbankaktualisierung so planen, dass der Bericht nur einmal pro Woche ausgeführt wird.

Die Trigger-basierte Terminierung gilt nur für den Eintrag und nicht für die ihm zugeordnete Eintragsansicht. Wenn z. B. eine triggerbasierte Terminierung für einen Bericht gilt, gilt dies nicht für Berichtsansichten, die dem Bericht zugeordnet sind. Sie können jedoch eine Berichtsansicht mithilfe eines Auslösers planen.

In **IBM Cognos Administration**können Sie den Zugriff auf die Terminierung durch Auslöser mithilfe der Funktion **Zeitplan nach Auslöser** steuern.

Auslöserbasierte Zeitplanung einrichten

Um einen Eintrag auf der Basis eines Auftretens zu planen und eine Trigger-basierte Terminierung zu bestätigen, müssen Sie Lese-, Schreib-, Ausführungs-und Transitberechtigungen haben.

Zum Planen von Berichten, die in den CSV-, PDF-, Microsoft -(XLS) oder XML-Ausgabeformaten ausgeführt werden sollen, benötigen Sie die Funktion zur Generierung der Ausgabe für das bestimmte Format. Weitere Informationen finden Sie unter „Berichtsformate“ auf Seite 367.

Sie benötigen außerdem die folgenden Zugriffsberechtigungen für alle Datenquellen, die vom Eintrag verwendet werden.

Tabelle 68. Datenquellen und Berechtigungen, die für eine Trigger-basierte Terminierung erforderlich sind

Datenquelle	**Berechtigungen**
Datenquelle	Ausführen und Traverse
dataSourceConnection	Ausführen und Traverse Wenn Sie nur den Zugriff ausführen, werden Sie aufgefordert, sich bei der Datenbank anzumelden.
dataSourceSignon	Ausführen

Bevor Sie eine Trigger-basierte Terminierung einrichten, stellen Sie sicher, dass Ihre Berechtigungsnachweise vorhanden sind und auf dem neuesten Stand sind.

Tipp: Klicken Sie auf die Schaltfläche 'Meine Bereichsoptionen'  , **Eigene Vorgaben**und klicken Sie auf der Registerkarte **Personal** auf **Berechtigungsnachweise erneuern**.

Führen Sie den folgenden Prozess aus, um eine Trigger-basierte Terminierung zu konfigurieren:

- „Eintrag basierend auf einem Vorkommen planen“ auf Seite 274.
- Auslöservorkommen auf einem Server konfigurieren.

Trigger-Vorkommen können auch von einem Software Development Kit-Entwickler mit dem IBM Cognos Software Development Kit konfiguriert werden. Weitere Informationen finden Sie im *Software Development Kit-Entwicklerhandbuch*.

Trigger-Vorkommen auf einem Server einrichten

Im Rahmen der Einrichtung einer auslösebasierten Berichtszeitplanung müssen Sie das Auftreten des Auslösers auf einem Server einrichten.

Sie verknüpfen das externe Vorkommen, wie z. B. eine Datenbankaktualisierung oder eine E-Mail, mit einem Auslöser auf dem Server, der die Ausführung des Eintrags bewirkt. Sie müssen auch den Namen des Vorkommens angeben.

Trigger-Vorkommen können auch von einem Software Development Kit-Entwickler mit dem Software-Development-Kit von IBM Cognos konfiguriert werden. Weitere Informationen finden Sie im *IBM Cognos Software Development Kit Developer Guide*.

Mit dem Script "trigger.bat" von Microsoft Fenster oder mit dem Shell-Script "trigger.sh" können Sie einen oder mehrere Zeitpläne für die Ausführung auf dem Server auslösen. Die Scriptsyntax folgt, wenn URL die URL des IBM Cognos -Servers ist, `Benutzername` ein gültiger Benutzername im angegebenen Namespace ist, `Kennwort` das Kennwort für den Benutzernamen, `Namensbereich` der Namensbereich für den Benutzernamen und `Triggerliste` eine durch Kommas getrennte Liste mit Auslösernamen ist:

```
trigger.bat URL [username password namespace]
triggerlist
```

Wenn Benutzer beispielsweise einen Bericht auf der Basis einer Datenbankaktualisierung planen und einen zweiten Bericht auf der Basis des Empfangs einer E-Mail terminieren möchten, sieht Ihre angepasste Auslöserbefehlszeile möglicherweise ähnlich wie folgt aus:

```
trigger.bat http://localhost:9300/p2pd/servlet/dispatch username
password namespace databaserefreshtriggername,emailtriggername
```

Vorgehensweise

1. Wenn Sie ein Auslöserereignis auf einem anderen Server als einem IBM Cognos -Server einrichten, führen Sie die folgenden Tasks aus:
   - Stellen Sie sicher, dass der Server über eine unterstützte Version von Java Runtime Environment oder ein Java Development Kit verfügt.
   - Kopieren Sie die folgenden Dateien aus dem Verzeichnis *cognos_analytics_installation_location*/webapps/p2pd/WEB-INF/lib auf einem IBM Cognos -Server in die Position auf dem Server, auf dem Sie das Auslöserereignis einrichten:

     activation.jar

     axis.jar

     axisCrnpClient.jar

     commons-discovery-0.2.jar

     commons-logging-1.1.jar

     commons-logging-adapters-1.1.jar

     commons-logging-api-1.1.jar

     jaxrpc.jar

     saaj.jar

     wsdl4j-1.5.1.jar

- Kopieren Sie `mail.jar` von *cognos_analytics_installation_location*/bin64 auf einem IBM Cognos -Server an die Position auf dem Server, auf dem Sie das Auslöserereignis konfigurieren.
- Kopieren Sie die folgenden Dateien aus dem *cognos_analytics_installation_location*/webapps/utilities/trigger auf einem IBM Cognos -Server an die Position auf dem Server, auf dem Sie das Auslöserereignis einrichten:

  trigger.bat

  trigger.sh

  trigger.class (a Java utility that can run on any IBM Cognos-supported platform)

2. Stellen Sie sicher, dass die Befehlszeile ausgeführt wird, wenn das externe Vorkommen, wie z. B. eine Datenbankaktualisierung oder eine E-Mail, auftritt.

   Der Mechanismus, den Sie zum Aufrufen Ihres angepassten Auslöserbefehls verwenden, hängt von der Anwendung ab, mit der Sie arbeiten, wie z. B. ein Datenbanksystem oder eine E-Mail-Anwendung. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Anwendung.
3. Informieren Sie die Benutzer darüber, dass sie jetzt Einträge basierend auf dem Auslöserereignis planen können.

   Wenn ein Benutzer einen Eintrag auf der Basis des Auftretens terminiert, wenn der Benutzer auf die Zeitplanschaltfläche für eine Berichtsansicht klickt, werden Informationen zum Vorkommen auf der **Zeitplan** -Seite ersetzt.

Ergebnisse

Nachdem das Script ausgeführt wurde, gibt die Auslösermethode einen ganzzahligen Wert zurück, der die Anzahl der ausgeführten Zeitpläne darstellt. Die folgenden Ganzzahlen stellen Fehler dar:

- -1 ist ein Syntaxfehler, wie z. B. ein ungültiger Parameter oder eine ungültige Syntax.
- -2 ist ein Kommunikationsproblem mit IBM Cognos -Server

Eintrag basierend auf einem Vorkommen planen

Im Rahmen der Einrichtung einer Triggern-basierten Terminierung müssen Sie einen Eintrag auf der Basis eines Vorkommens planen.

Der Trigger-basierte Zeitplan wird aktiviert, wenn der Benutzer, der den Auslöser abfeuert, Folgendes hat

- Lese-und Transitberechtigungen für den Zeitplaneintrag
- Traversenberechtigungen für alle Vorfahren des Zeitplaneintrags
- Zugriff auf IBM Cognos Administration

Zum Planen von Berichten, die in den CSV-, PDF-, Microsoft -(XLS) oder XML-Ausgabeformaten ausgeführt werden sollen, benötigen Sie die Funktion zur Generierung der Ausgabe für das bestimmte Format. Weitere Informationen finden Sie unter „Berichtsformate“ auf Seite 367.

Vorbereitende Schritte

Wenn sie von einem Auslöser geplant wird, kann ein Bericht nur ausgeführt werden, wenn Sie bereits ein Auslöserereignis eingerichtet haben. Weitere Informationen finden Sie unter „Trigger-Vorkommen auf einem Server einrichten“ auf Seite 273.

Vorgehensweise

1. Klicken Sie auf die Schaltfläche "Mehr"  für den Eintrag, den Sie planen möchten.
2. Klicken Sie auf  **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Zeitplan** .
4. Klicken Sie auf  **Neu**.

5. Klicken Sie in der Anzeige **Zeitplan erstellen** auf das schwarze Dreieck im Feld **Zeitplan** , und klicken Sie anschließend auf **Nach Auslöser**.
6. Geben Sie in das Feld **Triggername** den Namen des Auslöservorkommens ein.

   Hinweis: Der Triggername, den Sie eingeben, kann Ihnen von Ihrem Administrator oder Ihrem Entwickler zur Verfügung gestellt werden. Wenn dies nicht der Fall ist, müssen Sie Ihren Administrator oder Entwickler über den von Ihnen verwendeten Triggernamen informieren.
7. Legen Sie die Start-und Endzeit des **Zeitraum** s fest, während dessen ein Auslöser den Zeitplan für die Ausführung des Zeitplans verursacht.

   Tipp: Der Auslöserzeitplan wird ausgeführt, wenn der Auslöser (entweder aus trigger.bat oder aus einer Software-Development-Kit-Anwendung) zwischen dem Start-und dem Enddatum ausgelöst wird.
8. Klicken Sie auf **Erstellen**.

Kapitel 18. Zeitplanmanagement

Sie können IBM Cognos-Einträge mittels eines Zeitplans so planen, dass sie zu einem für Sie günstigen Zeitpunkt ausgeführt werden. Es empfiehlt sich beispielsweise, Berichte oder Agenten außerhalb der Arbeitszeit auszuführen, wenn die Belastung des Systems gering ist. Außerdem können Sie sie in regelmäßigen Intervallen jede Woche oder jeden Monat ausführen.

Um diese Funktion zu nutzen, müssen Sie in **IBM Cognos Administration** über die erforderlichen Berechtigungen für die geschützte Funktion **Zeitplan** verfügen.

Um die Ausführung von Berichten in den Ausgabeformaten CSV (Text mit Trennzeichen), PDF, XLS (Microsoft Excel-Arbeitsblatt) oder XML planen zu können, benötigen Sie die Berechtigung zum Generieren von Ausgabe für das jeweilige Format. Weitere Informationen finden Sie in „Berichtsformate" auf Seite 367. Sie können einen vorhandenen Zeitplan aktualisieren, der Formate angibt, die nicht ausgeführt werden sollen. Sie können allerdings keine Formate in den Zeitplan einführen, die nicht ausgeführt werden sollen.

In **IBM Cognos Administration** können Sie Zeitpläne nach Tag, Woche, Monat und Jahr steuern und die Zeitplanung mit der entsprechenden Funktion auslösen. Sie können die Zeitplanung auch innerhalb eines Tages durch Verwendung der Funktionen **Zeitplan nach Minuten** und **Zeitplan nach Stunden** einschränken (siehe Kapitel 13, „Funktionen", auf Seite 207).

Wenn Sie über Administratorberechtigungen verfügen, können Sie auch Aufgaben für folgende Zwecke planen:

- Verwalten des Content Stores (siehe „Wartungstasks für Content-Store" auf Seite 60)
- Planen von Caching-Aufgaben für Abfrageservices (siehe „Administrationsaufgaben für Abfrageservices erstellen und planen" auf Seite 162)
- Importieren von Einträgen aus einem Bereitstellungsarchiv oder Exportieren in ein Bereitstellungsarchiv (siehe Kapitel 19, „Implementierung", auf Seite 299)
- Ausführen von Jobs (siehe „Job zum Planen mehrerer Einträge erstellen" auf Seite 269)
- Ausführen der Metrikverwaltung (siehe Kapitel 4, „Systemleistungsmetriken", auf Seite 25)

Sie können Einträge so planen, dass sie in festgelegten Intervallen ausgeführt werden. Sie können für einzelne Einträge einen Zeitplan festlegen oder Sie können mithilfe von Jobs einen Zeitplan für mehrere Einträge festlegen. Jobs verfügen über eigene Zeitpläne, die von den Berichtszeitplänen unabhängig sind.

Sie können Einträge so planen, dass sie am letzten Tag jeden Monats ausgeführt werden. Sie können die Ausführung eines Eintrags auch auf Basis eines Ereignisses wie einer Datenbankaktualisierung oder einer E-Mail planen.

Sie können Berichte ausführen, um Ausgaben basierend auf den von Ihnen definierten Optionen, z. B. Format, Sprache und Eingabehilfen, zu erstellen.

Jedem Eintrag kann jeweils nur ein Zeitplan zugeordnet werden. Wenn Sie mehrere Zeitpläne für einen Bericht oder einen Agenteneintrag benötigen, können Sie Berichtsansichten oder Agentenansichten erstellen und anschließend für jede Ansicht einen Zeitplan erstellen.

Nachdem Sie einen Zeitplan erstellt haben, wird der Eintrag oder der Job am entsprechenden Datum und zu der angegebenen Uhrzeit ausgeführt. Anschließend können Sie die geplanten Einträge anzeigen und verwalten. Weitere Informationen finden Sie in Kapitel 17, „Zeitpläne und Aktivitäten", auf Seite 247.

Berechtigungsnachweise für geplante Einträge

Wenn Sie einen geplanten Eintrag öffnen, wird in den Berechtigungsnachweise der aktuelle Eigentümer des Zeitplans angezeigt. Wenn Sie noch nicht der Eigentümer des Zeitplans sind, können Sie dies selbst festlegen (siehe „Beispiel-Die Berechtigungsnachweise für einen Zeitplan ändern" auf Seite 290).

Berechtigungsnachweise für einen Zeitplan werden bei Änderung eines Zeitplans nicht automatisch geändert. Die Berechtigungsnachweise müssen explizit geändert werden.

Informationen zu Datenquellen-Berechtigungsnachweise finden Sie in „Vertrauenswürdige Berechtigungsnachweise" auf Seite 202.

Eingabeaufforderungen in geplanten Einträgen

Wenn ein Eintrag geplant wird, der Eingabeaufforderungen enthält, müssen Sie die Werte für die Eingabeaufforderungen speichern oder Standardwerte angeben (siehe „Geben Sie die Standardaufforderungswerte für einen Bericht an." auf Seite 369), damit bei der planmäßigen Ausführung Werte vorhanden sind.

Bei einem Job können Sie Eingabeaufforderungswerte für die Einzelschritte des Jobs angeben. Wenn ein Eintrag als Teil eines Jobs ausgeführt wird, werden die in der Jobdefinition gespeicherten Eingabeaufforderungswerte anstelle der im Eintrag gespeicherten Werte verwendet. Wenn in der Jobdefinition keine Werte angegeben sind, werden in IBM Cognos die im Eintrag gespeicherten Werte verwendet.

Priorität für geplante Einträge

Beim Planen von Einträgen können Sie u. U. eine Ausführungspriorität von 1 bis 5 auswählen. Wenn mehr als ein Eintrag über eine bestimmte Priorität verfügt, wird zuerst der Eintrag ausgeführt, der sich zuerst in der Warteschlange befunden hat. Der Standardwert ist 3. Wenn Sie nicht berechtigt sind, Eintragsprioritäten festzulegen, wird die Priorität zwar angezeigt, kann von Ihnen aber nicht geändert werden.

Beim Planen eines Jobs können Sie die Priorität nicht für einzelne Einträge innerhalb des Jobs festlegen, sondern nur für den gesamten Job. Sie können jedoch die Priorität einzelner Einträge ändern, wenn sich diese in der Warteschlange befinden.

Die Priorität der Einträge in der Warteschlange hat keinen Einfluss auf einen bereits ausgeführten Eintrag. Der ausgeführte Eintrag wird abgeschlossen und anhand der Warteschlangenpriorität der nächste auszuführende Eintrag ausgewählt.

Weitere Informationen finden Sie in „Priorität für die Eintragsausführung ändern" auf Seite 258.

Ausführungsverlaufsdaten für geplante Einträge

IBM Cognos speichert Verlaufsinformationen jedes Mal, wenn ein geplanter Eintrag ausgeführt wird. Dem Ausführungsverlauf können Sie entnehmen, zu welchen Zeiten und wie erfolgreich ein Eintrag ausgeführt wurde. Weitere Informationen finden Sie in „Anzeigen des Ausführungsprotokolls von Einträgen" auf Seite 266.

Bericht planen

11.1.7 Sie planen einen Bericht, um ihn zu einem späteren Zeitpunkt oder zu einem wiederkehrenden Datum und zu einem wiederkehrenden Zeitpunkt auszuführen.

Wenn Sie einen Zeitplan nicht mehr benötigen, können Sie ihn löschen. Sie können sie auch inaktivieren, ohne die Planungsdetails zu verlieren. Anschließend können Sie den Zeitplan zu einem späteren Zeitpunkt aktivieren.

Wenn Sie möchten, können Sie den aktuellen Zeitplaneigner ändern, indem Sie die Berechtigungsnachweise für einen geplanten Eintrag ändern. Weitere Informationen finden Sie im Artikel "Eigentumsrecht an einem Zeitplan übernehmen" in der *Benutzerhandbuch verwalten*.

Vorbereitende Schritte

Um diese Funktionalität zu verwenden, müssen Sie über die erforderlichen Berechtigungen für die Funktionalität von **Planung** verfügen. Sie können sehen, welche Funktionen mit der zugeordneten

Lizenzrolle im Thema "Standardberechtigungen auf der Basis von Lizenzen" in der *Benutzerhandbuch verwalten*verfügbar sind.

Um einen Bericht zu planen, benötigen Sie außerdem die folgenden Zugriffsberechtigungen für alle Datenquellen, die im Bericht verwendet werden:

- dataSource-Ausführen und Traverse
- dataSourceConnection-Ausführen und Traverse

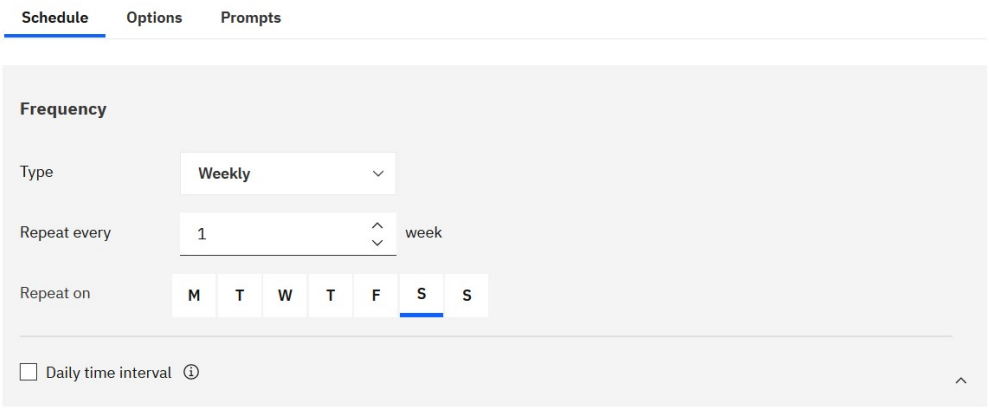
  Wenn Sie nur den Zugriff ausführen, werden Sie aufgefordert, sich bei der Datenbank anzumelden.
- dataSourceSignon-Ausführen

Zum Planen von Berichten, die in den eingeschränkten CVS-, PDF-, XLS-oder XML-Ausgabeformaten ausgeführt werden sollen, benötigen Sie die Generierung der Ausgabefunktion für das bestimmte Format. Weitere Informationen finden Sie im Artikel *Berichtsformate* in der *Verwaltung und Sicherheit*.

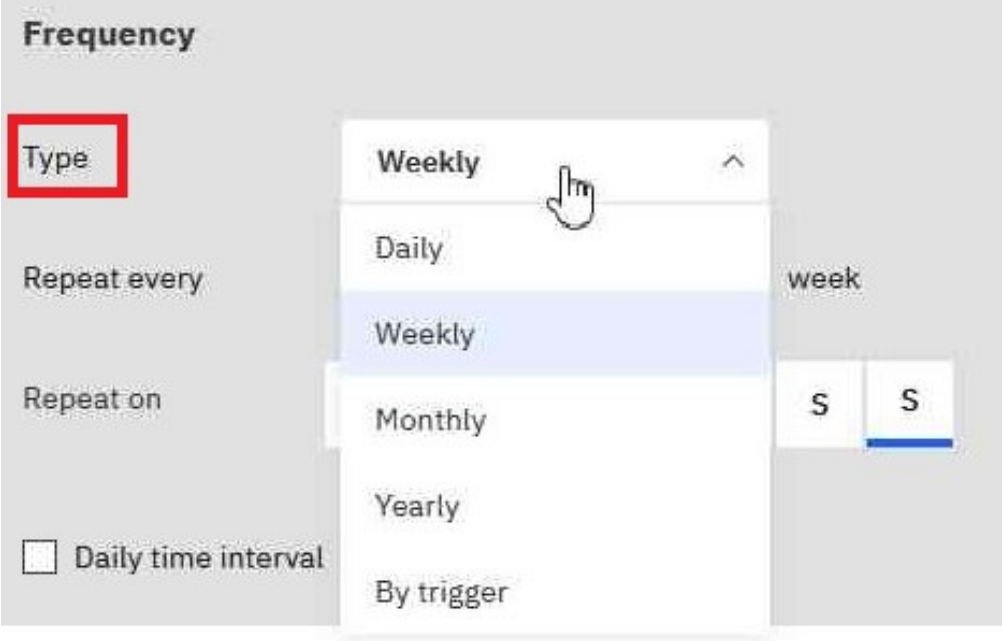
Um die Priorität für einen Eintrag festlegen zu können, müssen Sie über die erforderlichen Berechtigungen für das gesicherte Feature **Terminierungspriorität** verfügen. Weitere Informationen finden Sie unter Funktionen ..

Vorgehensweise

1. Klicken Sie auf das Symbol 'Mehr' ..., und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie im Teilfenster **Eigenschaften** auf die Registerkarte **Zeitplan** und anschließend:
   - Klicken Sie auf **Zeitplan erstellen**.

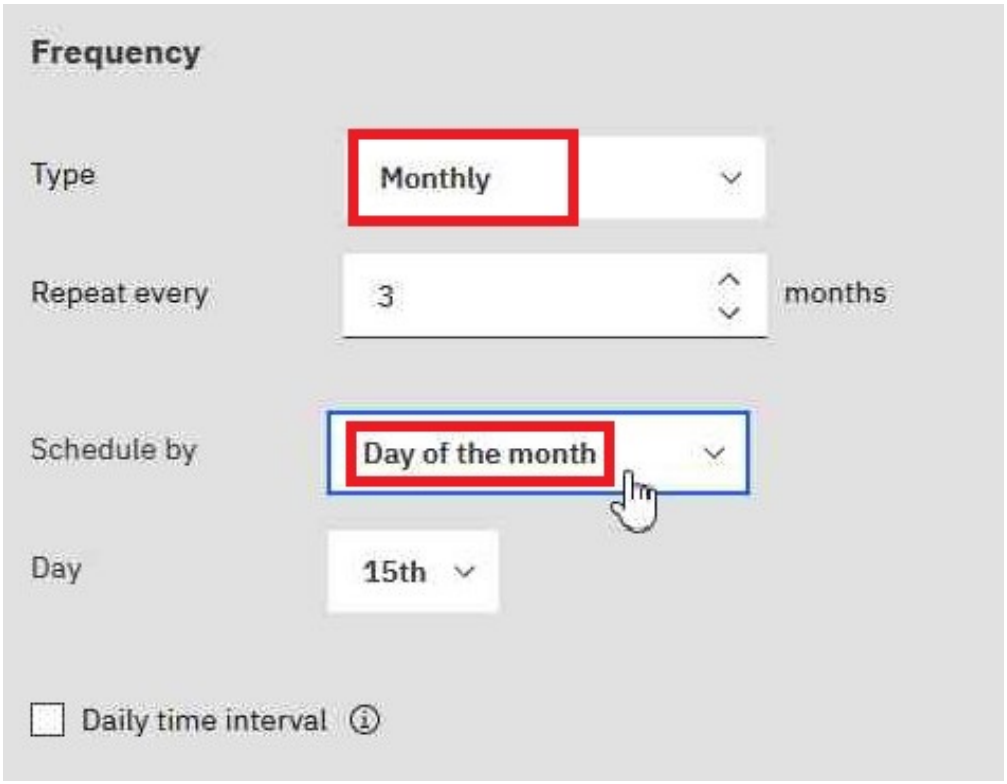


     Tipp: Die verfügbaren Optionen ändern sich bei jeder Auswahl. Warten Sie, bis das Teilfenster aktualisiert wird, bevor Sie weitere Einstellungen auswählen.
3. Geben Sie im Abschnitt **Häufigkeit** an, wann und wie häufig der Bericht ausgeführt wird:
   - Wählen Sie das **Typ** der Zeiteinheit aus, um das Intervall zwischen Besprechungen zu messen.



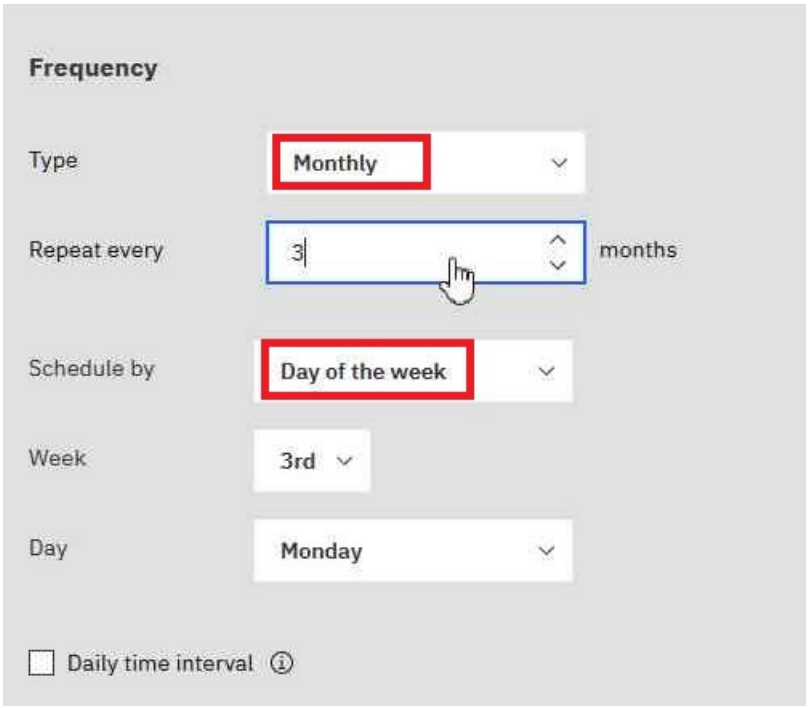
Tipp: Versuchen Sie, verschiedene **Typ** -Werte auszuwählen, und beobachten Sie dann, wie sich die anderen Felder ändern. Wenn Sie beispielsweise **Täglich**, **Wöchentlich**oder **Monatlich** auswählen, können Sie eine **Wiederholen Sie alle** *Ganze Zahl*auswählen. Sie können daher ein Intervall auswählen, bei dem es sich um ein Vielfaches der von Ihnen ausgewählten Zeiteinheit handelt, z. B. "alle 3 Wochen".

- Wenn Sie einen **Typ** -Wert von **Monatlich**auswählen,



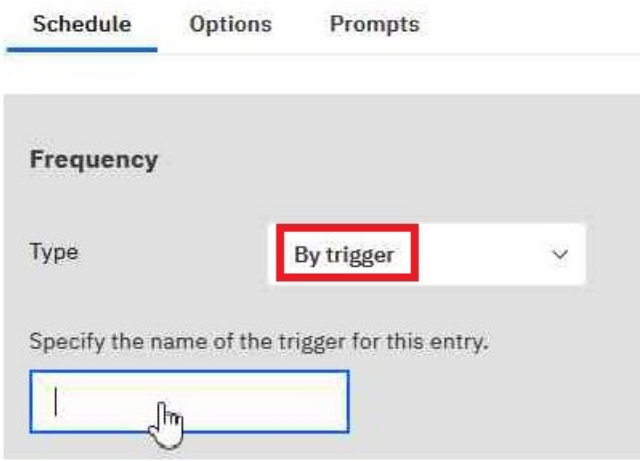
–

Wählen Sie **Tag des Monats** im Feld **Planen nach** aus, damit Sie z. B. "Wiederholung alle 3 Monate am 15. des Monats" auswählen können (siehe Abbildung oben).



– Wählen Sie **Tag der Woche** im Feld **Planen nach** aus, damit Sie z. B. "Wiederholung alle 3 Monate am 3. Montag des Monats" auswählen können (siehe Abbildung oben).

· Wenn Sie einen **Typ** -Wert von **Nach Auslöser**auswählen,



Tipp: Wenn ein Bericht von einem Auslöser geplant wird, kann er nur ausgeführt werden, wenn Sie bereits ein Auslöserereignis eingerichtet haben. Weitere Informationen finden Sie unter "Trigger-Vorkommen auf einem Server einrichten" in der *Verwaltung und Sicherheit* ..

Geben Sie in dem oben dargestellten Feld den Namen des Auslöservorkommens ein, z. B. `trigger.bat`.

4. Wenn Sie eine tägliche Frequenz für Ihre geplanten Einträge auswählen möchten, gehen Sie wie folgt vor:

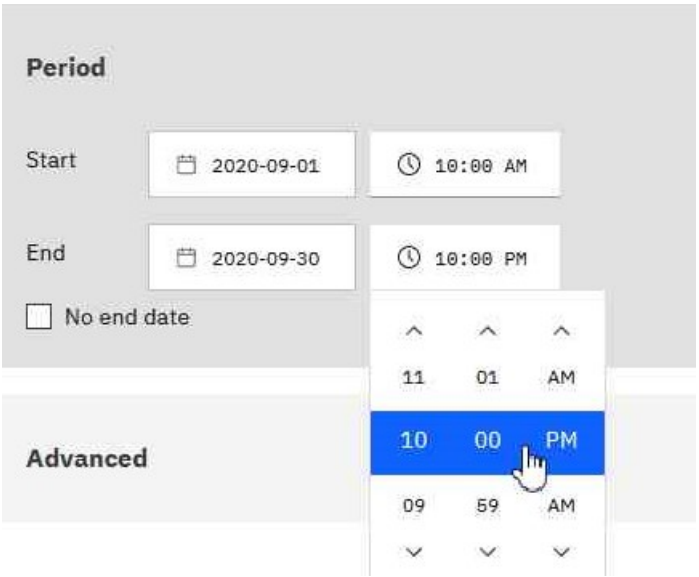
   · Wählen Sie das Markierungsfeld **Tägliches Zeitintervall** aus.

Tipp: Geben Sie die Häufigkeit und den Zeitraum während des Tages an, in dem der Bericht ausgeführt wird. Beispiel: "alle 2 Stunden zwischen 10:00 und 22:00 Uhr" (siehe Abbildung oben).

Es wird empfohlen, eine stündliche Frequenz auszuwählen, die gleichmäßig in die 24-Stunden-Uhr unterteilt wird. Auf diese Weise wird sichergestellt, dass Ihr Bericht jeden Tag zur selben Zeit ausgeführt wird. Wenn Sie eine stündliche Frequenz auswählen, die nicht gleichmäßig in die 24-Stunden-Uhr aufgeteilt wird, wird Ihr Bericht in den folgenden Tagen zu verschiedenen Zeiten ausgeführt.

5. Wenn Sie den Zeitraum festlegen möchten, innerhalb dessen die ersten und letzten Ausführungen des Berichts ausgeführt werden sollen, gehen Sie wie folgt vor:

   · Blättern Sie zum Abschnitt **Zeitraum** .



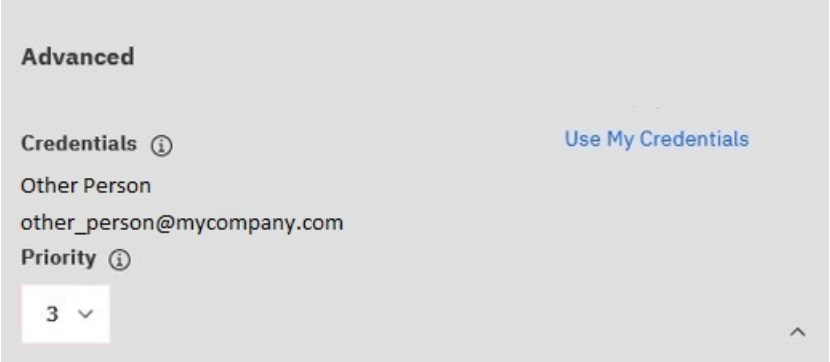
Tipp: Im obigen Beispiel wird der erste Berichtslauf am 1. September um 10:00 Uhr stattfinden, und der letzte Berichtslauf endet am 30. September um 22:00 Uhr.

Legen Sie das Datum und die Uhrzeit für den Beginn und das Ende der Periode fest.

Wenn Sie im Abschnitt **Zeitraum** nichts eingeben, beginnt der Zeitraum standardmäßig, sobald Sie den Zeitplan speichern, und es ist kein Enddatum vorhanden.

6. Gehen Sie wie folgt vor, wenn Sie die Berechtigungsnachweise oder die Priorität des Zeitplans ändern möchten:

   · Klicken Sie auf den Abschnitt **Erweitert** .



Tipp:

Informationen zum Feld 'Berechtigungsnachweise'

Die Berechtigungsnachweise zeigen den aktuellen Zeitplaneigner an. Wenn Sie nicht bereits der Zeitplaneigner sind, können Sie auf **Eigene Berechtigungsnachweise verwenden** klicken und temporäre Änderungen an dem Zeitplan vornehmen.

Weitere Informationen finden Sie im Artikel " Eigentumsrecht an einem Zeitplan übernehmen" in der *Benutzerhandbuch verwalten*.

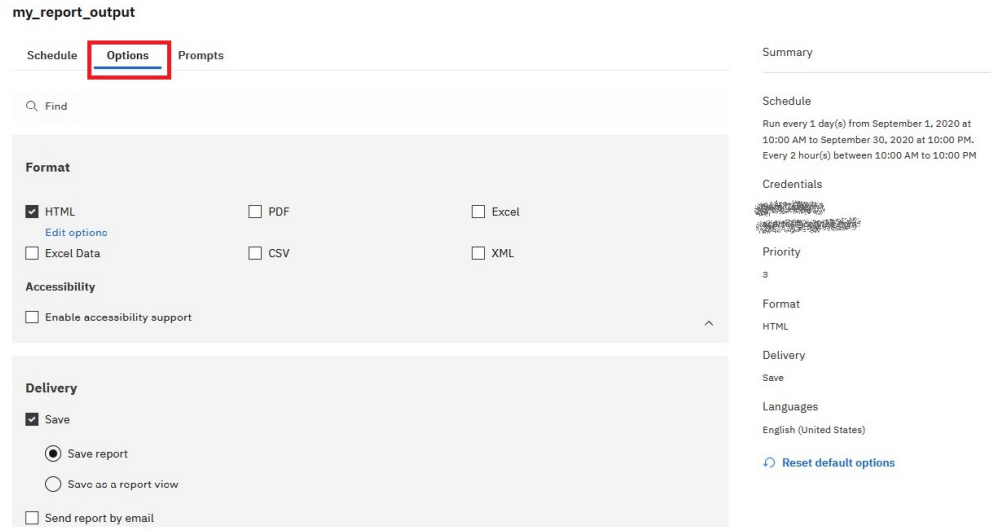
Informationen zum Feld "Priorität"

Wenn Sie die Funktion "Terminierungspriorität" zugeordnet haben, können Sie für den geplanten Eintrag eine Priorität von 1 bis 5 auswählen. Priorität 1 wird zuerst ausgeführt.

Weitere Informationen finden Sie im Artikel " Priorität für die Eintragsausführung ändern" in der *Benutzerhandbuch verwalten*.

7. Gehen Sie wie folgt vor, um das Standardformat, die Bereitstellungsmethode und die Sprache Ihres Berichts anzuzeigen:

   · Klicken Sie auf die Registerkarte **Optionen** .

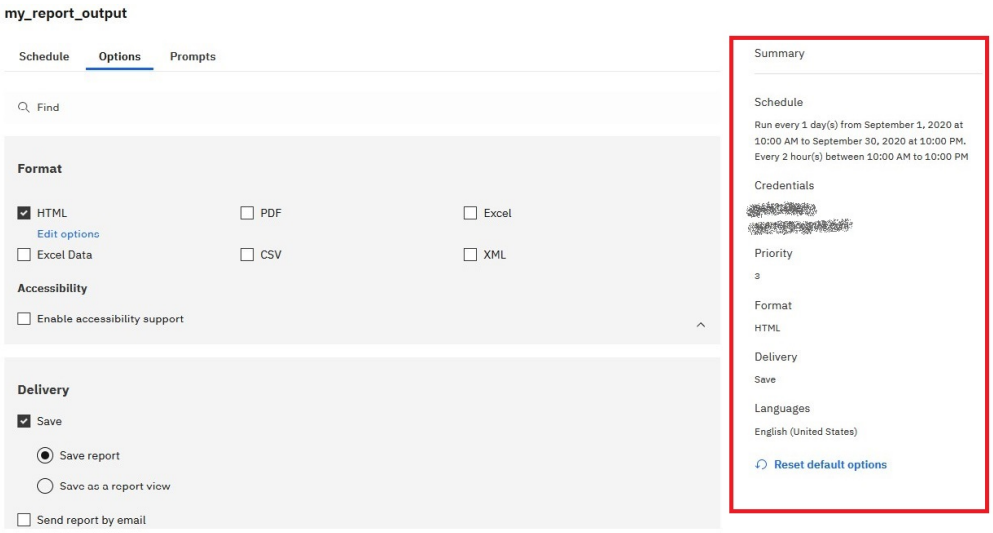


Tipp:

Die Standardoptionen werden angezeigt:

- **Format**: Nur HTML, behindertengerechte behindertengerechte Bedienung
- **Zustellung**: Nur Bericht speichern
- **Sprachen**: Nur Englisch

· Haben Sie das Teilfenster **Zusammenfassung** bemerkt?



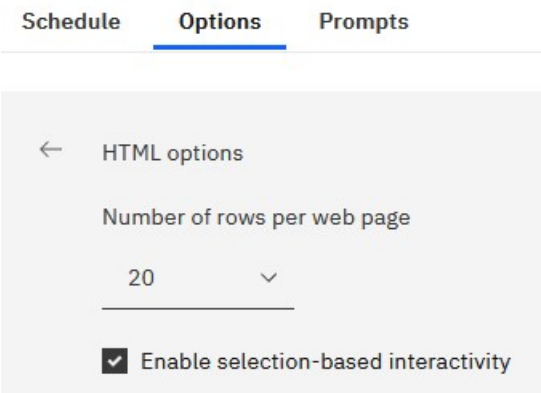
Tipp:

Wenn Sie Ihren Zeitplan erstellen, verwendet das Teilfenster **Zusammenfassung** auf der rechten Seite Ihres Fensters die natürliche Sprache, um alle Ihre Auswahl in Echtzeit zu beschreiben.

Sie können jederzeit auf **Standardoptionen zurücksetzen** klicken, um die Optionen zu löschen, die Sie auf jeder Registerkarte festgelegt haben.

8. Wenn Sie möchten, ändern Sie die **Format** -Optionen:

· Wenn Sie das HTML-Format auswählen, können Sie auf **Optionen bearbeiten**klicken.



Tipp:

Wenn Sie in einem Bericht eine Drilloperation durchführen oder einen Drillthrough zu anderen Berichten durchführen möchten, müssen Sie das Kontrollkästchen **Auswahlbasierte Interaktivität aktivieren** auswählen. Wenn Ihr Bericht jedoch sehr groß ist, können Sie das Kontrollkästchen abwählen, um die Zeit zu verkürzen, die für die Ausführung des Berichts erforderlich ist.

· Wenn Sie das PDF-Format auswählen, können Sie auf **Optionen bearbeiten**klicken.

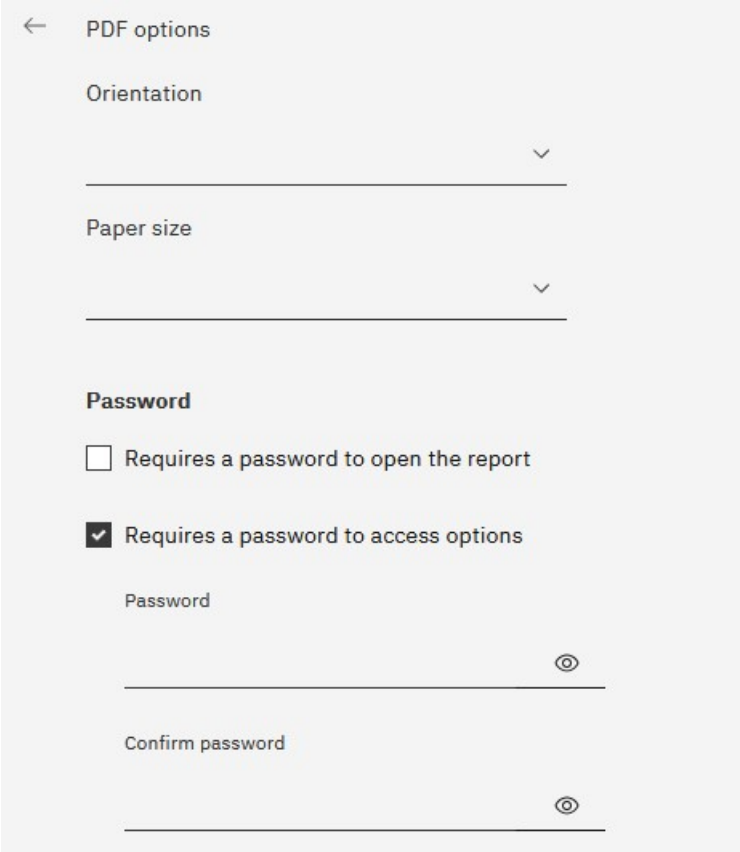


Abbildung 9. PDF-Optionen-Teil 1

Tipp: Sie können ein Kennwort erstellen, um zusätzliche Sicherheit zu Ihrem Bericht hinzuzufügen. Dies ist zusätzlich zu den Berechtigungen, die Benutzer durch ihre Funktionalität erhalten.

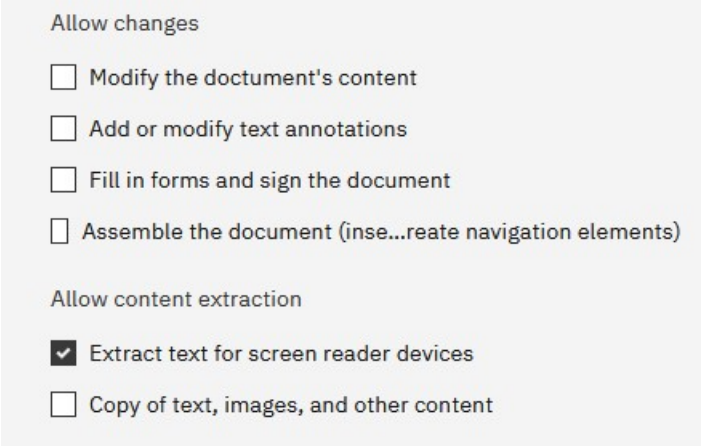


Abbildung 10. PDF-Optionen-Teil 2

Tipp: Sie können die Arten von Änderungen, die andere Benutzer an dem Bericht vornehmen können, begrenzen.

- Wenn Sie das Markierungsfeld **Unterstützung für Eingabehilfen aktivieren** auswählen.

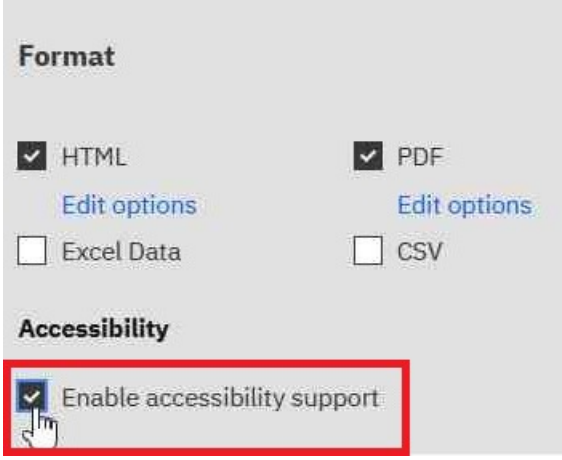


Abbildung 11. PDF-Optionen-Teil 1

Tipp: Sie können die Berichtsausgabe zugänglich machen. Zugängliche Berichte enthalten Features, wie z. B. Alternativtext, die Benutzern mit Behinderungen den Zugriff auf Berichtsinhalte mit Hilfe von unterstützenden Technologien ermöglichen, wie z. B. Sprachausgabeprogrammen.

In IBM ® Cognos ® -Anwendungen können Sie eine zugängliche Ausgabe für Berichte, Jobs, Schritte innerhalb von Jobs und geplante Einträge in PDF und HTML erstellen.

Für barrierefreie Berichte ist mehr Berichtsverarbeitung erforderlich und eine größere Dateigröße als nicht zugängliche Berichte. Folglich kann die Zugänglichkeit von Berichten negative Auswirkungen auf die Leistung haben.

9. Sie können die **Zustellung** -Optionen ändern:

· Wenn Sie den Bericht in Cognos Analytics speichern möchten, haben Sie zwei Optionen.

Abbildung 12. PDF-Optionen-Teil 1

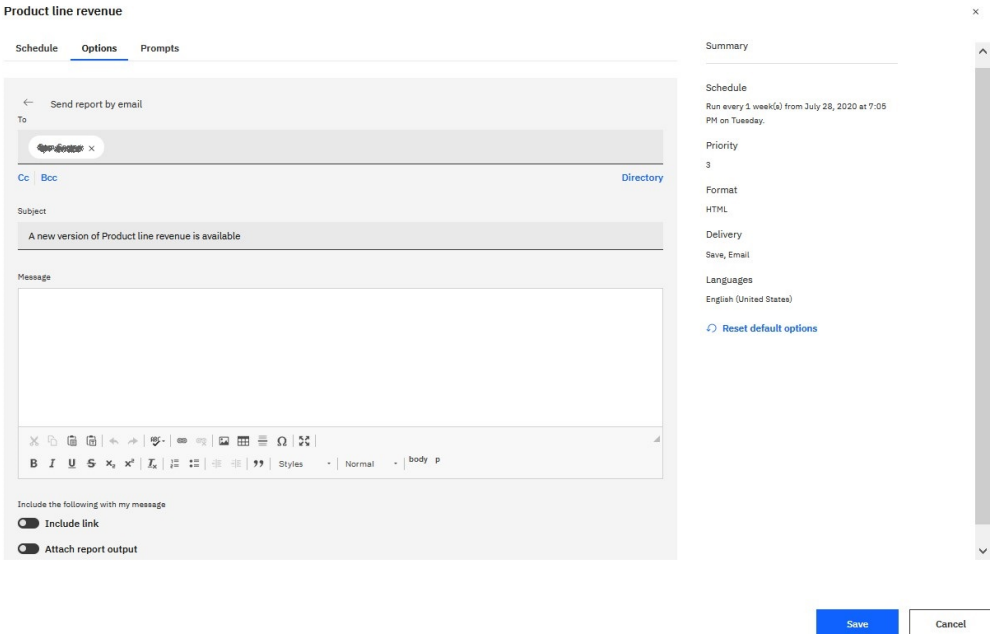
Tipp:

– **Bericht speichern**. Diese Option ist standardmäßig ausgewählt.

– **Als Berichtsansicht speichern**. Anders als beim Speichern des Berichts können Sie den Namen oder Zielordner in der Berichtsansicht ändern. Eine Berichtsansicht verwendet dieselbe Berichtsspezifikation wie der Quellenbericht, weist jedoch unterschiedliche Eigenschaften auf, z. B. Eingabeaufforderungswerte, Zeitpläne, Bereitstellungsmethoden, Ausführungsoptionen, Sprachen und Ausgabeformate.

  Beim Erstellen einer Berichtsansicht wird der ursprüngliche Bericht nicht geändert. Sie können den Quellenbericht für eine Berichtsansicht ermitteln, indem Sie die zugehörigen Eigenschaften anzeigen. Die Eigenschaften der Berichtsansicht geben auch einen Link zu den Eigenschaften des Quellenberichts an.

· Wenn Sie **Bericht per E-Mail senden** auswählen und anschließend auf **Details bearbeiten**klicken.

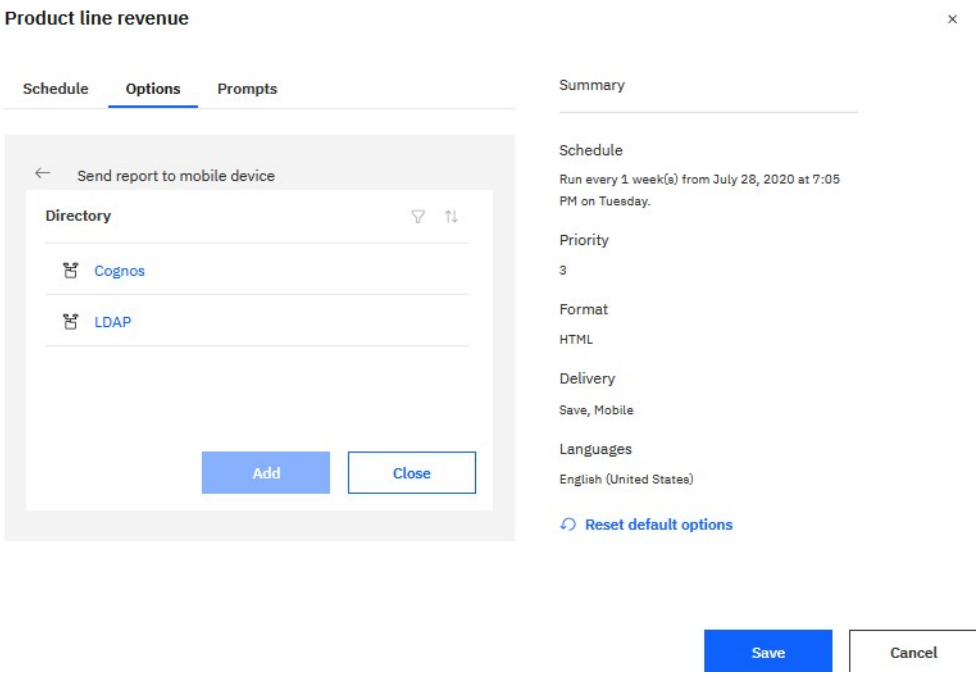


Tipp:

Es wird ein E-Mail-Fenster angezeigt, in dem Sie die Namen der Empfänger eingeben können, wenn Sie über die Berechtigung verfügen. Andernfalls können Sie Ihre E-Mail-Empfänger aus Ihrem lokalen LDAP-Verzeichnis auswählen. Wenn Ihr Verzeichnis sehr groß ist, können Sie Such-, Filter- und Sortierfunktionen verwenden, um Ihre Empfänger schnell zu finden.

Nachdem Sie Ihre Nachricht eingegeben haben und über die korrekten Berechtigungen verfügen, können Sie die Berichtsausgabe an die E-Mail anhängen. Oder Sie können einen Link hinzufügen, auf den Ihr Empfänger klicken kann, um den Bericht zu sehen.

- Wenn Sie **Bericht an mobiles Gerät senden**auswählen.

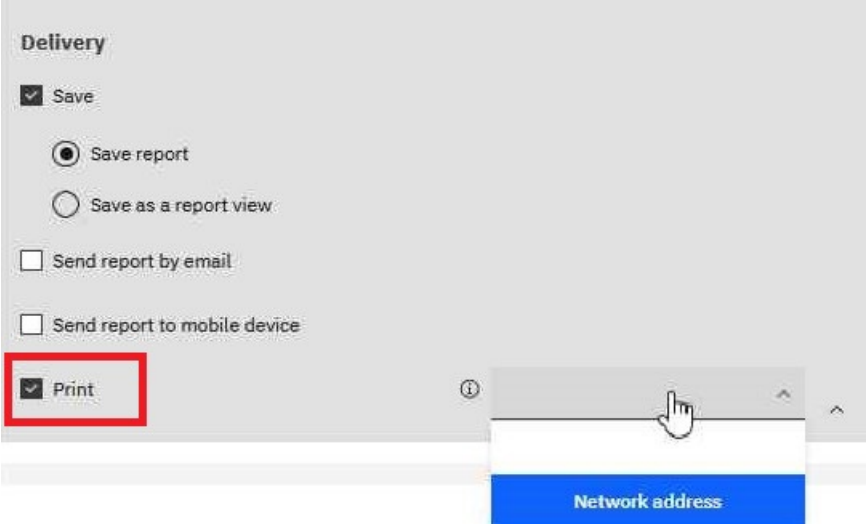


Tipp:

Diese Option ist nur für Benutzer von Cognos Analytics on Demand oder Cognos Analytics on Cloud Hosted verfügbar.

Ähnlich wie bei der E-Mail-Option, können Sie Ihren Empfänger im Verzeichnis finden. Wenn der Bericht ausgeführt wird, wird er über Cognos Analytics for Mobile an das mobile Gerät des Empfängers gesendet.

- Wenn Sie **Drucken**auswählen.



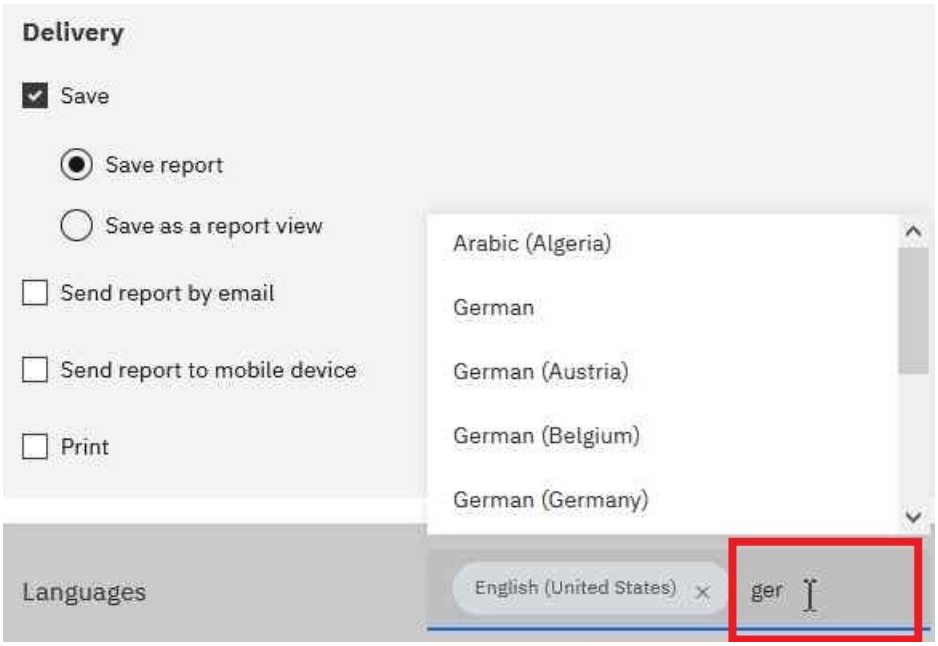
Tipp: Es kann bequem sein, dass Sie eine gedruckte Kopie eines Berichts haben.

Möglicherweise müssen Sie einen Bericht prüfen, wenn Ihr Computer nicht verfügbar ist, oder Sie benötigen möglicherweise eine Kopie eines Berichts an eine Besprechung.

Um Berichte zu drucken, müssen Sie die Funktion 'PDF-Ausgabe generieren' haben.

Wählen Sie einen Drucker aus der Liste aus oder geben Sie einen gültigen Druckernamen, einen gültigen Standort oder eine gültige Adresse ein, und klicken Sie anschließend auf **Hinzufügen**.

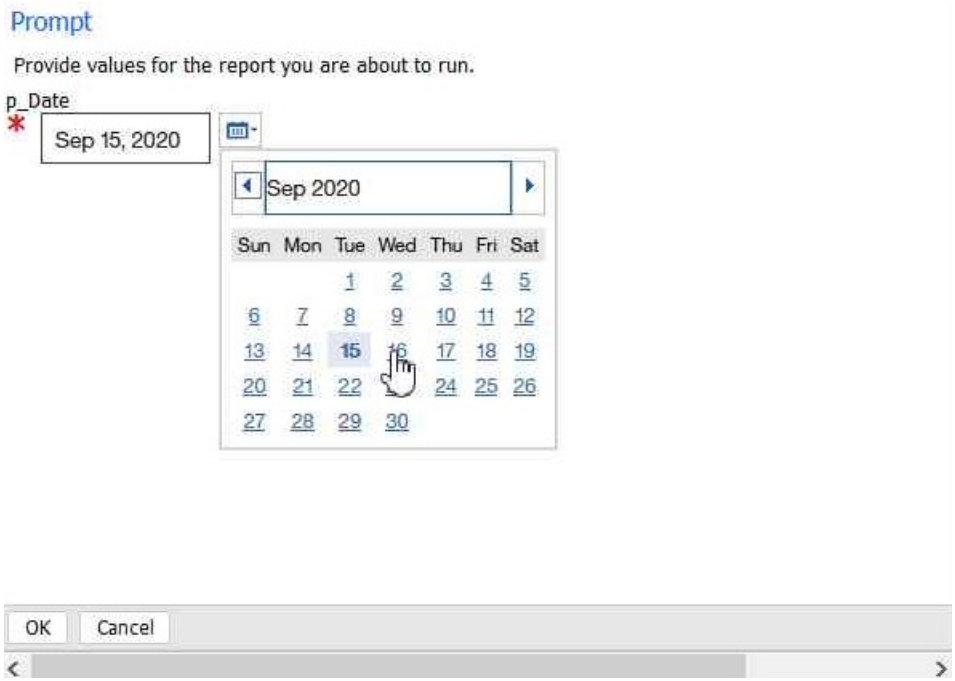
- Wenn Sie Ihre Ausgabe in anderen Sprachen als Englisch wünschen (Standardeinstellung).



Tipp: Beginnen Sie mit der Eingabe des Namens der Sprache in das Feld **Sprachen** . Es wird eine dynamische Liste der Sprachen angezeigt, aus der Sie die gewünschte Sprache auswählen können.

10. Wenn in Ihrem Bericht Eingabeaufforderungen angezeigt werden:

- Klicken Sie auf die Registerkarte **Eingabeaufforderungen** , und klicken Sie dann auf **Werte festlegen**.



Tipp: In dem oben gezeigten Beispiel **Eingabeaufforderung** wird der Wert für den Parameter **p_Date** für einen Datumswert angezeigt.

11. Klicken Sie auf **Speichern**.

Ergebnisse

Es wird ein Zeitplan erstellt, und der Bericht wird zum nächsten geplanten Zeitpunkt ausgeführt.

Verwalten geplanter Aktivitäten

Sie können eine Liste der geplanten Einträge für alle Benutzer anzeigen.

Die einzelnen Einträge werden nach Name, Status und Priorität aufgeführt. Ein Balkendiagramm zeigt einen Überblick über die Aktivitäten, sortiert nach aktivierten und inaktivierten Zeitplänen.

Das Datum und die Uhrzeit der Zeitplanänderung und der für die Planung zuständige Benutzer werden ebenfalls aufgeführt.

Sie können die Einträge filtern, sodass nur die gewünschten Einträge angezeigt werden. Sie können wählen, ob nur Einträge mit einem bestimmten Status oder einer bestimmten Priorität oder Einträge eines bestimmten Typs oder Bereichs angezeigt werden sollen. Sie können auch nach dem Benutzer, der den Eintrag geplant hat, und nach dem Eigentümer des Eintrags filtern.

Sie können Eigenschaften festlegen, den Zeitplan einmal ausführen, geplante Einträge inaktivieren und aktivieren, den Zeitplan bearbeiten, den Zeitplan entfernen, die Priorität festlegen (siehe „Priorität für die Eintragsausführung ändern" auf Seite 258) und den Ausführungsverlauf anzeigen (siehe „Anzeigen des Ausführungsprotokolls von Einträgen" auf Seite 266). In Abhängigkeit vom Eintrag können Sie möglicherweise auch andere Funktionen ausführen, z. B. das Anzeigen von Ausgaben oder Ereignislisten.

Weitere Informationen über Zeitpläne finden Sie in Kapitel 18, „Zeitplanmanagement", auf Seite 277.

Vorgehensweise

1. Klicken Sie im Menü **Verwalten** auf **Aktivitäten**.
2. Klicken Sie auf das Typsymbol und anschließend auf die Option **Zeitplan**.
3. Klicken Sie im Bereich **Filter** auf die zu verwendenden Filteroptionen.

Tipp: Wenn Sie erweiterte Filteroptionen verwenden möchten, klicken Sie auf **Erweiterte Optionen**. die Auswahl auf die Standardeinstellungen zurückzusetzen, klicken Sie auf **Auf Standard zurücksetzen**.

4. Klicken Sie auf **Anwenden**.

   In der Liste werden die ausgewählten Einträge angezeigt.

5. Zum Ausführen einer Aktion für einen einzelnen Eintrag klicken Sie auf **Mehr** ( ) neben dem betreffenden Eintrag und wählen dann die gewünschte Aktion aus.

   In der folgenden Tabelle sind die für die jeweiligen Einträge verfügbaren Aktionen sowie die zugehörigen Symbole aufgeführt:

Tabelle 69. Geplante Aktivitäten - Aktionen und Symbole

Aktion	**Symbol**
Eigenschaften	
Diesen Zeitplan ändern	
Versionen anzeigen	
Diesen Zeitplan inaktivieren	
Diesen Zeitplan entfernen	
Priorität festlegen	
Eigene Berechtigungsnachweise verwenden	

Tipp: Wenn Sie alle Einträge in der Liste auswählen möchten, wählen Sie das Kontrollkästchen für die Liste aus.

Beispiel-Die Berechtigungsnachweise für einen Zeitplan ändern

Sie möchten die Berechtigungsnachweise für einen Zeitplan ändern, um Sie als den aktuellen Zeitplaneigner zu identifizieren.

Vorgehensweise

1. Klicken Sie im Menü **Verwalten** auf **Aktivitäten**.
2. Klicken Sie auf die Schaltfläche "Typ" und dann auf **Zeitplan**.
3. Klicken Sie auf **Mehr** ( ) neben dem Eintrag, und klicken Sie dann auf **Meine Berechtigungsnachweise verwenden** .
4. Speichern Sie Ihre Änderungen.

Ergebnisse

Wenn Sie den Zeitplan das nächste Mal öffnen, identifizieren Sie Ihre Berechtigungsnachweise als Eigentümer.

Tipp: Wenn Sie als anonymer Benutzer angemeldet sind, stehen Informationen zum aktuellen Zeitplaneigner nicht zur Verfügung.

Job zum Planen mehrerer Einträge erstellen

Sie können für mehrere Einträge denselben Zeitplan festlegen, indem Sie einen Job erstellen. Ein Job umfasst eine Sammlung von Berichten, Berichtsansichten und anderen Jobs, für die ein gemeinsamer Zeitplan mit denselben Zeitplaneinstellungen erstellt wird. Wenn ein geplanter Job ausgeführt wird, werden sämtliche Einträge in diesem Job ausgeführt.

Wenn ein Jobelement nicht verfügbar ist, können Sie eine andere Verknüpfung auswählen, indem Sie auf **Mit einem Eintrag verknüpfen** klicken.

Jobs bestehen aus Einzelschritten, die sich auf einzelne Berichte, Jobs und Berichtsansichten beziehen. Sie können angeben, ob die Einzelschritte gleichzeitig oder nacheinander ausgeführt werden sollen.

- Wenn Schritte gleichzeitig ausgeführt werden, bedeutet das, dass sie alle auf einmal übergeben werden. Der Job gilt als erfolgreich ausgeführt, wenn alle Schritte ausgeführt wurden. Wenn bei einem Schritt ein Fehler auftritt, werden die anderen Schritte dennoch ausgeführt, aber der Job erhält den Status **Fehlgeschlagen**.
- Werden die Schritte nacheinander ausgeführt, können Sie die Ausführungsreihenfolge angeben. Ein Schritt wird erst dann übermittelt, wenn der vorherige Schritt erfolgreich ausgeführt wurde. Wenn bei einem Schritt ein Fehler auftritt, können Sie auswählen, ob der Job abgebrochen werden soll oder ob die anderen Schritte fortgesetzt werden.

Sie können die Ausführung eines Jobs planen, indem Sie einen einmaligen Termin, einen regelmäßigen Termin oder ein auslösendes Ereignis wie eine Datenbankaktualisierung oder eine E-Mail festlegen. Weitere Informationen finden Sie im Abschnitt „Trigger-basierte Eintragsplanung" auf Seite 272.

Den einzelnen Berichten, Jobs und Berichtsansichten in den jeweiligen Schritten können auch individuelle Zeitpläne zugeordnet sein. Ausführungsoptionen für einzelne Schritteinträge überschreiben die für den Job festgelegten Ausführungsoptionen. Sie können Ausführungsoptionen für den Job angeben, die als Standardeinstellung für die Schritteinträge verwendet werden, die über keine eigenen Ausführungsoptionen verfügen.

Sie können Berichte ausführen, um Ausgaben basierend auf den von Ihnen definierten Optionen, z. B. Format, Sprache und Eingabehilfen, zu erstellen.

Die Berechtigungen, die zum Hinzufügen eines Eintrags zu einem Job erforderlich sind, variieren in Abhängigkeit vom Eintragstyp. Die Berechtigungen entsprechen den Berechtigungen für das zeitliche Planen eines Eintrags. Weitere Informationen finden Sie unter „Bericht planen" auf Seite 247.

Vorgehensweise

1. Klicken Sie in der Anwendungsleiste auf das + und dann auf ↗.

   Die Seite **Schritte** wird angezeigt.
2. Klicken Sie auf das Symbol **Jobschritt hinzufügen**, ⊕.
3. Wählen Sie Berichte aus, die im Job enthalten sein sollen.
   a) Navigieren Sie zu einem Ordner, der die gewünschten Berichte enthält.
   b) Wählen Sie Kontrollkästchen für einen oder mehrere Berichte aus.

      Tipps:

      - Klicken Sie mit gedrückter Strg-Taste, um mehrere Kontrollkästchen auszuwählen.
      - Verwenden Sie die Links **Alle in Ordner auswählen** und **Alle in Ordner abwählen**, und klicken Sie dann bei gedrückter Strg-Taste auf Kontrollkästchen, um die Auswahl in einem Ordner schnell abzuschließen.
      - Klicken Sie auf **Jobschritte hinzufügen**.

   c) Wiederholen Sie die Schritte „3.a" auf Seite 291 und „3.b" auf Seite 291, um Berichte in anderen Ordnern auszuwählen.

Im Fenster **Schritte** werden die Schritte aufgeführt, die für Ihren Job definiert sind. Jeder Schritteintrag zeigt Folgendes an:

- Der Name eines Berichts, den Sie ausgewählt haben.

  Tipp: Bewegen Sie den Mauszeiger über den Berichtsnamen, um den Navigationspfad zur Berichtsposition anzuzeigen.

- Ob die Schrittoptionen durch den Bericht definiert werden oder angepasst sind

4. So ändern Sie die aktuellen Schrittoptionen für einen beliebigen Schritt in Ihrem Job:
   a) Klicken Sie für den Schritt, den Sie ändern möchten, auf das Symbol "Optionen bearbeiten" .
   b) Bearbeiten Sie die Option **Format**, **Barrierefreiheit**, **Zielgruppenverteilung**, **Zustellung**, **Sprachen** oder **Eingabeaufforderung**.
   c) Klicken Sie auf **Schließen**.
5. So ändern Sie die Standardlaufoptionen für zukünftige Schritte:
   a) Wählen Sie **Standardschrittoptionen ändern** aus.
   b) Bearbeiten Sie die Option für **Format**, **Barrierefreiheit**, Zielgruppenverteilung, **Zustellung**, Eingabeaufforderungen oder **Sprachen**.
   c) Klicken Sie auf **Schließen**.
6. Wenn Sie einen Schritt entfernen möchten, bewegen Sie den Mauszeiger über den Schritt, und klicken Sie dann auf das Symbol "Jobschritt entfernen" .
7. Wählen Sie unter **Ausführungsreihenfolge** die Option **Alle auf einmal ausführen** oder **Nacheinander ausführen** für die Ausführung der Schritte aus.

   - Wenn Sie die Option **Nacheinander ausführen** auswählen, werden die Schritte in der Reihenfolge ausgeführt, in der sie in der Liste **Schritte** angezeigt werden.
   - Wenn die Option **Alle auf einmal ausführen** abgeblendet ist, hat Ihr Administrator diese Option inaktiviert.

     Weitere Informationen hierzu finden Sie im Abschnitt zum "Inaktivieren der Option 'Alle auf einmal ausführen' in Jobs" im Handbuch 'Cognos Analytics - Verwaltung'.
   - Wenn die Ausführung eines Jobs auch dann fortgesetzt werden soll, wenn einer der Schritte fehlschlägt, aktivieren Sie das Kontrollkästchen **Bei Fehler fortsetzen**.

   Tipp: Sie können zum Ändern der Reihenfolge der Schritte auf einen Schritt klicken und ihn an die gewünschte Position ziehen.
8. Klicken Sie in der Anwendungsleiste auf das Symbol zum Speichern .
9. Navigieren Sie zu einem Ordner, in dem der Job gespeichert werden soll, geben Sie einen Jobnamen im Feld **Speichern unter** an und klicken Sie anschließend auf **Speichern**.

   Im Abschnitt **Ausführungsoptionen** werden die Links **Jetzt ausführen** und **Zeitplan** angezeigt.
10. Wenn der Bericht sofort ausgeführt werden soll, klicken Sie auf **Jetzt ausführen** und anschließend auf **Fertigstellen**.
11. Wenn Sie die wiederholte Ausführung planen möchten, führen Sie die folgenden Schritte aus:
    a) Klicken Sie auf **Zeitplan**.
    b) Klicken Sie auf **Neu**.
    c) Geben Sie die Details zum Zeitpunkt der gewünschten Jobausführung ein.
    d) Klicken Sie auf **Erstellen**.

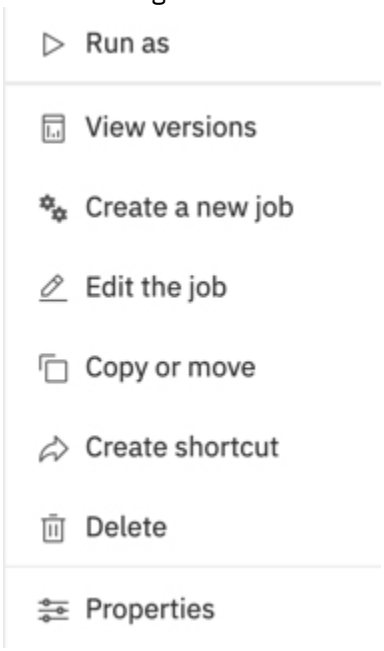
       Tipp: Falls die Nachricht "Für die Ausführung dieser Operation sind Ihre Berechtigungsnachweise erforderlich" angezeigt wird, klicken Sie auf **Erneuern** und geben Sie anschließend Ihre Cognos Analytics-Benutzer-ID und das zugehörige Kennwort ein.

Ergebnisse

In dem von Ihnen ausgewählten Ordner wird ein Job erstellt, mit dem Jobsymbol gekennzeichnet und zum nächsten geplanten Zeitpunkt ausgeführt.

Nächste Schritte

Wenn Sie für den von Ihnen erstellten Job auf das Symbol 'Mehr' klicken, können Sie Operationen aus dem nachfolgenden Menü auswählen:



Zwischengespeicherte Eingabeaufforderungsdaten

Für Berichte, bei denen jedes Mal, wenn der Bericht ausgeführt wird, für Werte angezeigt wird, können Sie zwischengespeicherte Eingabeaufforderungsdaten verwenden. Berichte werden schneller ausgeführt, da Daten aus dem Cache und nicht aus der Datenbank abgerufen werden.

Der Cache wird nur verwendet, wenn eine angeforderte Sprache die gleiche wie eine im Cache ist. Der Cache enthält beispielsweise Daten für Englisch, Englisch (Vereinigte Staaten) und Deutsch (Deutschland). Wenn Sie dazu aufgefordert werden, fordern Sie Englisch (Vereinigte Staaten) für den Bericht an. Es gibt eine exakte Übereinstimmung, und die zwischengespeicherten Daten werden verwendet. Die zwischengespeicherten Daten werden auch verwendet, wenn eine Teilübereinstimmung vorhanden ist. Wenn Sie Englisch (Kanada) anfordern, werden die zwischengespeicherten Daten für Englisch verwendet. Wenn Sie Deutsch (Österreich) anfordern, gibt es keine Übereinstimmung, und die zwischengespeicherten Daten werden nicht verwendet.

Sie können Caches für Berichte oder Berichtsansichten verwenden. Für Berichtsansichten wird zuerst der Cache für die Berichtsansicht verwendet. Wenn kein Cache für Berichtsansichten gefunden wird, wird der Cache für den zugehörigen Bericht verwendet.

Sie müssen einen Job verwenden, um einen Cache zu erstellen oder zu aktualisieren. Sie können den Cache automatisch aktualisieren, indem Sie den Job so planen, dass er regelmäßig ausgeführt wird. Wenn Sie die Live-Daten beim nächsten Ausführen des Berichts verwenden möchten, können Sie den Cache löschen.

Trigger-basierte Eintragsplanung

Sie können Einträge, die auf einem Vorkommen basieren, wie z. B. eine Datenbankaktualisierung oder eine E-Mail, planen. Das Vorkommen wirkt als Auslöser und führt dazu, dass der Eintrag ausgeführt wird. Sie können beispielsweise jedes Mal, wenn eine Datenbank aktualisiert wird, einen Bericht ausführen.

Die Trigger-basierte Terminierung kann verwendet werden, um Einträge automatisch basierend auf einem Vorkommen auszuführen. Es kann auch verwendet werden, um zu begrenzen, wenn Benutzer Einträge ausführen können. Beispiel: In einer Data-Warehouse-Umgebung, in der die Datenbank nur einmal pro Woche aktualisiert wird, ist es nicht mehr erforderlich, Berichte häufiger auszuführen.

Sie können den Bericht basierend auf der Datenbankaktualisierung so planen, dass der Bericht nur einmal pro Woche ausgeführt wird.

Die Trigger-basierte Terminierung gilt nur für den Eintrag und nicht für die ihm zugeordnete Eintragsansicht. Wenn z. B. eine triggerbasierte Terminierung für einen Bericht gilt, gilt dies nicht für Berichtsansichten, die dem Bericht zugeordnet sind. Sie können jedoch eine Berichtsansicht mithilfe eines Auslösers planen.

In **IBM Cognos Administration**können Sie den Zugriff auf die Terminierung durch Auslöser mithilfe der Funktion **Zeitplan nach Auslöser** steuern.

Auslöserbasierte Zeitplanung einrichten

Um einen Eintrag auf der Basis eines Auftretens zu planen und eine Trigger-basierte Terminierung zu bestätigen, müssen Sie Lese-, Schreib-, Ausführungs-und Transitberechtigungen haben.

Zum Planen von Berichten, die in den CSV-, PDF-, Microsoft -(XLS) oder XML-Ausgabeformaten ausgeführt werden sollen, benötigen Sie die Funktion zur Generierung der Ausgabe für das bestimmte Format. Weitere Informationen finden Sie unter „Berichtsformate“ auf Seite 367.

Sie benötigen außerdem die folgenden Zugriffsberechtigungen für alle Datenquellen, die vom Eintrag verwendet werden.

Tabelle 70. Datenquellen und Berechtigungen, die für eine Trigger-basierte Terminierung erforderlich sind

Datenquelle	**Berechtigungen**
Datenquelle	Ausführen und Traverse
dataSourceConnection	Ausführen und Traverse Wenn Sie nur den Zugriff ausführen, werden Sie aufgefordert, sich bei der Datenbank anzumelden.
dataSourceSignon	Ausführen

Bevor Sie eine Trigger-basierte Terminierung einrichten, stellen Sie sicher, dass Ihre Berechtigungsnachweise vorhanden sind und auf dem neuesten Stand sind.

Tipp: Klicken Sie auf die Schaltfläche 'Meine Bereichsoptionen'  , **Eigene Vorgaben**und klicken Sie auf der Registerkarte **Personal** auf **Berechtigungsnachweise erneuern**.

Führen Sie den folgenden Prozess aus, um eine Trigger-basierte Terminierung zu konfigurieren:

- „Eintrag basierend auf einem Vorkommen planen“ auf Seite 274.
- Auslöservorkommen auf einem Server konfigurieren.

Trigger-Vorkommen können auch von einem Software Development Kit-Entwickler mit dem IBM Cognos Software Development Kit konfiguriert werden. Weitere Informationen finden Sie im *Software Development Kit-Entwicklerhandbuch*.

Trigger-Vorkommen auf einem Server einrichten

Im Rahmen der Einrichtung einer auslösebasierten Berichtszeitplanung müssen Sie das Auftreten des Auslösers auf einem Server einrichten.

Sie verknüpfen das externe Vorkommen, wie z. B. eine Datenbankaktualisierung oder eine E-Mail, mit einem Auslöser auf dem Server, der die Ausführung des Eintrags bewirkt. Sie müssen auch den Namen des Vorkommens angeben.

Trigger-Vorkommen können auch von einem Software Development Kit-Entwickler mit dem Software-Development-Kit von IBM Cognos konfiguriert werden. Weitere Informationen finden Sie im *IBM Cognos Software Development Kit Developer Guide*.

Mit dem Script "trigger.bat" von Microsoft Fenster oder mit dem Shell-Script "trigger.sh" können Sie einen oder mehrere Zeitpläne für die Ausführung auf dem Server auslösen. Die Scriptsyntax folgt, wenn URL die URL des IBM Cognos -Servers ist, `Benutzername` ein gültiger Benutzername im angegebenen Namespace ist, `Kennwort` das Kennwort für den Benutzernamen, `Namensbereich` der Namensbereich für den Benutzernamen und `Triggerliste` eine durch Kommas getrennte Liste mit Auslösernamen ist:

```
trigger.bat URL [username password namespace]
triggerlist
```

Wenn Benutzer beispielsweise einen Bericht auf der Basis einer Datenbankaktualisierung planen und einen zweiten Bericht auf der Basis des Empfangs einer E-Mail terminieren möchten, sieht Ihre angepasste Auslöserbefehlszeile möglicherweise ähnlich wie folgt aus:

```
trigger.bat http://localhost:9300/p2pd/servlet/dispatch username
password namespace databaserefreshtriggername,emailtriggername
```

Vorgehensweise

1. Wenn Sie ein Auslöserereignis auf einem anderen Server als einem IBM Cognos -Server einrichten, führen Sie die folgenden Tasks aus:
   - Stellen Sie sicher, dass der Server über eine unterstützte Version von Java Runtime Environment oder ein Java Development Kit verfügt.
   - Kopieren Sie die folgenden Dateien aus dem Verzeichnis *cognos_analytics_installation_location*/webapps/p2pd/WEB-INF/lib auf einem IBM Cognos -Server in die Position auf dem Server, auf dem Sie das Auslöserereignis einrichten:

     activation.jar

     axis.jar

     axisCrnpClient.jar

     commons-discovery-0.2.jar

     commons-logging-1.1.jar

     commons-logging-adapters-1.1.jar

     commons-logging-api-1.1.jar

     jaxrpc.jar

     saaj.jar

     wsdl4j-1.5.1.jar
   - Kopieren Sie `mail.jar` von *cognos_analytics_installation_location*/bin64 auf einem IBM Cognos -Server an die Position auf dem Server, auf dem Sie das Auslöserereignis konfigurieren.
   - Kopieren Sie die folgenden Dateien aus dem *cognos_analytics_installation_location*/webapps/utilities/trigger auf einem IBM Cognos -Server an die Position auf dem Server, auf dem Sie das Auslöserereignis einrichten:

     trigger.bat

     trigger.sh

     trigger.class (a Java utility that can run on any IBM Cognos-supported platform)

2. Stellen Sie sicher, dass die Befehlszeile ausgeführt wird, wenn das externe Vorkommen, wie z. B. eine Datenbankaktualisierung oder eine E-Mail, auftritt.

   Der Mechanismus, den Sie zum Aufrufen Ihres angepassten Auslöserbefehls verwenden, hängt von der Anwendung ab, mit der Sie arbeiten, wie z. B. ein Datenbanksystem oder eine E-Mail-Anwendung. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Anwendung.
3. Informieren Sie die Benutzer darüber, dass sie jetzt Einträge basierend auf dem Auslöserereignis planen können.

   Wenn ein Benutzer einen Eintrag auf der Basis des Auftretens terminiert, wenn der Benutzer auf die Zeitplanschaltfläche für eine Berichtsansicht klickt, werden Informationen zum Vorkommen auf der **Zeitplan** -Seite ersetzt.

Ergebnisse

Nachdem das Script ausgeführt wurde, gibt die Auslösermethode einen ganzzahligen Wert zurück, der die Anzahl der ausgeführten Zeitpläne darstellt. Die folgenden Ganzzahlen stellen Fehler dar:

· -1 ist ein Syntaxfehler, wie z. B. ein ungültiger Parameter oder eine ungültige Syntax.

· -2 ist ein Kommunikationsproblem mit IBM Cognos -Server

Eintrag basierend auf einem Vorkommen planen

Im Rahmen der Einrichtung einer Triggern-basierten Terminierung müssen Sie einen Eintrag auf der Basis eines Vorkommens planen.

Der Trigger-basierte Zeitplan wird aktiviert, wenn der Benutzer, der den Auslöser abfeuert, Folgendes hat

· Lese-und Transitberechtigungen für den Zeitplaneintrag

· Traversenberechtigungen für alle Vorfahren des Zeitplaneintrags

· Zugriff auf IBM Cognos Administration

Zum Planen von Berichten, die in den CSV-, PDF-, Microsoft -(XLS) oder XML-Ausgabeformaten ausgeführt werden sollen, benötigen Sie die Funktion zur Generierung der Ausgabe für das bestimmte Format. Weitere Informationen finden Sie unter „Berichtsformate” auf Seite 367.

Vorbereitende Schritte

Wenn sie von einem Auslöser geplant wird, kann ein Bericht nur ausgeführt werden, wenn Sie bereits ein Auslöserereignis eingerichtet haben. Weitere Informationen finden Sie unter „Trigger-Vorkommen auf einem Server einrichten” auf Seite 273.

Vorgehensweise

1. Klicken Sie auf die Schaltfläche "Mehr"  für den Eintrag, den Sie planen möchten.
2. Klicken Sie auf  **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Zeitplan** .
4. Klicken Sie auf  **Neu**.
5. Klicken Sie in der Anzeige **Zeitplan erstellen** auf das schwarze Dreieck im Feld **Zeitplan** , und klicken Sie anschließend auf **Nach Auslöser**.
6. Geben Sie in das Feld **Triggername** den Namen des Auslöservorkommens ein.

   Hinweis: Der Triggername, den Sie eingeben, kann Ihnen von Ihrem Administrator oder Ihrem Entwickler zur Verfügung gestellt werden. Wenn dies nicht der Fall ist, müssen Sie Ihren Administrator oder Entwickler über den von Ihnen verwendeten Triggernamen informieren.
7. Legen Sie die Start-und Endzeit des **Zeitraum** s fest, während dessen ein Auslöser den Zeitplan für die Ausführung des Zeitplans verursacht.

Tipp: Der Auslöserzeitplan wird ausgeführt, wenn der Auslöser (entweder aus trigger.bat oder aus einer Software-Development-Kit-Anwendung) zwischen dem Start-und dem Enddatum ausgelöst wird.

8. Klicken Sie auf **Erstellen**.

Kapitel 19. Implementierung

Bei der Implementierung werden Anwendungen von einer Installation in eine andere versetzt. You can deploy IBM Cognos content from a source environment to a target environment.

Sie können den gesamten Content-Store oder nur bestimmte Inhalte, wie z. B. Pakete, Ordner, Namespaces, Benutzerkonten oder Visualisierungen, implementieren.

In der Regel überträgt die Implementierung Einträge aus einer Entwicklungsumgebung in eine Testumgebung und anschließend in eine Produktionsumgebung. Sie können auch zwischen den Betriebssystemen implementieren.

Es ist wichtig, Implementierung planen sicherzustellen, dass Sie die richtigen Informationen implementieren und die Zielumgebung nicht stören. Sie ist auch für Sicherheit prüfen in den Quellen-und Zielumgebungen wichtig.

Sie können Einträge aus früheren Releases aktualisieren, indem Sie den Importassistenten für die Implementierung ausführen. Weitere Informationen finden Sie im Artikel „In eine Zielumgebung importieren" auf Seite 317.

Sie können ein Betriebssystem oder einen Scripting-Mechanismus verwenden, um die Implementierung über eine Befehlszeile auszuführen. Mit dem Software-Development-Kit von IBM Cognos können Sie den Implementierungsprozess automatisieren.

- Implementierungsspezifikation erstellen, aktualisieren und löschen
- Laden einer Implementierungsspezifikation aus einem Bereitstellungsarchiv
- Übergabe von Implementierungs-und Importanforderungen
- Zugriffsprotokoll

Weitere Informationen finden Sie im IBM Cognos Software Development Kit *Entwicklerhandbuch*.

Informationen zur Bereitstellung von Inhalten in einer Multi-Tenant-Umgebung von IBM Cognos Analytics finden Sie unter „Implementierung von TenantInhalten" auf Seite 351.

Die Implementierung von Benutzertaskservice ist eine separate Task. Weitere Informationen finden Sie unter „Human Task-und Anmerkungsservices implementieren" auf Seite 322.

Implementierungsspezifikationen

Eine Implementierungsspezifikation ist ein Eintrag im Content-Store, in dem die zu implementierenden Einträge, die Implementierungsvorgaben und der Name des Bereitstellungsarchivs definiert werden.

Es gibt zwei Typen von Implementierungsspezifikationen. Exportspezifikationen werden in der Quellenumgebung erstellt und steuern die Erstellung von Bereitstellungsarchiven. Importspezifikationen werden in der Zielumgebung erstellt und steuern den Import von Einträgen aus dem Bereitstellungsarchiv.

Sie können das Implementierungsprotokoll für jede Implementierungsspezifikation anzeigen, um das Datum, die Uhrzeit und die Details des Imports oder Exports anzuzeigen.

Bereitstellungsarchive

Ein Bereitstellungsarchiv ist eine komprimierte Datei, die tatsächliche Einträge enthält, die erstellt werden, wenn Sie aus der Quellenumgebung exportieren.

Sie verschieben das Bereitstellungsarchiv aus der Quellenumgebung in die Zielumgebung. Anschließend importieren Sie aus dem Bereitstellungsarchiv in die Zielumgebung.

Um ein Bereitstellungsarchiv zu verschieben, benötigen Sie Zugriff auf die Installationsverzeichnisse auf dem Computer, auf dem die IBM Cognos -Software installiert ist. Diese Position wird im Konfigurationstool

festgelegt. Die Standardposition ist *Installationsposition*/deployment. For information about changing the location, see the IBM Cognos *Installations-und Konfigurationshandbuch*.

Wenn Sie in ein vorhandenes Bereitstellungsarchiv exportieren, werden die Inhalte des Archivs überschrieben.

Implementierungsplanung

Wenn Sie die Implementierung durchführen, müssen Sie überlegen, wie Sie die Sicherheit handhaben und welche Implementierungsmethode auswählen soll.

Um zu vermeiden, Referenzen in der Zielumgebung zu brechen, müssen Sie alle Einträge implementieren, die sich auf Einträge in einem anderen Paket oder einem anderen Ordner beziehen. Folgende Einträge sind zu berücksichtigen:

- Jobs und Berichtsansichten
- Mitgliedschaften und Einreiseberechtigungen

Sicherheit und Implementierung

Vor der Implementierung müssen Sie die Zugriffsberechtigungen, die Sicherheit von Bereitstellungsarchiven und Verweise auf andere Namespaces als **Cognos**berücksichtigen.

Zugriffsberechtigungen

Die Einträge, die Sie implementieren, können auf sie angewendet werden, z. B. auf die Zugriffsberechtigungen Kapitel 12, „Zugriffsberechtigungen und Berechtigungsnachweise“ , auf Seite 193 , die angeben, auf welche Benutzer und Gruppen auf sie zugreifen können. Wenn Sie den gesamten Content-Store „Gesamter Content-Store implementieren“ auf Seite 302implementieren, werden alle Zugriffsberechtigungen implementiert. Wenn Sie ausgewählte Pakete, öffentliche Ordner und Verzeichnisinhalte implementieren, können Sie auswählen, ob die Zugriffsberechtigungen „Ausgewählte öffentliche Ordner und Verzeichnisinhalte implementieren“ auf Seite 304implementiert werden sollen.

Gehen Sie wie folgt vor:

- Referenzierte Benutzer und Gruppen

  Wenn Sie Zugriffsberechtigungen für eine Zielumgebung implementieren, müssen die referenzierten Benutzer und Gruppen in der Zielumgebung vorhanden sein.

- Regeln für Zugriffsberechtigungen

  Damit Zugriffsberechtigungen für die Arbeit nach der Implementierung von Einträgen verwendet werden können, müssen die Quellenumgebung und die Zielumgebung denselben Authentifizierungsprovider mit derselben Konfiguration verwenden. Andernfalls funktionieren die Berechtigungen möglicherweise nicht nach der Implementierung.

  Verwenden Sie den Cognos -Namespace, um sicherzustellen, dass die Berechtigungen aus der Quellenumgebung in der Zielumgebung funktionieren. Erstellen Sie beispielsweise in der Quellenumgebung Cognos -Gruppen mit der Gruppe 'Jeder' als Mitglied und setzen Sie anschließend Zugriffsberechtigungen für die Gruppen. Ordnen Sie nach der Implementierung in der Zielumgebung die Cognos -Gruppen den entsprechenden Benutzern und Gruppen des Authentifizierungsproviders zu und entfernen Sie dann 'Jeder' von der Zugehörigkeit zur Gruppe.

Informationen zum Implementieren von Cognos -Gruppen und -Rollen finden Sie im Artikel „Einschließlich Cognos Gruppen und Rollen“ auf Seite 306.

Bereitstellungsarchive sichern

Ein Bereitstellungsarchiv „Bereitstellungsarchive“ auf Seite 299 kann sensible Informationen, wie z. B. signons und vertrauliche Konto-oder Kreditkartennummern in Berichtsausgaben, enthalten. Wenn Sie exportieren, können Sie das Bereitstellungsarchiv verschlüsseln, indem Sie ein Kennwort festlegen.

Später, wenn Sie importieren, müssen Sie das Verschlüsselungskennwort eingeben. Das Kennwort muss acht oder mehr Zeichen enthalten.

Sie müssen das Bereitstellungsarchiv verschlüsseln, wenn es Datenquellensignonen enthält, oder wenn Sie den gesamten Content-Store „Gesamter Content-Store implementieren" auf Seite 302implementieren.

Die Verschlüsselungseinstellungen werden im Konfigurationstool konfiguriert. For more information, see the IBM Cognos *Installations-und Konfigurationshandbuch*.

Einschließlich Verweise auf andere Namensbereiche

Einige Einträge, wie z. B. Gruppen, Rollen, Verteilerlisten, Kontakte, Datenquellensignonen und einige Berichtseigenschaften, wie z. B. E-Mail-Empfänger und Berichtskontakte, können sich auf Entitäten in anderen Namespaces als den **Cognos** -Namespace beziehen. Wenn Sie öffentliche Ordner und Verzeichnisinhalte implementieren, können Sie diese Einträge mit oder ohne Verweise auf diese Namespaces implementieren.

Gehen Sie wie folgt vor:

- Eingeschlossene Referenzen

  Wenn Sie die Verweise auf andere Namespaces einschließen, überprüft das System, ob jede der referenzierten Entitäten in den gültigen Namespaces vorhanden ist. Daher müssen Sie sicherstellen, dass Sie an jedem Namespace angemeldet sind und dass Sie über die erforderlichen Berechtigungen für den Zugriff auf die erforderlichen Entitäten in den Namespaces verfügen. Wenn Sie nicht auf die Namespaces zugreifen können, treten während der Implementierung Fehler auf.

- Keine eingeschlossenen Referenzen

  Wenn Sie die Verweise auf andere Namespaces nicht einschließen, werden die referenzierten Entitäten aus der Mitgliederliste entfernt. Die Mitgliederliste enthält Gruppen, Rollen, Verteilerlisten und Datenquellensignonen und andere Eigenschaften, in denen sie möglicherweise vorhanden sind.

Wenn Sie den gesamten Content-Store „Gesamter Content-Store implementieren" auf Seite 302implementieren, werden die Verweise auf alle Namespaces eingeschlossen.

Lokalisierte Objektnamen beim Importieren älterer Archive beibehalten

Neue Releases von IBM Cognos-Software stellen Unterstützung für neue Ländereinstellungen bereit. Das Importieren älterer Archive in neuere Versionen von kann zu fehlenden Übersetzungen für Objektnamen bei einigen Ländereinstellungen führen. Um dieses Problem zu vermeiden, müssen Sie die erweiterte Eigenschaft CM.UpdateInitialContentNamesAfterImport vor dem Import festlegen.

Informationen zu diesem Vorgang

Beispielsweise wurde die Unterstützung für katalanische, kroatische, dänische, griechische, kasachische, norwegische, slowakische, slowenische und thailändische Locales in den IBM Cognos Business Intelligence-Versionen 10.1.1 und 10.2 hinzugefügt. Archive, die mit früheren Versionen erstellt wurden, unterstützen diese Ländereinstellungen nicht. Wenn Sie diese Typen von Archiven importieren möchten, setzen Sie die Eigenschaft **`CM.UpdateInitialContentNamesAfterImport`** , bevor der Import gestartet wird. Dadurch wird sichergestellt, dass Objektnamen, wie z. B. **Öffentliche Ordner** oder **Meine Ordner**, in diesen zusätzlichen Ländereinstellungen übersetzt werden und ordnungsgemäß angezeigt werden.

Wenn Sie feststellen, dass Objektnamen nach dem Import eines älteren Archivs nicht in der angegebenen Sprache angezeigt werden, lesen Sie den Abschnitt *Handbuch zur Fehlerbehebung für IBM Cognos Analytics*.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt„Erweiterte Einstellungen für bestimmte Services konfigurieren" auf Seite 519aus.
2. Geben Sie für die **ContentManagerService**den Parameternamen **CM.UpdateInitialContentNamesAfterImport**ein.
3. Geben Sie in der Spalte **Wert** die betroffenen Ländereinstellungen ein, und trennen Sie sie jeweils durch ein Komma.

   Geben Sie beispielsweise für slowenische und kroatische Inhaltslocales die folgende Textzeichenfolge ein:

   ```
   sl, hr
   ```

Ergebnisse

Entfernen Sie diese erweiterte Einstellung, wenn die Unterstützung für das ältere Archiv nicht mehr erforderlich ist, da die Leistung, die mit dieser Einstellung verbunden ist, aktiviert ist.

Gesamter Content-Store implementieren

Durch die Implementierung des gesamten Content-Stores wird sichergestellt, dass alle Pakete, Ordner und Verzeichnisinhalte in eine neue Position kopiert werden.

Wenn Sie beispielsweise den Computer ändern, auf dem IBM Cognos -Software installiert ist, können Sie den gesamten Content-Store von der alten Umgebung in die neue Umgebung verschieben und alle Berichte und anderen Einträge, die von Administratoren und Benutzern erstellt wurden, beibehalten.

Weitere Gründe für die Implementierung des gesamten Content-Stores sind:

- Verschieben einer ganzen Anwendung in eine neue leere Umgebung, wie z. B. einen neuen Computer, aus einer Entwicklungsumgebung
- Aktualisierung einer vollständigen Anwendung in einer vorhandenen Umgebung, z. B. einem vorhandenen Computer, aus einer Entwicklungsumgebung
- Verschieben einer Anwendung aus einer vorhandenen Umgebung, die eine andere zugrunde liegende Technologie verwendet, wie z. B. einen anderen Datenbanktyp für den Content-Store oder ein anderes Betriebssystem
- Upgrade für den Inhalt des Content Store

Wenn Sie einen Content-Store von einer Umgebung in eine andere verschieben, müssen Sie dieselben Namespaces für Richtlinien, Benutzer, Rollen und Gruppen verwenden, um ordnungsgemäß zu arbeiten.

Wenn Sie den gesamten Content-Store implementieren, werden, sofern keine Konflikte auftreten, der Inhalt des Zielinhaltspeichers entfernt und durch den Inhalt des Quelleninhaltspeichers ersetzt, mit Ausnahme der Konfigurationsdaten. Die importierten Einträge halten die Eigner aus dem Quelleninhaltsspeicher. Informationen zur Konfliktlösung finden Sie unter „Regeln zur Konfliktlösung" auf Seite 309.

Nachdem die Implementierung abgeschlossen ist, können einige Links für Pakete, die Berichten zugeordnet sind, nicht funktionieren. Möglicherweise müssen Sie Pakete erneut mit Berichten verknüpfen. Informationen zum Verbinden von Paketen mit Berichten finden Sie in der Dokumentation zu den Studios.

Tipp: Anstatt den gesamten Content-Store zu implementieren, können Sie nur bestimmte öffentliche Ordner und Verzeichnisinhalte „Ausgewählte öffentliche Ordner und Verzeichnisinhalte implementieren" auf Seite 304implementieren.

Content Store

Der Content-Store enthält alle Einträge im Portal, wie z. B.:

- Öffentliche Ordner

· Pakete
· Berichte
· Datenquellen
· Verteilerlisten und Kontakte
· Drucker
· Cognos -Namespace
· Implementierungsspezifikationen

Sie enthält nicht das Implementierungsprotokoll „Bereitstellungsverlauf" auf Seite 303. Konfigurationsobjekte „Konfigurationsinformationen" auf Seite 303 , wie z. B. Dispatcher, werden standardmäßig in die Exporte eingeschlossen, jedoch bei den Importen ausgeschlossen.

Wenn Sie persönliche Ordner und persönliche Seiten von Benutzern implementieren möchten, müssen Sie auswählen, dass die Benutzerkontoinformationen bei der Export-und Importoperation eingeschlossen werden sollen.

Bereitstellungsverlauf

Wenn Sie einen gesamten Content-Store exportieren, werden die Export-und Importimplementierungsspezifikationen exportiert, die im Quelleninhaltsspeicher vorhanden sind. Ihre Implementierungshistorien werden nicht exportiert.

Wenn Sie später den gesamten Content-Store importieren, importieren Sie auch die Export-und Importimplementierungsspezifikationen. Es werden keine Einträge auf der **Bereitstellungsverlauf anzeigen** -Seite für die importierten Spezifikationen angezeigt.

Wenn eine der importierten Implementierungsspezifikationen für ein verschlüsseltes Bereitstellungsarchiv verwendet wird, können Sie diese löschen. Um einen gesamten Content-Store zum ersten Mal zu importieren, müssen Sie eine neue Importimplementierungsspezifikation erstellen.

Die in den Implementierungsdatensätzen gespeicherten Informationen enthalten standardmäßig nur den Fortschritt und die Zusammenfassungsberichte. Wenn Sie detailliertere Informationen einschließen möchten, ändern Sie die Aufzeichnungsstufe mithilfe der erweiterten Einstellung CM.DEPLOYMENTDETAILENTIRECONTENT. Verwenden Sie die Schritte in „Erweiterte Content Manager-Parameter festlegen" auf Seite 56. Weitere Aufzeichnungsstufen sind in der partiellen Implementierung „Implementierungsdetails aufzeichnen" auf Seite 307verfügbar.

Konfigurationsinformationen

Wenn Sie einen gesamten Content-Store importieren, werden die Konfigurationsdaten in den Export eingeschlossen, aber standardmäßig von der Import ausgeschlossen. Es wird empfohlen, diese Einstellung nicht zu ändern. Wenn Sie jedoch Konfigurationseinstellungen importieren müssen, können Sie die Standardeinstellung in den erweiterten Einstellungen „Konfigurationsobjekte in den Import des gesamten Content Store einschließen" auf Seite 320ändern.

Wenn Sie die Konfigurationsdaten, insbesondere in einer verteilten Umgebung mit mehreren Content-Managern, importieren, können die aktuellen Informationen zum Inhalt des Content-Manager-Status durch die importierten Daten überschrieben werden.

Tipp: Wenn Sie die Konfiguration importieren, starten Sie den Service in der Zielumgebung erneut, um die Statusinformationen ordnungsgemäß zu aktualisieren.

Informationen zum Einschließen von Konfigurationsdaten in den Import finden Sie unter „Konfigurationsobjekte in den Import des gesamten Content Store einschließen" auf Seite 320.

Informationen dazu, wie bestimmte Objekte im Content-Store importiert werden, finden Sie unter „Regeln zur Konfliktlösung für die Bereitstellung des gesamten Content Store" auf Seite 310.

Ausgewählte öffentliche Ordner und Verzeichnisinhalte implementieren

Sie können eine partielle Implementierung ausführen, indem Sie nur ausgewählte öffentliche Ordner und Verzeichnisinhalte und nicht den gesamten Content-Store implementieren.

Sie können alle Pakete und Ordner in öffentlichen Ordnern implementieren. Durchsuchen Sie die Hierarchie für öffentliche Ordner, und wählen Sie ein Paket oder einen Ordner aus. Auf diese Weise wird der gesamte Inhalt implementiert. Sie können keine bestimmten Einträge in den Paketen oder Ordnern auswählen. Während des Exports werden die übergeordneten Pakete und Ordner nicht exportiert, und Content Manager erstellt keine Platzhalterpositionen für sie in der Zielumgebung. Während der Export- und Importoperation können Sie eine neue Zielposition in der Content Manager-Hierarchie für jedes implementierte Paket und jeden Ordner angeben.

Zu den Verzeichnisinhalten, die Sie implementieren können, gehören der Cognos -Namespace, die Verteilerlisten und -kontakte sowie die Datenquellen und deren Verbindungen und Anmeldungen.

Wenn Sie öffentliche Ordner und Verzeichnisinhalte implementieren, können Sie keine Objekte aus den Bereichen Konfiguration, Funktion, ExportDeploymentOrdner und Ordner 'importDeploymentFolder' des Content-Stores „Partielle Implementierungsoptionen” auf Seite 305einschließen. Weitere Informationen finden Sie unter „Einschließlich Verweise auf andere Namensbereiche” auf Seite 301.

Informationen dazu, wie bestimmte Objekte im Content-Store importiert werden, finden Sie unter „Regeln für die Auflösung von Implementierungskonflikten beim Importieren und Exportieren” auf Seite 308.

Nachdem die Implementierung abgeschlossen ist, funktionieren einige Links für Pakete, die Berichten zugeordnet sind, möglicherweise nicht, auch wenn Sie Pakete und deren Berichte in die Implementierung eingeschlossen haben. Möglicherweise müssen Sie Pakete erneut mit Berichten verknüpfen. Informationen zum Verbinden von Paketen mit Berichten finden Sie in der Dokumentation zu den Studios.

Tipp: Wenn Sie bestimmte Einträge implementieren möchten, können Sie einen Ordner auf der Stammebene der öffentlichen Ordner erstellen, die einzelnen Einträge in diesen Ordner kopieren und diesen Ordner bei der Implementierung auswählen.

Pakete implementieren

Während einer partiellen Implementierung können Sie jeweils ein oder mehrere Pakete implementieren.

Ein Paket kann auf Objekte verweisen, die sich außerhalb des Pakets befinden, wie z. B. Sicherheitsobjekte, Datenquellen und Verteilerlisten. Referenzierte Objekte werden jedoch nicht mit dem Paket implementiert.

Während Sie importieren, können Sie Pakete im Bereitstellungsarchiv abwählen, die Sie nicht importieren möchten.

Pakete und Ordner umbenennen

Während einer partiellen Implementierung können Sie Pakete und Ordner so umbenennen, dass sie einen neuen Namen in der Zielumgebung haben.

Dies ist nützlich, wenn Sie kein Paket oder einen Ordner überschreiben möchten, der bzw. der denselben Namen in der Zielumgebung hat. Das ursprüngliche Paket oder der ursprüngliche Ordner bleibt intakt, und die implementierte Einheit wird umbenannt.

Sie können auch mehrsprachige Namen für Pakete und Ordner hinzufügen, damit Benutzer die Namen anzeigen können, die für ihre Ländereinstellung geeignet sind. Eine Ländereinstellung gibt linguistische Informationen und kulturelle Konventionen für den Zeichentyp, die Sortierfolge, das Format von Datum und Uhrzeit, die Währungseinheit und die Nachrichten an.

Pakete und Ordner inaktivieren

Während einer partiellen Implementierung können Sie die Pakete und Ordner in der Zielumgebung inaktivieren, damit die Benutzer nicht auf sie zugreifen können.

Das Inaktivieren von Paketen und Ordnern ist nützlich, wenn Sie sie in der Zielumgebung testen möchten, bevor Sie diese für Benutzer verfügbar machen.

Sie können Pakete und Ordner zum Zeitpunkt des Exports oder Imports inaktivieren.

Wenn Sie ein Paket oder einen Ordner inaktivieren, sind die darin enthaltenen Einträge nach dem Import in der Zielumgebung nicht zugänglich. Benutzer können Einträge nicht ausführen, anzeigen oder bearbeiten. Nur Benutzer, die über Schreibberechtigungen für die inaktivierten Einträge verfügen, können auf sie zugreifen.

Partielle Implementierungsoptionen

Während einer partiellen Implementierung können Sie bei der Export-und Importoperation die folgenden Optionen auswählen.

Wenn Sie keine Option auswählen, wenn Sie exportieren, ist sie beim Import nicht verfügbar.

Berichtsausgabeversionen einschließen

Sie können auswählen, dass die Berichtsausgabeversionen in Ihre Implementierung eingeschlossen werden sollen. Wenn Sie diese Option auswählen, können Sie auswählen, was zu tun ist, wenn ein Konflikt auftritt. Sie können die vorhandenen Berichtsausgabeversionen in der Zielumgebung durch die Versionen aus dem Bereitstellungsarchiv ersetzen oder die Zielumgebungsversionen beibehalten.

Ausführungsverlauf einschließen

Der Ausführungsverlauf eines Berichts zeigt Statistikdaten zum Status und zu den Zeiten an, in denen der Bericht „Anzeigen des Ausführungsprotokolls von Einträgen” auf Seite 266 in Ihrer Implementierung ausgeführt hat. Sie können auswählen, ob die Ausführungshistorie von Berichten eingeschlossen werden soll.

Wenn Sie diese Option auswählen, können Sie auswählen, was zu tun ist, wenn ein Konflikt auftritt. Sie können die vorhandenen Berichtslaufhistorien in der Zielumgebung durch die aus dem Bereitstellungsarchiv ersetzen oder die Zielumgebungshistorien beibehalten.

Zeitpläne einschließen

Sie können auswählen, ob Zeitpläne Kapitel 17, „Zeitpläne und Aktivitäten”, auf Seite 247 in Ihre Implementierung eingeschlossen werden sollen. Wenn Sie Zeitpläne nicht implementieren, werden sie aus den Jobs und Berichten in der Zielumgebung entfernt.

Wenn Sie diese Option auswählen, können Sie auswählen, was zu tun ist, wenn ein Konflikt auftritt. Sie können die vorhandenen Zeitpläne in der Zielumgebung durch solche aus dem Bereitstellungsarchiv ersetzen oder die Zeitpläne für die Zielumgebung beibehalten.

Wenn Sie Zeitpläne in der Implementierung importieren möchten, können Sie die Berechtigungsnachweise für den importierten Zeitplan in Ihre Berechtigungsnachweise ändern. Der Berechtigungsnachweis eines Zeitplans ist der Berechtigungsnachweis, der für die Ausführung des Berichts im Zeitplan verwendet wird. Dieser Berechtigungsnachweis bestimmt die Berechtigungen für den Bericht sowie die Funktionen, die für die Berichtsausführung gelten. Wenn für den Bericht die Eigenschaft **Als Eigner ausführen** nicht auf 'true' gesetzt ist, wird der Berechtigungsnachweis auch für den Zugriff auf die Datenquelle, die Datenverbindung und die Anmeldeobjekte verwendet. Die Änderung des Berechtigungsnachweises kann die Operation auf die folgenden Arten beeinflussen:

- Keine Auswirkung
- Bericht erstellt verschiedene Daten als Ergebnis der Auswahl einer anderen Verbindung oder Anmeldung in der Datenquelle
- Der Bericht kann nicht ausgeführt werden, da der Benutzer nicht über die entsprechenden Funktionen oder Berechtigungen verfügt.

Gehen Sie wie folgt vor, um die Berechtigungsnachweise für den importierten Zeitplan in die Berechtigungsnachweise der Person zu ändern, die den Import ausgeführt hat:

- Fügen Sie die erweiterte Einstellung CM.DeploymentUpdateScheduleCredential hinzu und setzen Sie den Wert auf **Wahr**. Siehe Prozedur, „Erweiterte Content Manager-Parameter festlegen” auf Seite 56.
- Wenn Sie mit dem Assistenten für den neuen Import „In eine Zielumgebung importieren” auf Seite 317in die Zielumgebung importieren, klicken Sie auf **Zeitpläne einschließen** , und wählen Sie **Vorhandene Einträge ersetzen** unter **Konfliktlösung**aus. Wählen Sie als Nächstes unter **Eigentumsrecht für Eintrag**die Option **Der Benutzer, der den Import ausführt**aus.

Einschließlich Cognos Gruppen und Rollen

Sie können auswählen, ob Cognos -Gruppen und -Rollen Kapitel 11, „Benutzer, Gruppen und Rollen”, auf Seite 187 in Ihre Implementierung eingeschlossen werden sollen.

Wenn Sie die Cognos -Gruppen und -Rollen implementieren, müssen Sie sie alle implementieren. Die folgenden integrierten Gruppen werden jedoch nicht implementiert:

- Anonym
- Alle authentifizierten Benutzer
- Jeder

Wenn Sie Gruppen implementieren, werden Mitglieder der Gruppe 'Systemadministratoren' mit den Mitgliedern dieser Gruppe bereits in der Zielumgebung zusammengeführt. Dadurch wird sichergestellt, dass die Zielumgebung für den Fall zugänglich ist, dass die implementierten Member nicht gültig sind. Möglicherweise müssen Sie die Mitgliedschaftsliste jedoch ändern, wenn die Implementierung abgeschlossen ist.

Wenn Sie diese Option auswählen, können Sie auswählen, was zu tun ist, wenn ein Konflikt auftritt. Sie können Gruppen und Rollen in der Zielumgebung durch solche aus dem Bereitstellungsarchiv ersetzen oder die Zielumgebungsgruppen und -rollen beibehalten.

Einschließlich Verteilerlisten und -kontakte

Sie können auswählen, ob Verteilerlisten und Kontakte in Ihrer Implementierung eingeschlossen werden sollen. Wenn Sie Verteilerlisten und Kontakte implementieren möchten, müssen Sie sie alle implementieren.

Wenn Sie diese Option auswählen, können Sie auswählen, was zu tun ist, wenn ein Konflikt auftritt. Sie können angeben, ob die Verteilerlisten und -kontakte in der Zielumgebung durch diejenigen aus dem Bereitstellungsarchiv ersetzt werden sollen oder ob die Zielverteilungslisten und -kontakte beibehalten werden sollen.

Datenquellen einschließen

Sie können auswählen, dass Datenquellen und die zugehörigen Verbindungen Kapitel 6, „Datenquellen und Verbindungen”, auf Seite 99 in Ihre Implementierung eingeschlossen werden sollen. Wenn Sie Datenquellen implementieren möchten, müssen Sie diese alle implementieren.

Sie können die Datenquellen mit oder ohne ihre Anmeldedaten implementieren. Wenn Sie die Anmeldedaten nicht implementieren, müssen Sie die Datenquellen entsprechend in der Zielumgebung konfigurieren. Wenn Sie die Anmeldedaten implementieren, müssen Sie das Bereitstellungsarchiv verschlüsseln.

Wenn Sie diese Option auswählen, können Sie auswählen, was zu tun ist, wenn ein Konflikt auftritt. Sie können angeben, ob die Datenquellen in der Zielumgebung durch die Datenquellen aus dem Bereitstellungsarchiv ersetzt werden sollen oder ob die Datenquellen der Zielumgebung beibehalten werden sollen.

Wenn Sie die Zieldatenquellen ersetzen und die Datenquellenverbindungen in den Quellen-und Zielumgebungen nicht übereinstimmen, können Sie Datenbankverbindungen verlieren. In diesem Fall

müssen Sie die Verbindung zu den Datenquellen in der Zielumgebung nach dem Import manuell wiederherstellen, indem Sie die Datenbankclientsoftware verwenden.

Einschließlich Zugriffsberechtigungen

Sie können auswählen, dass die Zugriffsberechtigungen „Zugriffsberechtigungen" auf Seite 300 in Ihre Implementierung eingeschlossen werden sollen.

Wenn Sie diese Option auswählen, können Sie auswählen, was zu tun ist, wenn ein Konflikt auftritt. Sie können angeben, ob die Zugriffsberechtigungen in der Zielumgebung durch die Berechtigungen aus dem Bereitstellungsarchiv ersetzt werden sollen oder ob die Zugriffsberechtigungen für die Zielumgebung beibehalten werden sollen.

Implementierungsdetails aufzeichnen

Sie können angeben, welche Art von Informationen in den Implementierungsdatensätzen gespeichert werden sollen, indem Sie die **Aufzeichnungsstufe** für die Implementierung festlegen. Die Menge an Informationen, die in den Datensätzen aufbewahrt werden, wirkt sich auf die Leistung aus.

Sie können die folgenden Aufzeichnungsstufen festlegen:

- **Basis**

  Speichert den Implementierungsfortschritt und die Übersichtsdaten. Dies ist die Standardoption.
- **Minimal**

  Speichert nur die Informationen zur Implementierungszusammenfassung. Für diese Option ist der geringste Speicher erforderlich.
- **Trace**

  Speichert alle Implementierungsdetails. Für diese Option ist der größte Speicher erforderlich.

Informationen zum Aufzeichnen von Implementierungsdetails, wenn ein ganzer Content-Store implementiert ist, finden Sie unter „Bereitstellungsverlauf" auf Seite 303.

Aspekte des Eigentumsrechts

Sie können das Eigentumsrecht für importierte Einträge an den Benutzer ändern, der den Import ausführt. Sie können diese Option zum Zeitpunkt des Exports oder Imports auswählen. Wenn Sie die Eigner aus der Quelle verwenden, werden die Eigner zusammen mit den Einträgen importiert. Sie können die Eigentümeroptionen auf neue Einträge oder auf neue und vorhandene Einträge anwenden.

Erweiterte Implementierungseinstellungen

Sie können erweiterte Einstellungen verwenden, um anzugeben, wie die Implementierung in Ihrer Umgebung funktioniert.

Mit den erweiterten Einstellungen können Sie

- Angabe, ob die Berichtsausgabe Teil der Implementierung ist
- Angeben, ob Konfigurationsobjekte und untergeordnete Elemente Teil der Implementierung sind

Angeben, ob die Berichtsausgabe Teil der Implementierung ist

Sie können angeben, ob die Berichtsausgabe Teil der Implementierung ist.

Es gibt zwei erweiterte Einstellungen, die Sie verwenden können:

- CM.DEPLOYMENTSKIPALLREPORTOUTPUT, um alle Berichtsausgaben von **Mein Inhalt** und **Teaminhalt**einzuschließen oder zu überspringen.

· CM.DEPLOYMENTSKIPUSERREPORTOUTPUT zum Einschließen oder Überspringen der Benutzerberichtsausgabe nur von **Mein Inhalt** .

Standardmäßig sind diese auf False (ausschließen) gesetzt. Wenn Sie die Standardeinstellung ändern möchten, setzen Sie sie auf "Wahr".

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf **IBM Cognos Administration** Kapitel 13, „Funktionen”, auf Seite 207verfügen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Aktionsmenü von **Systeme** auf **Eigenschaften festlegen**.
3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Klicken Sie neben **Erweiterte Einstellungen**auf **Bearbeiten** .
5. Wählen Sie **Über den übergeordneten Eintrag erfasste Einstellungen außer Kraft setzen**aus.
6. Geben Sie in der Spalte **Parameter** den Wert CM.DEPLOYMENTSKIPALLREPORTOUTPUT oder CM.DEPLOYMENTSKIPUSERREPORTOUTPUTEIN.
7. Geben Sie in der Spalte **Wert** die Einstellung ein, die Sie verwenden möchten.
8. Klicken Sie auf **OK**.
9. Klicken Sie auf der **Eigenschaften festlegen** -Seite auf **OK**.

Konfigurationsobjekte und ihre untergeordneten Elemente in Bereitstellungen einschließen

Setzen Sie die erweiterte Eigenschaft CM.DEPLOYMENTINCLUDECONFIGURATION auf "true", um Konfigurationsobjekte und deren untergeordnete Elemente als Teil von Implementierungen einzuschließen. In IBM Cognos Analyticsist der Wert für die Eigenschaft standardmäßig 'false'.

Vorbereitende Schritte

Sie müssen über die erforderlichen Berechtigungen für den Zugriff auf **IBM Cognos Administration** Kapitel 13, „Funktionen”, auf Seite 207verfügen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie auf den Pfeil für das Menü "Aktionen" neben **Systeme** , und klicken Sie auf **Eigenschaften festlegen**.
3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Klicken Sie neben **Erweiterte Einstellungen**auf **Bearbeiten** .
5. Wählen Sie **Über den übergeordneten Eintrag erfasste Einstellungen außer Kraft setzen**aus.
6. Geben Sie in der Spalte **Parameter** den Typ CM.DEPLOYMENTINCLUDECONFIGURATION.
7. Geben Sie in der Spalte **Wert** die Einstellung ein, die Sie verwenden möchten.
8. Klicken Sie auf **OK**.
9. Klicken Sie auf der **Eigenschaften festlegen** -Seite auf **OK**.

Regeln für die Auflösung von Implementierungskonflikten beim Importieren und Exportieren

Die Regeln für die Konfliktlösung gelten, wenn Sie in eine Zielumgebung importieren oder exportieren.

Die Regeln sind unterschiedlich, je nachdem, ob Sie den gesamten Content-Store oder ausgewählte öffentliche Ordner und Verzeichnisinhalte implementieren. Die Methode, die Sie auswählen, legt fest, welche Objekte in den Import eingeschlossen werden und wie Konflikte aufgelöst werden, wenn ein Objekt bereits in der Zielumgebung vorhanden ist.

Objekte im Content Store stellen Einträge im Portal und die Eigenschaften dieser Einträge dar. Beispielsweise stellt das Objekt 'reportView' einen Berichtsansichtseintrag im Portal dar, und das Objekt 'runHistory' stellt den Ausführungsverlauf eines Eintrags dar. Weitere Informationen zu Objekten finden Sie im IBM Cognos Software Development Kit *Entwicklerhandbuch*.

Objekte in **Öffentliche Ordner** übernehmen Implementierungsregeln standardmäßig, je nachdem, ob Sie den gesamten Content-Store oder nur ausgewählte **Öffentliche Ordner** -und Verzeichnisinhalte implementieren.

Konflikte können zwar nur während des Imports auftreten, nicht aber beim Export, werden jedoch dieselben Regeln verwendet, um Objekte im Archiv während des Exports zu verarbeiten. Wenn die Regel für ein Objekt KEEP ist, wird sie während einer Exportoperation nicht in das Archiv aufgenommen. Für jede andere Einstellung ist sie im Archiv enthalten.

Regeln zur Konfliktlösung

Ein Konflikt kann auftreten, wenn der Eintrag, den Sie aus dem Bereitstellungsarchiv importieren möchten, bereits im Zielinhaltsspeicher vorhanden ist.

In diesem Fall wird eine der folgenden Regeln für die Konfliktlösung verwendet, je nach dem Eintrag und den erweiterten Einstellungen, die Sie verwendet haben.

Tabelle 71. Regeln zur Konfliktlösung

Regel	**Beschreibung**
Ersetzen	Ersetzt den Eintrag und seine untergeordneten Elemente. Der Eintrag und alle zugehörigen untergeordneten Elemente werden aus dem Quelleninhaltsspeicher entfernt. Der neue Eintrag und alle seine untergeordneten Elemente werden dem Quelleninhaltsspeicher hinzugefügt.
Beibehalten	Behält den Eintrag bei. Die Eigenschaften des Eintrags und aller untergeordneten Elemente werden nicht aktualisiert. Vorhandene untergeordnete Elemente des Eintrags werden beibehalten. Neue Kinder können hinzugefügt werden.
Aktualisieren	Aktualisiert den Eintrag. Die Eigenschaften des Eintrags und seiner untergeordneten Elemente werden aktualisiert. Vorhandene untergeordnete Elemente des Eintrags werden beibehalten. Neue Kinder können hinzugefügt werden.
Zusammenführen	Führt die Eigenschaften der Einträge mit vorhandenen Einträgen zusammen.

Wenn für einen Eintrag keine untergeordneten Elemente vorhanden sind, haben die Ersetzung und die Aktualisierung das gleiche Endergebnis.

Inhalt

Alle Objekte im Inhaltsbereich des Content-Stores werden eingeschlossen und ersetzt, wenn Sie den gesamten Content-Store importieren.

Verzeichnis

Wenn Sie Datenquellen, Verbindungen und Anmeldungen einschließen und vorhandene Einträge beibehalten, werden die zugeordneten Objekte aus dem Archiv mit den Objekten in der Zielumgebung zusammengeführt. Auch wenn die Objekte zusammengeführt werden, gelten die Aufbewahrungsregeln weiterhin. Eine vollständige Zusammenführung kann nicht auftreten, weil einige Objekte gelöscht werden können.

Beachten Sie, dass diese Elemente, wenn Sie Cognos -Gruppen und -Rollen sowie Verteilerlisten und -kontakte einschließen möchten, in einem Ordner im Namespace gespeichert werden müssen, damit sie implementiert werden können.

Die Mitglieder von Verteilerlisten, Gruppen und Rollen im Archiv werden nicht mit dem Inhalt in der Zielumgebung zusammengeführt. Stattdessen werden die Gruppe der Verteilerlisten, Gruppen und Rollen mit dem bereits in der Zielumgebung vorhandenen Satz zusammengeführt. Die Mitglieder der Gruppe 'Systemadministratoren' werden jedoch immer zusammengeführt, wenn diese Gruppe importiert wird. Weitere Informationen finden Sie unter „Einschließlich Cognos Gruppen und Rollen” auf Seite 306.

Regeln zur Konfliktlösung für die Bereitstellung des gesamten Content Store

Die Standardregel zur Konfliktlösung für die Implementierung des gesamten Content-Stores ist 'replace'.

Ausnahmen von der Standardregel für Konfliktlösung sind in der folgenden Tabelle aufgeführt:

Tabelle 72. Vollständige Implementierung, Ausnahmen von der Standardregel zur Konfliktlösung

Objektname	**Konfliktlösungsregel**
OUTPUT, GRAPHIC, PAGE	Beibehalten, wenn · Die erweiterte Einstellung CM.DEPLOYMENTSKIPALLREPORTOUTPUT ist auf True gesetzt · Das Objekt befindet sich unter Benutzerkonten, und die erweiterte Einstellung CM.DEPLOYMENTSKIPUSERREPORTOUTPUT ist auf True gesetzt. Weitere Informationen zu den Einstellungen finden Sie unter „Angeben, ob die Berichtsausgabe Teil der Implementierung ist” auf Seite 307.
ACCOUNT	Aktualisieren Sie, wenn **Benutzeraccountinformationen einschließen** während der Implementierung ausgewählt wird, falls nicht. Weitere Informationen zum Einschließen von Benutzerkontoinformationen finden Sie unter „Gesamter Content-Store implementieren” auf Seite 302.
SESSION, CACHEOUTPUT, REPORTCACHE, REPORTMETADATACACHE, DEPLOYMENTDETAIL	Beibehalten

Tabelle 72. Vollständige Implementierung, Ausnahmen von der Standardregel zur Konfliktlösung (Forts.)	
Objektname	**Konfliktlösungsregel**
ORDNER, MRUFOLDER, SUBSCRIPTIONFOLDER	Ersetzen Sie das Objekt direkt unter Cognos -Namespace-Benutzerkontoobjekt (Ordner**Meine Ordner**) oder direkt unter dem Benutzeraccountobjekt des Drittanbieters (**Meine Ordner** -Ordner).
FÄHIGKEIT, SECUREDFUNKTION, KONFIGURATION, KONFIGURATIONSORDNER, DISPATCHER, VERZEICHNIS, NAMESPACE, NAMESPACEORDNER, PORTAL, PORTALPACKAGE, PORTALSKINFOLDER, PORTLETORDNER, PORTLETPRODUCER, PORTLET, PAGELETFOLDER, PAGELET, PAGELETINSTANCE, PORTLETINSTANCE	Aktualisieren
ROLE, GROUP	Ersetzen (aber Objekt-ID beibehalten).
CONTENT, ADMINFOLDER, TRANSIENTSTATEORDNER	Ersetzen. Beachten Sie, dass die Implementierungsoption "entireContentStoreReplace" nur mit einer Anwendung "Software Development Kit" in "false" (Aktualisieren) geändert werden kann. Weitere Informationen finden Sie in der Dokumentation zu Software Development Kit.
GESCHICHTE, HISTORYDETAIL, HISTORYDETAILANFRAGEARGUMENTE	Beibehalten, wenn unter ADMINFOLDER Objekt angegeben ist.

Regeln zur Konfliktlösung für partielle Implementierung

Wenn Sie öffentliche Ordner und Verzeichnisinhalte und nicht den gesamten Content-Store implementieren, können Sie den Inhalt auswählen, den Sie implementieren möchten.

Einige Regeln zur Konfliktlösung hängen von den Entscheidungen ab, die Sie treffen.

Wenn ein übergeordnetes Objekt aktualisiert wird, werden neue untergeordnete Elemente aus dem Bereitstellungsarchiv hinzugefügt und schließen sich der vorhandenen Gruppe von untergeordneten Elementen in der Zielumgebung an. Tritt ein Konflikt auf, ist die Konfliktlösungsregel, die Kinder zu ersetzen.

Da alle Jobschritte ersetzt werden, ist beim Importieren von JobStepDefinition-Objekten kein Konflikt möglich.

Wenn Sie Berichtsausgabeversionen und Ausführungshistorien einschließen und vorhandene Einträge beibehalten, werden die zugeordneten Objekte aus dem Archiv mit den Objekten in der Zielumgebung zusammengeführt. Auch wenn die Objekte zusammengeführt werden, gelten die Aufbewahrungsregeln weiterhin. Eine vollständige Zusammenführung kann nicht auftreten, weil einige Objekte gelöscht werden können.

Die Standardregel zur Konfliktlösung für partielle Bereitstellungen wird ersetzt.

Ausnahmen von der Standardregel für Konfliktlösung sind in der folgenden Tabelle aufgeführt:

Tabelle 73. Partielle Implementierung, Ausnahmen von der Standardregel zur Konfliktlösung

Objektname	**Konfliktlösungsregel**
REPORTVERSIONSQL	Hängt davon ab, ob **Berichtsausgabeversionen einschließen** gesetzt ist, um „Berichtsausgabeversionen einschließen" auf Seite 305zu ersetzen oder zu halten.
AUSGABE	Beibehalten, wenn die erweiterte Einstellung DEPLOYMENTSKIPREPORTOUTPUT auf True „Angeben, ob die Berichtsausgabe Teil der Implementierung ist" auf Seite 307gesetzt ist. Anderenfalls hängt davon ab, ob **Berichtsausgabeversionen einschließen** gesetzt ist, um „Berichtsausgabeversionen einschließen" auf Seite 305zu ersetzen oder zu halten.
GRAPHICPAGE	Beibehalten, wenn die erweiterte Einstellung DEPLOYMENTSKIPREPORTOUTPUT auf True „Angeben, ob die Berichtsausgabe Teil der Implementierung ist" auf Seite 307gesetzt ist. Anderenfalls hängt davon ab, ob **Berichtsausgabeversionen einschließen** gesetzt ist, um „Berichtsausgabeversionen einschließen" auf Seite 305zu ersetzen oder zu halten.
GESCHICHTE	Hängt davon ab, ob **Laufprotokoll einschließen** gesetzt ist, um „Ausführungsverlauf einschließen" auf Seite 305zu ersetzen oder zu halten.
ZEITPLAN	Hängt davon ab, ob **Zeitpläne einschließen** gesetzt ist, um „Zeitpläne einschließen" auf Seite 305zu ersetzen oder zu halten.
JOBSTEPDEFINITION	Ersetzen.
JOBDEFINITION	Aktualisieren und entfernen Sie alle JOBSTEPDEFINITION children.If PackageHistories is specified and packageHistoriesConflictResolution ist gesetzt, um zu ersetzen, entfernen Sie HISTORY-Objekte als auch.
DATENQUELLE, DATASOURCECONNECTION, DATASOURCENAMEBINDING	Hängt davon ab, ob **Datenquellen und Verbindungen einschließen** gesetzt ist, um„Datenquellen einschließen" auf Seite 306beizubehalten oder zu ersetzen.
DATASOURCESIGNON	Hängt davon ab, ob **Datenquellen und Verbindungen einschließen** und **Signons einschließen** gesetzt sind, um „Datenquellen einschließen" auf Seite 306beizubehalten oder zu ersetzen.

Tabelle 73. Partielle Implementierung, Ausnahmen von der Standardregel zur Konfliktlösung (Forts.)	
Objektname	**Konfliktlösungsregel**
DISTRIBUTIONSLISTE, KONTAKT	Hängt davon ab, ob **Verteilerlisten und Kontakte einschließen** gesetzt ist, um „Einschließlich Verteilerlisten und -kontakte" auf Seite 306beizubehalten oder zu ersetzen.
ROLE, GROUP	Hängt davon ab, ob **Cognos-Gruppen und -Rollen einschließen** gesetzt ist, um „Einschließlich Cognos Gruppen und Rollen" auf Seite 306beizubehalten oder zu ersetzen. (Wenn dieser Wert ersetzt werden soll, wird die Objekt-ID beibehalten.)
CACHEOUTPUT, REPORTCACHE, REPORTMETADATACACHE	Beibehalten

IBM Cognos -Einträge implementieren

Wenn Sie IBM Cognos -Software implementieren möchten, müssen Sie das Bereitstellungsarchiv in der Quellenumgebung exportieren und dann das Archiv in die Zielumgebung verschieben und dort importieren.

Sie können Ihre Implementierungsspezifikation in Ordnern auf die gleiche Weise organisieren, wie Sie alle Ihre Einträge organisieren.

Implementierung und Agenten

Die Implementierung kann Teil eines Agenten sein.

Implementierungszeitpläne und Ausführungsverlauf

Sie können die Implementierung so planen, dass sie automatisch zu einem bestimmten Zeitpunkt oder als Teil eines Jobs ausgeführt wird. IBM Cognos software saves the run history for each deployment specification. Nach dem Exportieren oder Importieren können Sie das Datum und die Uhrzeit sowie den Status der Implementierung anzeigen. Sie können auch alle Fehlernachrichten anzeigen, die durch die Implementierung erstellt wurden, und die Liste der Einträge, die exportiert oder importiert wurden. Weitere Informationen finden Sie unter Kapitel 17, „Zeitpläne und Aktivitäten", auf Seite 247.

Berechtigungen

Um IBM Cognos -Einträge zu implementieren, müssen Sie über Ausführungsberechtigungen für die **Verwaltungstasks** gesicherten Feature-und Transitberechtigungen für die geschützte **Verwaltung** -Funktion verfügen. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen", auf Seite 207.

Sie sollten auch zur Gruppe 'Systemadministratoren' gehören und über Lese-und Schreibzugriff auf den Cognos -Namespace verfügen, damit Sie die Gruppe 'Systemadministratoren' implementieren können. Weitere Informationen finden Sie unter „Zugriffsberechtigungen für einen Eintrag festlegen" auf Seite 200.

Wenn Sie einen Teil-Export von öffentlichen Ordnern und Verzeichnisinhalt „Ausgewählte öffentliche Ordner und Verzeichnisinhalte implementieren" auf Seite 304 durchführen, anstatt den gesamten Content-Store „Gesamter Content-Store implementieren" auf Seite 302zu exportieren, müssen Sie über Lese-und Transitberechtigungen für die Einträge verfügen, die Sie exportieren. Außerdem benötigen Sie Schreibberechtigungen, weil Sie beim Exportieren eine Implementierungsspezifikation und ein

Implementierungsprotokoll erstellen. Wenn Sie importieren, müssen Sie über Schreib-und Maßnahmenberechtigungen für die Einträge verfügen, die Sie importieren.

Voraussetzungen

IBM Cognos -Software und andere Produkte müssen in den Quellen-und Zielumgebungen installiert und konfiguriert werden. For more information, see the IBM Cognos *Installations-und Konfigurationshandbuch*.

Es wird empfohlen, den Content Manager-Service zu stoppen, bevor Sie exportieren und importieren. Dadurch wird verhindert, dass Benutzer unvorhersehbare Ergebnisse erhalten, wenn sie Operationen während der Implementierung ausführen. Wenn beispielsweise Benutzer Berichte in einem Paket anzeigen, während das Paket importiert wird, treten möglicherweise Fehler auf, wenn die Berichtsausgaben ersetzt werden. Weitere Informationen finden Sie unter „Stoppen und Starten von Disponenten und Services" auf Seite 45.

Bevor Sie beginnen, müssen Sie die Implementierung planen, um festzustellen, welche Implementierungsoptionen verwendet werden sollen und welche Einträge für die Implementierung von „Implementierungsplanung" auf Seite 300verwendet werden sollen. Möglicherweise möchten Sie eine Sicherung vor der Implementierung Kapitel 8, „Daten sichern", auf Seite 167durchführen.

Aus einer Quellenumgebung exportieren

Um die IBM Cognos -Einträge zu exportieren, erstellen oder ändern Sie eine Exportimplementierungsspezifikation und führen Sie dann den Export aus.

Sie können auch eine zuvor gespeicherte Implementierungsspezifikation für den Export oder für die erneute Implementierung Ihrer Einträge verwenden.

Die Einträge werden in ein Exportimplementierungsarchiv „Bereitstellungsarchive" auf Seite 299 in der Quellenumgebung exportiert. Später importieren Sie die Archiveinträge in die Zielumgebung. Mithilfe der Einträge aus dem Bereitstellungsarchiv können Sie die Einträge in der Zielumgebung aktualisieren.

Informationen zur Konfliktlösung bei Implementierungen finden Sie im Artikel „Regeln für die Auflösung von Implementierungskonflikten beim Importieren und Exportieren" auf Seite 308.

Wenn Sie exportieren, wählen Sie die zu implementierenden Einträge aus, und Sie legen die Optionen fest, die beim Importieren als Standardwerte verwendet werden.

Neue Exportimplementierungsspezifikation erstellen

Eine Exportimplementierungsspezifikation definiert den Inhalt, der exportiert werden muss.

Informationen zum Exportieren von Inhalten in einer Multi-Tenant- IBM Cognos Analytics -Umgebung finden Sie unter „Implementierung von TenantInhalten" auf Seite 351.

Vorbereitende Schritte

Wenn Sie beim Exportieren eines Content-Stores Datenquellenzugriffskonten beibehalten möchten, müssen Sie **Benutzeraccountinformationen einschließen**auswählen. Wenn Sie die Konfigurationsdaten beim Exportieren beibehalten möchten, können Sie die erweiterte Einstellung CM.DEPLOYMENTINCLUDECONFIGURATION auf TRUE setzen. Weitere Informationen finden Sie unter „Konfigurationsobjekte und ihre untergeordneten Elemente in Bereitstellungen einschließen" auf Seite 308.

Vorgehensweise

1. Öffnen Sie in der Quellenumgebung **IBM Cognos Administration**.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
3. Klicken Sie in der Symbolleiste auf das Symbol **Neuer Export**  . Der **Neuer Export** -Assistent wird angezeigt.

4. Geben Sie einen eindeutigen Namen und eine optionale Beschreibung und einen Anzeigentipp für die Implementierungsspezifikation ein. Wählen Sie den Ordner aus, in dem Sie ihn speichern möchten, und klicken Sie auf **Weiter**.
5. Wählen Sie aus, ob der gesamte Content Store exportiert werden soll oder ob ein Teilexport bestimmter Inhalte durchgeführt werden soll:
   - Um bestimmte Inhalte zu exportieren, klicken Sie auf **Wählen Sie öffentliche Ordner, Verzeichnis und Bibliotheksinhalte aus.**. Klicken Sie auf **Weiter** und fahren Sie mit Schritt 7 fort.
   - Um den gesamten Content Store zu exportieren, klicken Sie auf **Gesamten Content Store auswählen** , und wählen Sie aus, ob Benutzerkontoinformationen eingeschlossen werden sollen. Klicken Sie auf **Weiter** und fahren Sie mit Schritt 15 fort.
6. Klicken Sie auf der Seite **Inhalt der öffentlichen Ordner auswählen** auf **Hinzufügen**.
7. Wählen Sie auf der **Einträge auswählen** -Seite im Feld **Verfügbare Einträge** einen der folgenden Einträge oder ihren Inhalt aus:
   - **Öffentliche Ordner**

     Enthält Pakete und Ordner. Wählen Sie die Pakete und Ordner aus, die Sie exportieren möchten.
   - **Verzeichnis**

     Enthält Namensbereiche, Namensbereichsordner, Gruppen und Rollen sowie einzelne Benutzerkonten. Wenn Sie ein Benutzerkonto auswählen, wird der gesamte Inhalt, der dem Benutzer zugeordnet ist, einschließlich des Inhalts des Benutzers **Meine Ordner**, in den Export eingeschlossen.
   - **Bibliothek**

     Enthält Bibliotheks-Ressourcen, wie z. B. Visualisierungen.
8. Klicken Sie auf das Pfeilsymbol  , um die ausgewählten Elemente in das Feld **Ausgewählte Einträge** zu verschieben, und klicken Sie auf **OK**.
9. Führen Sie für jeden Eintrag, den Sie exportieren, einen der folgenden Schritte aus:
   - Wenn Sie möchten, dass der Eintrag einen anderen Namen in der Zielumgebung hat, oder wenn Sie die Zielposition ändern oder mehrsprachige Namen hinzufügen möchten, klicken Sie auf das Symbol **Bearbeiten**  , nehmen Sie die Änderungen vor und klicken Sie auf **OK**.
   - Wenn Sie nicht möchten, dass Benutzer auf die Einträge und ihren Inhalt zugreifen, wählen Sie das Kontrollkästchen in der Spalte **Nach dem Import inaktivieren** aus. Dies ist zum Beispiel nützlich, wenn Sie die Berichte testen möchten, bevor Sie sie in der Zielumgebung verfügbar machen.
10. Wählen Sie unter **Optionen**aus, ob Sie die Berichtsausgabeversionen, die Ausführungshistorie und die Zeitpläne sowie die Einträge im Fall eines Konflikts einschließen möchten.
11. Wählen Sie auf der Seite **Verzeichnisinhalt auswählen** aus, ob Sie Cognos -Gruppen und -Rollen, Verteilerlisten und -kontakte sowie Datenquellen und -verbindungen exportieren möchten und was mit den Einträgen im Fall eines Konflikts zu tun ist.
12. Wählen Sie auf der Seite **Allgemeine Optionen angeben** aus, ob Zugriffsberechtigungen und Verweise auf andere Namespaces als **IBM Cognos**eingeschlossen werden sollen und welche Einträge nach dem Import in der Zielumgebung Eigner der Einträge sein sollten.
13. Geben Sie die **Aufzeichnungsstufe** für die Implementierungshistorie an. Weitere Informationen finden Sie unter „Implementierungsdetails aufzeichnen" auf Seite 307.
14. Wählen Sie auf der **Bereitstellungsarchiv angeben** -Seite unter **Bereitstellungsarchiv**ein vorhandenes Bereitstellungsarchiv aus der Liste aus, oder geben Sie einen neuen Namen ein, um einen zu erstellen.

    Wenn Sie einen neuen Namen für das Bereitstellungsarchiv eingeben, verwenden Sie keine Leerzeichen im Namen. Wenn der Name der neuen Implementierungsspezifikation mit dem Namen eines vorhandenen Implementierungsarchivs übereinstimmt, werden die Zeichen _# am Ende des Namens hinzugefügt, wobei # eine Zahl wie 1 ist.

15. Klicken Sie unter **Verschlüsselung**auf **Verschlüsselungskennwort festlegen**, geben Sie ein Kennwort ein, und klicken Sie auf **OK**.
16. Klicken Sie auf **Weiter**.

    Die Übersichtsdaten werden angezeigt.
17. Überprüfen Sie die Übersichtsdaten, und klicken Sie auf **Weiter**.

    Wenn Sie die Informationen ändern möchten, klicken Sie auf **Zurück** und befolgen Sie die Anweisungen.
18. Geben Sie an, wie die Exportimplementierungsspezifikation ausgeführt werden soll:

    - Klicken Sie auf **Speichern und einmal ausführen** , und klicken Sie auf **Fertigstellen**, um jetzt oder später auszuführen. Geben Sie die Uhrzeit und das Datum für die Ausführung an. Klicken Sie anschließend auf **Ausführen**. Überprüfen Sie die Laufzeit und klicken Sie auf **OK**.
    - Klicken Sie auf **Speichern und planen** , und klicken Sie auf **Fertigstellen**, um einen Zeitplan zu einem wiederkehrenden Zeitpunkt zu planen Wählen Sie dann Frequenz, Start-und Enddatum aus, und klicken Sie auf **OK**.

      Tipp:

      Wenn Sie den Zeitplan vorübergehend inaktivieren möchten, wählen Sie das Kontrollkästchen **Zeitplan inaktivieren** aus.
    - Klicken Sie zum Speichern ohne Terminierung oder Ausführung auf **Nur speichern**und klicken Sie auf **Fertigstellen**.

Ergebnisse

Nachdem Sie den Export ausgeführt haben, können Sie Bereitstellungsarchiv verschieben. Sie können auch den Exportlaufverlauf „Anzeigen des Ausführungsprotokolls von Einträgen” auf Seite 266anzeigen.

Vorhandene Implementierungsspezifikation ändern

Sie können eine zuvor gespeicherte Implementierungsspezifikation für den Export oder für die erneute Implementierung Ihrer Einträge wiederverwenden.

Vorgehensweise

1. Öffnen Sie in der Zielumgebung **IBM Cognos Administration starten**.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
3. Klicken Sie in der Spalte **Aktionen** auf die Eigenschaftenschaltfläche  , um die Implementierungsspezifikation zu ändern, die Sie ändern möchten, und klicken Sie dann auf die Registerkarte **Exportieren** .
4. Ändern Sie die Implementierungsoptionen nach Bedarf.

   Tipp: Wenn Sie die Zielposition für den Export ändern möchten, klicken Sie auf die Schaltfläche 'Bearbeiten'  neben dem Exportnamen in der Spalte **Zielname** , im Abschnitt **Inhalt der öffentlichen Ordner** , und wählen Sie das gewünschte Paket bzw. den gewünschten Ordner aus.
5. Klicken Sie auf **OK**.

Ergebnisse

Dadurch werden die Optionen gespeichert, und Sie können den Export jetzt oder zu einem späteren Zeitpunkt ausführen. Weitere Informationen finden Sie unter „Ausführen eines Exports” auf Seite 316.

Ausführen eines Exports

Nachdem Sie ein neues Exportimplementierungsarchiv erstellt oder eine vorhandene exportiert haben, können Sie es ausführen.

Vorgehensweise

1. Klicken Sie in der Spalte **Aktionen** auf die Schaltfläche 'Ausführen mit Optionen'  .
2. Klicken Sie auf **Jetzt** , um den Export sofort auszuführen, oder klicken Sie auf **Später**, und geben Sie die Zeit ein, die der Export ausführen soll.

   Sie können auch eine Task planen, die auf einer wiederkehrenden Basis ausgeführt werden soll, und eine Liste geplanter Tasks anzeigen. Weitere Informationen finden Sie unter Kapitel 17, „Zeitpläne und Aktivitäten", auf Seite 247.

   Um Warnungen zu vermeiden, wenn Sie bei mehreren Namespaces angemeldet sind, bevor Sie den Export das nächste Mal ausführen, müssen Sie Ihre Berechtigungsnachweise erneuern.

Ergebnisse

Sie können das Bereitstellungsarchiv jetzt verschieben.

Implementierungsarchiv verschieben

Verschieben Sie das Bereitstellungsarchiv, das Sie in der Quellenumgebung erstellt haben, in die Zielumgebung.

Wenn die Quellen-und Zielumgebungen denselben Content-Store verwenden, können Sie importieren, ohne das Bereitstellungsarchiv zu verschieben.

Die Position, an der Bereitstellungsarchive gespeichert werden, wird im Konfigurationstool festgelegt. Die Standardposition ist *Installationsposition*/deployment.

Vorbereitende Schritte

Wenn Sie das Bereitstellungsarchiv an eine Position in einem LAN verschieben möchten, müssen Sie sicherstellen, dass genügend Plattenspeicherplatz vorhanden ist. Wenn Sie das Bereitstellungsarchiv nicht verschlüsselt haben, empfehlen wir Ihnen, es an einen sicheren Ort zu kopieren.

Vorgehensweise

1. Kopieren Sie das Bereitstellungsarchiv aus der Quellenumgebung in eine Position im LAN oder auf eine CD.
2. Kopieren Sie das Bereitstellungsarchiv aus dem LAN oder der CD in die Zielumgebung in der Position, die im Konfigurationstool festgelegt ist.

Ergebnisse

Sie können nun Konfigurationsobjekte einschließen, wenn Sie einen gesamten Content-Store importieren oder in die Zielumgebung importieren.

In eine Zielumgebung importieren

Erstellen Sie eine neue Importimplementierungsspezifikation, oder ändern Sie eine vorhandene Spezifikation, und führen Sie dann den Import aus.

Sie können unter Verwendung einer vorhandenen Implementierungsspezifikation importieren, wenn Sie sie zuvor ohne Import gesichert haben oder wenn Sie Ihre IBM Cognos -Einträge erneut implementieren möchten. Sie können die Einträge in der Zielumgebung mit Einträgen aus dem Bereitstellungsarchiv aktualisieren.

Informationen zur Konfliktlösung bei Implementierungen finden Sie im Artikel „Regeln für die Auflösung von Implementierungskonflikten beim Importieren und Exportieren" auf Seite 308.

Wenn Sie importieren, wählen Sie die Einträge aus, die exportiert wurden. Sie können entweder die Standardoptionen akzeptieren, die während des Exports festgelegt wurden, oder sie ändern. Sie können keine Optionen auswählen, die während des Exports nicht in das Bereitstellungsarchiv aufgenommen

wurden. Informationen dazu, wie bestimmte Objekte im Content-Store importiert werden, finden Sie unter „Regeln für die Auflösung von Implementierungskonflikten beim Importieren und Exportieren“ auf Seite 308.

Sie können den Assistenten 'Neuer Import' auch verwenden, um Einträge aus früheren Releases des Produkts zu aktualisieren. Sie können die Berichtsspezifikationen während des Imports aktualisieren oder sie zu einem späteren Zeitpunkt mithilfe des Assistenten 'Neues Berichtsupgrade' aktualisieren. Weitere Informationen finden Sie unter „Aktualisieren von Berichtsspezifikationen“ auf Seite 321.

Wenn Sie einen Import ausführen, werden Inhaltsspeicher-IDs gelöscht und neue IDs zugeordnet. Wenn die Geschäfts-IDs beibehalten werden müssen, weil sie von bestimmten IBM Cognos -Funktionen verwendet werden, können Sie die Filial-IDs beibehalten. Weitere Informationen finden Sie unter „Inhalt-ID-Zuordnung“ auf Seite 321.

Informationen zur Verwendung einer vorhandenen Importimplementierungsspezifikation finden Sie unter „Vorhandene Importimplementierungsspezifikation ändern“ auf Seite 319 .

Wenn Sie eine partielle Implementierung bestimmter öffentlicher Ordner und Verzeichnisinhalte durchführen, zeigt der Importassistent an, ob Pakete und Ordner bereits in der Zielumgebung vorhanden sind und ob das Datum und die Uhrzeit der letzten Änderung angegeben wurden. Sie können diese Informationen verwenden, um zu entscheiden, wie Konflikte gelöst werden können. Wenn Sie erneut implementieren, zeigt der Assistent außerdem an, ob die Pakete und Ordner in der ursprünglichen Implementierung waren.

Neue Importimplementierungsspezifikation erstellen

Eine Importimplementierungsspezifikation definiert den Inhalt, der importiert werden muss.

Informationen zum Importieren von Inhalt in einer Multi-Tenant- IBM Cognos Analytics -Umgebung finden Sie unter „Implementierung von TenantInhalten“ auf Seite 351.

Vorgehensweise

1. Öffnen Sie in der Zielumgebung **IBM Cognos Administration**.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
3. Klicken Sie in der Symbolleiste auf das Symbol **Neuer Import**  . Der **Neuer Import** -Assistent wird angezeigt.
4. Klicken Sie im Feld **Bereitstellungsarchiv** auf das Implementierungsarchiv, das Sie importieren möchten.
5. Geben Sie das Kennwort ein, das zum Verschlüsseln des Inhalts verwendet wurde, und klicken Sie auf **OK** und dann auf **Weiter**.
6. Geben Sie einen eindeutigen Namen und eine optionale Beschreibung sowie eine Anzeigenspitze für die Implementierungsspezifikation ein, wählen Sie den Ordner aus, in dem Sie ihn speichern möchten, und klicken Sie auf **Weiter**.
7. Wählen Sie den Inhalt aus, den Sie in den Import einschließen möchten.

   Tipp: Um sicherzustellen, dass die erforderlichen Zieleinträge im Zielinhaltsspeicher vorhanden sind, klicken Sie auf die Schaltfläche 'Bearbeiten'  neben dem Paket, und überprüfen Sie die Position. Wenn Sie möchten, können Sie die Zielposition jetzt ändern.
8. Wählen Sie die gewünschten Optionen zusammen mit Ihrer Auswahl für die Konfliktlösung für Optionen aus, die Sie auswählen.
9. Wählen Sie auf der Seite **Allgemeine Optionen angeben** aus, ob Zugriffsberechtigungen und Verweise auf andere Namespaces als **IBM Cognos**eingeschlossen werden sollen und welche Einträge nach dem Import in der Zielumgebung Eigner der Einträge sein sollten.
10. Geben Sie die **Aufzeichnungsstufe** für die Implementierungshistorie an. Weitere Informationen finden Sie unter „Implementierungsdetails aufzeichnen“ auf Seite 307.
11. Klicken Sie auf **Weiter**.

12. Überprüfen Sie die Übersichtsdaten, und klicken Sie auf **Weiter**.
13. Wählen Sie aus, wie die Importimplementierungsspezifikation ausgeführt werden soll:
    - Klicken Sie auf **Speichern und einmal ausführen** , und klicken Sie auf **Fertigstellen**, um jetzt oder später auszuführen. Geben Sie die Uhrzeit und das Datum für die Ausführung an. Klicken Sie anschließend auf **Ausführen**. Überprüfen Sie die Laufzeit und klicken Sie auf **OK**.
    - Klicken Sie auf **Speichern und planen** , und klicken Sie auf **Fertigstellen**, um einen Zeitplan zu einem wiederkehrenden Zeitpunkt zu planen Wählen Sie dann Frequenz, Start-und Enddatum aus, und klicken Sie auf **OK**.

      Tipp: Wenn Sie den Zeitplan vorübergehend inaktivieren möchten, wählen Sie das Kontrollkästchen **Zeitplan inaktivieren** aus. Informationen zum Anzeigen des Zeitplanstatus finden Sie unter Kapitel 17, „Zeitpläne und Aktivitäten” , auf Seite 247.
    - Klicken Sie zum Speichern ohne Planung oder Ausführung auf **Nur speichern** und klicken Sie dann auf **Fertigstellen**.

      Wenn Sie den Import ausführen, haben Sie die Möglichkeit, das Upgrade der Berichtsspezifikation zu aktivieren. Wenn Sie die Implementierungsspezifikation zu diesem Zeitpunkt nicht aktualisieren möchten, können Sie das Upgrade später durchführen. Weitere Informationen finden Sie unter „Aktualisieren von Berichtsspezifikationen” auf Seite 321.

Ergebnisse

Nachdem Sie den Import ausgeführt haben, können Sie Implementierung testen. Sie können auch den Import-Ausführungsprotokoll „Anzeigen des Ausführungsprotokolls von Einträgen” auf Seite 266anzeigen.

Vorhandene Importimplementierungsspezifikation ändern

Sie können eine vorhandene Implementierungsspezifikation ändern.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
2. Klicken Sie in der Spalte **Aktionen** auf die Eigenschaftenschaltfläche  , um die Implementierungsspezifikation zu ändern, die Sie ändern möchten, und klicken Sie dann auf die Registerkarte **Importieren** .
3. Ändern Sie die Implementierungsoptionen nach Bedarf.

   Tipp: Wenn Sie die Position des Importziels ändern möchten, klicken Sie auf die Schaltfläche 'Bearbeiten'  neben dem Importnamen in der Spalte **Zielname** , im Abschnitt **Inhalt der öffentlichen Ordner** , und wählen Sie das gewünschte Paket bzw. den gewünschten Ordner aus.
4. Klicken Sie auf **OK**.

Ergebnisse

Dadurch werden die Optionen gespeichert, und Sie können den Import jetzt oder zu einem späteren Zeitpunkt ausführen. Weitere Informationen finden Sie unter „Import ausführen” auf Seite 319.

Import ausführen

Nachdem Sie eine Importimplementierungsspezifikation erstellt oder geändert haben, führen Sie den Import aus.

Vorgehensweise

1. Klicken Sie in der Spalte **Aktionen** auf die Schaltfläche 'Ausführen mit Optionen'  .

2. Klicken Sie auf **Jetzt** , um den Import sofort auszuführen, oder klicken Sie auf **Später**und geben Sie die Zeit ein, die der Import ausgeführt werden soll.
3. Wenn Sie ein Upgrade für die Berichtsspezifikationen durchführen möchten, klicken Sie auf **Führen Sie ein Upgrade aller Berichtsspezifikationen auf die neueste Version durch**.

   Sie können auch eine Task planen, die auf einer wiederkehrenden Basis ausgeführt werden soll, und eine Liste geplanter Tasks anzeigen. Weitere Informationen finden Sie unter Kapitel 17, „Zeitpläne und Aktivitäten", auf Seite 247.
4. Um anzugeben, wie Inhalts-IDs zugeordnet werden sollen, wählen Sie unter **Inhalt-IDs** die Option
   - **Neue IDs beim Import zuordnen** , um die vorhandenen Inhalts-IDs durch neue IDs zu ersetzen
   - **Beim Import keine neuen IDs zuordnen** , um vorhandene Inhalts-IDs beim Import beizubehalten

Ergebnisse

Sie können jetzt Implementierung testen.

Konfigurationsobjekte in den Import des gesamten Content Store einschließen

Sie können Konfigurationsobjekte einschließen, wenn Sie einen gesamten Content-Store importieren.

Vorbereitende Schritte

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 zur Gruppierung von Dispatchern verwendet werden. Weitere Informationen finden Sie unter „Regeln zur Konfliktlösung für die Bereitstellung des gesamten Content Store" auf Seite 310.

Es wird empfohlen, Konfigurationsobjekte nicht zu importieren. Die Dispatcher sollten in Ihrer Zielumgebung konfiguriert werden, bevor Sie Daten aus einer Quellenumgebung importieren. Wenn Sie Konfigurationsobjekte importieren müssen, sollten Sie entweder die Quellen-Dispatcher-Services vor dem Import stoppen oder die IBM Cognos -Software in der Zielumgebung nach dem Import erneut starten. Andernfalls können Fehler mit dem Status der Dispatcher auftreten. Wenn Sie Konfigurationsobjekte importieren möchten, müssen Sie auf eine kurze Unterbrechung der Services vorbereitet sein.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Dispatcher konfigurieren" auf Seite 518aus.
2. For the **ContentManagerService**, type **`CM.DEPLOYMENTINCLUDECONFIGURATION`** as the **Parameter** name.
3. Geben Sie **Wahr** als Wert für diesen Parameter ein und klicken Sie auf **OK**.

Implementierte Anwendungen testen

Nachdem Sie die Pakete aus dem Bereitstellungsarchiv importiert haben, überprüfen Sie, ob alle Einträge erfolgreich in der Zielumgebung implementiert wurden.

Sie können Ihre Implementierung testen, indem Sie

- Ausführen des Ausführungsprotokolls für eine Implementierung
- Sicherstellen, dass die richtigen Pakete und Ordner zusammen mit ihrem Inhalt importiert wurden
- Sicherstellung, dass die Datenquellen, Verbreitungslisten und Kontakte sowie Cognos -Gruppen und -rollen importiert wurden
- Überprüfung der Berechtigungen für die importierten Einträge

- Sicherstellung, dass die Zeitpläne importiert wurden
- Sicherstellung, dass alle Verweise auf umbenannte Pakete aktualisiert wurden
- importierte Berichte und Berichtsansichten ausführen

Aktualisieren von Berichtsspezifikationen

Wenn Sie bei der Ausführung des Importassistenten keine Upgradeberichtsspezifikationen durchgeführt haben, können Sie sie mit dem Assistenten für neue Berichte aktualisieren aktualisieren.

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. Melden Sie sich als Administrator mit Ausführungsberechtigungen für die **Inhaltsverwaltung** -Funktion an.
2. Öffnen Sie **IBM Cognos Administration**.
3. Klicken Sie auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
4. Klicken Sie in der Symbolleiste auf den Pfeil auf der neuen Schaltfläche für die Inhaltsverwaltung  und klicken Sie dann auf **Neues Berichtsupgrade** .
5. Geben Sie einen Namen für die Upgrade-Task und, wenn Sie möchten, eine Beschreibung und einen Anzeigentipp ein. Klicken Sie auf **Weiter**.
6. 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.
7. 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.

Inhalt-ID-Zuordnung

Wenn Sie eine Importimplementierung ausführen, können Sie auswählen, wie Inhalts-IDs für Objekte im Content-Store zugeordnet werden sollen.

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 die Inhalts-IDs beibehalten müssen, z. B. beim Archivieren der Berichtsausgabe in einem externen Berichtsrepository. Wenn dies der Fall ist, können Sie bei der Ausführung des Imports die Inhalts-IDs beibehalten. Weitere Informationen zum Zuordnen von IDs beim Importieren von Objekten finden Sie unter „Import ausführen" auf Seite 319.

Die Aufbewahrung von Inhalts-IDs kann auf eine Teilimplementierung oder eine Implementierung des gesamten Content-Stores angewendet werden.

Content-ID-Konflikte

Wenn Sie vorhandene Inhalts-IDs beibehalten, können Konflikte beim Import auftreten. Hier sind die Konfliktsituationen, die auftreten können.

Tabelle 74. Konflikt mit übereinstimmender Inhalts-ID

Informationen	Details
Beschreibung	Wenn ein importiertes Objekt in der Zielumgebung an einer anderen Position, aber mit einer übereinstimmenden Inhalts-ID vorhanden ist, wird die ID beim Import nicht beibehalten, sondern durch eine neu generierte ID ersetzt. Das Objekt, das in der Zielumgebung vorhanden ist, könnte eine andere Version desselben Objekts sein, oder es könnte ein völlig anderes Objekt sein.
Warnung	In einer Warnung wird beschrieben, dass der Inhalt nicht beibehalten wurde. Wenn die Sicherheitsberechtigungen dies zulassen, wird angegeben, welches Objekt in der Zielumgebung in Konflikt steht. Es werden keine Informationen zur Lösung des Konflikts ausgegeben.
Auflösung	Zur Behebung von Konflikten mit Inhalts-IDs können Sie · Nehmen Sie nach dem Import keine Änderungen an den Inhalts-IDs vor, und behalten Sie die IDs in ihrer Form bei. Alle Links für das importierte Objekt würden nun auf das Zielumgebungsobjekt verweisen, bei dem es sich wahrscheinlich um eine ältere Version desselben Objekts handelt. Wenn die Inhalts-ID für das importierte Objekt nicht von außerhalb des Content-Stores referenziert wird, sind nach dem Import keine defekten externen Verweise vorhanden. Das importierte Objekt ist weiterhin als separates Objekt vorhanden. · Löschen Sie das importierte Objekt und das Objekt in der Zielumgebung. Wenn das Objekt erneut importiert wird, wird das Objekt mit seiner Inhalts-ID an dieselbe Position hinzugefügt. · Aktualisieren Sie das Zielobjekt manuell mit Eigenschaften aus dem importierten Objekt. Alle Links für das Objekt werden beibehalten, da sich die Inhalts-ID nicht geändert hat. Das importierte Objekt konnte dann gelöscht werden.

Tabelle 75. Konflikt mit unterschiedlicher Inhalts-ID

Informationen	Details
Beschreibung	Wenn ein importiertes Objekt in der Zielumgebung an derselben Position, aber mit einer anderen Inhalts-ID vorhanden ist, bleibt die ID beim Import erhalten und ersetzt die vorhandene ID in der Zielumgebung.
Warnung	Es wird keine Warnung ausgegeben.
Auflösung	Beachten Sie, dass alle vorhandenen externen Verweise auf die Zielinhalts-ID, falls vorhanden, dauerhaft verloren gehen, wenn die Inhalts-ID ersetzt wird.

Human Task-und Anmerkungsservices implementieren

Der Inhalt für die Human Task-und Annotation-Services wird getrennt vom Hauptinhaltsspeicher gespeichert. Dieser Inhalt kann in derselben Datenbank gespeichert werden wie der Content Store als verschiedene Tabellen oder in einer separaten Datenbank. Um diesen Inhalt zu implementieren, werden Scripts verwendet, und nicht das Implementierungstool.

Die Prozedur in diesem Thema beschreibt die Verwendung von Scripts für die Implementierung von Benutzertask-und Annotation-Service-Inhalten. Informationen zur Verwendung von Scripts für die Implementierung von IBM Cognos -Arbeitsbereichskommentaren finden Sie unter „IBM Cognos -Arbeitsbereichskommentare implementieren" auf Seite 324.

Sie implementieren sie, indem Sie eine Stapeldatei ausführen, die Ihre Benutzertasks oder Annotationen aus einer Quellendatenbank abruft. Anschließend führen Sie eine andere Stapeldatei aus, um sie auf einem Zielserver zu installieren.

Vorgehensweise

1. Erstellen Sie Taskdaten in Ihrer Datenbank, indem Sie eine Auswahl von Tasks erstellen, die auf gültige Berichte verweisen.

   Anweisungen zum Erstellen von Benutzertasks finden Sie im IBM Cognos Event Studio *Benutzerhandbuch*. Weitere Informationen zu Anmerkungen (Kommentare) finden Sie im *IBM Cognos Arbeitsbereich 'Benutzerhandbuch'*.
2. Öffnen Sie auf dem Quellenserver eine Eingabeaufforderung in *Installationsposition*/bin.
3. Führen Sie das Datei htsDeployTool mit den folgenden Argumenten aus:

   `htsDeployTool -camUsername` *CamUsername* `-camPassword` *camPassword* `-camNamespace` *camNamespace* `-exportFile` *exportFileName* `-Kennwort` *exportFilePassword*

   wobei:

   · *CamUsername* ist der Benutzername für den Namespace.

   · *camPassword* ist das Benutzerkennwort für den Namespace.

   · *camNamespace* ist der Name des Namespace.

   · *exportFileName* ist der Name der Exportdatei, die erstellt wird, z. B. "HumanTaskExportFile1".

   · *exportFilePassword* ist das Kennwort für die Exportdatei.

   Schließen Sie Argumente ein, die Leerzeichen in Anführungszeichen enthalten. Vor Sonderzeichen mit einem Backslash. Beispiel:

   ```
   htsDeployTool -exportFile "jan \'s file"-password test2Password
   -camNamespace default -camUsername myId -camPassword meinKennwort
   ```

   Um anonymen Zugriff zu ermöglichen, lassen Sie die -cam-Argumente weglassen.

   Um Anmerkungen zu exportieren, fügen Sie das Argument `-persistenceUnit-Anmerkungenhinzu`. Beispiel:

   ```
   -camPassword < camPassword> -camNameSpace < camNamespace> -exportfile
   AnnotationExportFile1-password < exportFilePassword> -persistenceUnit-
   Annotationen.
   ```
4. Stellen Sie sicher, dass die Datei < exportFileName> .xml.gz in *Installationsposition*/deployment erstellt wurde. Beispiel: HumanTaskExportFile1.xml.gz. Kopieren Sie sie.
5. Fügen Sie auf dem Zielserver die Datei < exportFileName> .xml.gz in *Installationsposition*/deployment ein.
6. Öffnen Sie auf dem Zielserver eine Eingabeaufforderung in *Installationsposition*/bin, und führen Sie das Datei htsDeployTool mit den folgenden Argumenten aus:

   `htsDeployTool -camUsername` *CamUsername camPassword* `-camNamespace` *camNamespace* `-importFile` *importFileName* `-Kennwort` *importFilePassword*

   wobei:

   · *CamUsername* ist der Benutzername für den Namespace.

   · *camPassword* ist das Benutzerkennwort für den Namespace.

   · *camNamespace* ist der Name des Namespace.

· *importFileName* ist der Name der Datei, die Sie in Schritt 3 erstellt haben.

· *importFilePassword* ist das Kennwort für die Datei, die Sie in Schritt 3 erstellt haben.

Weitere Syntaxtipps finden Sie in Schritt 3.

IBM Cognos -Arbeitsbereichskommentare implementieren

You can deploy IBM Cognos Workspace comments using the following procedure.

Vorgehensweise

1. Exportieren Sie den Content-Store auf dem Computer mit den Annotationen, die implementiert werden sollen.

   Informationen zum Exportieren eines Content-Stores finden Sie im Artikel „Neue Exportimplementierungsspezifikation erstellen" auf Seite 314.
2. Öffnen Sie auf dem Quellenserver eine Eingabeaufforderung im Ordner install_location/bin.
3. Führen Sie im Ordner "bin" die Datei "htsDeployTool" mit den folgenden Argumenten aus:

   htsDeployTool -persistenceUnit-Annotationen -camUsername *CamUsername* -camPassword *camPassword* -camNamespace *camNamespace* -exportFile *exportFileName* -password *exportFilePassword*

   Dabei ist

   CamUsername ist der Benutzername für den Namensbereich.

   camPassword ist das Benutzerkennwort für den Namensbereich.

   camNamespace ist der Name des Namespace.

   exportFileName ist der Name der Exportdatei, die erstellt wird. Beispiel: HumanTaskExportFile1

   Beispiel: htsDeployTool -persistenceUnit Annotationen -exportFile myFile-password test2Password -camNamespace default -camUsername myId -camPassword myPassword

   Um anonymen Zugriff zu ermöglichen, lassen Sie die -cam-Argumente weglassen.
4. Stellen Sie sicher, dass die Datei *exportFileName*'.xml.gz' in 'install_location/deployment' erstellt wurde. Beispiel: HumanTaskExportFile1.xml.gz. Kopieren Sie sie.
5. Importieren Sie auf dem Zielserver eine Implementierung. Informationen zu Implementierungs-und Importspezifikationen finden Sie unter „Implementierungsspezifikationen" auf Seite 299.
6. Fügen Sie auf dem Zielserver die Datei *exportFileName*'.xml.gz' in 'install_location/deployment' ein.
7. Öffnen Sie auf dem Zielserver eine Eingabeaufforderung in install_location/bin, und führen Sie das htsDeployTool mit den folgenden Argumenten aus:

   htsDeployTool -persistenceUnit-Annotationen -camUsername *CamUsername* -camPassword *camPassword* -camNamespace *camNamespace* -importFile *importFileName* -password *importFilePassword*

   Dabei ist

   CamUsername ist der Benutzername für den Namensbereich.

   camPassword ist das Benutzerkennwort für den Namensbereich.

   camNamespace ist der Name des Namespace.

   importFileName ist der Name der Exportdatei, die Sie in Schritt 3 erstellt haben.

   importFilePassword ist das Kennwort für die Datei, die Sie in Schritt 3 erstellt haben.

Speicherung und Berichterstellung in IBM Cognos -Arbeitsbereichskommentaren

In diesem Abschnitt finden Sie Informationen zum Speichern und zur Berichterstellung zu Cognos -Arbeitsbereichskommentaren.

Kommentare speichern

Kommentare werden in ihren eigenen Datenbanktabellen gespeichert, die sich entweder in derselben Datenbank wie der Content Store oder in einer separaten Datenbank befinden können. Die Eigenschaft "Human Task and Annotation Services" in IBM Cognos Konfiguration definiert die Datenbankverbindung zur Datenbank, in der die Anmerkungstabellen gespeichert werden. Wenn keine Datenbankverbindung für Benutzertaskservice und Anmerkungsserviceeigenschaft angegeben ist, werden die Anmerkungstabellen in der Content Store-Datenbank erstellt.

Die Eigenschaft "Human Task and Annotation Services" definiert auch die Datenbankverbindung für die Human Task-Service-Tabellen. Obwohl der Benutzertaskservice und der Anmerkungsservice eine Datenbankverbindung gemeinsam nutzen, sind die Annotation-und Benutzertasktabellen getrennt. Anmerkungstabellen werden mit den ANS_-und Benutzertaskservicetabellen mit HTS_ vorfixiert.

Benutzer werden Scripts zum Exportieren und Importieren von Anmerkungs-und Benutzertaskdaten aus den Tabellen auf den Ziel IBM Cognos -Server bereitgestellt. Die Scripts erleichtern Aktivitäten wie das Sichern und Wiederherstellen von Kommentaren und das Implementieren von Kommentaren zwischen Servern.

Berichterstattung über Kommentare

In IBM Cognos Analyticsgibt es keine Ansicht oder IBM Cognos Framework Manager-Modelldarstellung von Cognos -Arbeitsbereichskommentaren, die aus der Box enthalten sind. Sie können jedoch ein Modell basierend auf den Datenbanktabellen für Anmerkungsservice in Framework Manager erstellen. Die Tabellen, die einfach sind, können verwendet werden, um den Kommentar oder Anmerkungstext zu finden, die Person, die den Kommentar erstellt hat, das Datum, an dem der Kommentar erstellt wurde, und den Bericht, dem der Kommentar zugeordnet ist. Sie können auch über den Kontext eines Kommentars berichten, indem Sie ein Berichtsmodell oder eine Abfrage für das Schema erstellen, in dem die Kommentare gespeichert werden. Die Dimensionen, Dimensionselemente, Metadatenelemente und Datenelemente stellen den Kontext der Annotation in dem Bericht dar.

Kapitel 20. Pakete

Sie können Pakete für Cognos PowerCube-und SAP BW-Datenquellen über IBM Cognos Administration erstellen.

Ein Modellierer kann ein Paket erstellen, während PowerCubes von Transformer veröffentlicht werden. Weitere Informationen finden Sie im Transformer *Benutzerhandbuch*.

Ein Modellierer kann auch Pakete mit Framework Manager erstellen und veröffentlichen. Informationen hierzu finden Sie im Framework Manager *Benutzerhandbuch*.

Erstellen eines Pakets für einen PowerCube

Bevor Sie eine PowerCube-Datenquelle in einem der IBM Cognos -Studios verwenden können, müssen Sie ein Paket erstellen.

Wenn Sie eine PowerCube-Datenquelle erstellen, haben Sie die Möglichkeit, ein Paket mit Ihrer neuen Datenquelle zu erstellen. Sie können auch ein Paket für eine vorhandene PowerCube-Datenquelle erstellen.

Um diese Tasks ausführen zu können, müssen Sie über Ausführungsberechtigungen für das gesicherte Feature "Datenquellenverbindungen" verfügen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Datenquellenverbindungen**.
2. Wählen Sie die neue Schaltfläche für die Datenquelle aus.
3. Führen Sie die Schritte in der **Assistent 'Neue Datenquelle'**aus.
   - Wählen Sie auf der **Verbindung angeben** -Seite in der Liste **Typ** die Option **IBM Cognos PowerCube**aus.
   - Wählen Sie auf der Seite **Fertigstellen** die Option **Paket erstellen**aus.

SAP BW-Pakete

Bevor Sie eine SAP BW-Datenquelle in einem der IBM Cognos -Studios verwenden können, müssen Sie ein Paket erstellen.

When you create a SAP BW data source from IBM Cognos Administration, you are given the option to create a package using your new data source. Sie können auch ein Paket für eine vorhandene SAP BW-Datenquelle erstellen. Weitere Informationen finden Sie unter „Datenquellenverbindungen” auf Seite 130.

Informationen zum Bearbeiten eines SAP BW-Pakets, nachdem es erstellt wurde, finden Sie unter „SAP BW-Paket bearbeiten” auf Seite 328.

Informationen zum Festlegen der maximalen Anzahl von Objekten, die in SAP BW-Paketen verwendet werden, finden Sie unter „Festlegen der maximalen Anzahl von Objekten, die in SAP BW-Paketen verwendet werden” auf Seite 328 .

Um diese Tasks ausführen zu können, müssen Sie über Ausführungsberechtigungen für das gesicherte Feature "Datenquellenverbindungen" verfügen, siehe Kapitel 13, „Funktionen”, auf Seite 207.

Sie können festlegen, wie viele Objekte in einem SAP BW-Paket verwendet werden können. Informationen zum Erstellen und Veröffentlichen von Paketen mit Framework Manager finden Sie im Framework Manager *Benutzerhandbuch*.

SAP BW-Paket erstellen

Die Prozedur zum Erstellen eines SAP BW-Pakets ist wie folgt.

Informationen zu diesem Vorgang

Weitere Informationen finden Sie unter „SAP Business Information Warehouse (SAP BW)-Datenquellen” auf Seite 123.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Datenquellenverbindungen**.
2. Wählen Sie die neue Schaltfläche für die Datenquelle aus.
3. Führen Sie die Schritte in der **Assistent 'Neue Datenquelle'**aus.
   - Wählen Sie auf der **Verbindung angeben** -Seite in der Liste **Typ** die Option **SAP BW**aus.
   - Wählen Sie auf der Seite **Fertigstellen** die Option **Paket erstellen**aus.

SAP BW-Paket bearbeiten

Die Prozedur zum Bearbeiten eines SAP BW-Pakets ist wie folgt.

Vorgehensweise

1. Klicken Sie auf **Mehr** neben dem Paket und klicken Sie dann auf **Paket bearbeiten**.
2. Wählen Sie eine der folgenden Optionen aus:
   - Um die Metadatenauswahl zu ändern, klicken Sie auf **Metadatenauswahl ändern**. Kehren Sie zu Schritt 5 in „SAP BW-Paket erstellen” auf Seite 328zurück.
   - Klicken Sie zum Bearbeiten der Paketvariablen auf **Variablen bearbeiten**. Klicken Sie auf den Wert, den Sie bearbeiten möchten, und wählen Sie dann die neue Variable aus. Klicken Sie auf **OK**.
   - Um die Paketeinstellungen zu ändern, klicken Sie auf **Paketeinstellungen ändern**und wählen Sie **Dynamischen Abfragemodus verwenden**aus.

Festlegen der maximalen Anzahl von Objekten, die in SAP BW-Paketen verwendet werden

Sie können die maximale Anzahl von Cubes und Info-Abfragen festlegen, die bei der Erstellung eines SAP BW-Pakets eingeschlossen werden können.

Je länger ein SAP BW-Import ausgeführt wird, desto mehr Zeit verbringt der Server die Verarbeitung der Anforderung, was sich auf seine Leistung für andere Anwendungen auswirken könnte. Finden Sie ein Gleichgewicht zwischen der Anzahl der Cubes und Informationsabfragen, die häufig von Benutzern benötigt werden, und der möglichen Auswirkung auf die Serverleistung.

Die folgenden Parameter (case-sensitive) sind verfügbar:

- **`com.ibm.cognos.metadatauiservice.sap.maxcubes`**

  Die maximale Anzahl von Cubes, die in einem SAP BW-Paket verwendet werden können. Gültige Einstellungen sind null und größer. Der Standardwert ist 2.

- **`com.ibm.cognos.metadatauiservice.sap.maxInfoQueries`**

  Die maximale Anzahl an Infoabfragen, die in einem SAP BW-Paket verwendet werden können. Gültige Einstellungen sind null und größer. Der Standardwert ist 5.

Weitere Informationen zu SAP BW-Datenquellen und zum Erstellen von SAP BW-Paketen finden Sie im Artikel Kapitel 6, „Datenquellen und Verbindungen” , auf Seite 99.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Status** auf **System**.
2. Klicken Sie im Teilfenster **Scorecard** im Menü der Änderungsansicht der aktuellen Ansicht auf **Dienstleistungen** > **Metadaten**.

   Tipp: Die aktuelle Ansicht ist einer der folgenden Werte: **Alle Server**, **Alle Servergruppen**, **Alle Dispatcher**oder **Dienstleistungen**.
3. Klicken Sie im Menü **Metadatenservice Aktionen** auf **Eigenschaften festlegen**.
4. Klicken Sie auf die Registerkarte **Einstellungen** .
5. Klicken Sie neben **Erweiterte Einstellungen**auf **Bearbeiten** .
6. Wählen Sie **Über den übergeordneten Eintrag erfasste Einstellungen außer Kraft setzen**aus.
7. Geben Sie in der Spalte **Parameter** den Parameternamen ein.

   Geben Sie beispielsweise `com.ibm.cognos.metadatauiservice.sap.maxcubes`ein.
8. Geben Sie in der Spalte **Wert** den zugeordneten Wert für die Einstellung ein.
9. Setzen Sie die Eingabe von Namen und Werten nach Bedarf fort.
10. Klicken Sie auf **OK**.
11. Klicken Sie auf der **Eigenschaften festlegen** -Seite auf **OK**.

Kapitel 21. Benutzerprofile verwalten

Ein Benutzerprofil definiert die Portalregisterkarten, auf die der Benutzer zugreifen kann, und gibt Benutzervorgaben an, wie z. B. die Produktsprache, das bevorzugte Ausgabeformat der Berichte und den in der Benutzerschnittstelle verwendeten Stil.

Ein Benutzerprofil wird erstellt, wenn sich der Benutzer zum ersten Mal bei der IBM Cognos -Software anmeldet. Sie kann auch von einem Administrator erstellt werden. Zunächst basiert das Profil auf dem Standardbenutzerprofil.

Benutzer können die Benutzervorgaben, die ihrem Profil zugeordnet sind, anzeigen und ändern.

Um Benutzerprofile zu kopieren, zu bearbeiten oder zu löschen, muss ein Administrator über Schreibberechtigungen für den Namespace verfügen, der die entsprechenden Benutzer enthält. Die vordefinierte Rolle IBM Cognos , **Verzeichnisadministratoren**, verfügt nicht über Schreibberechtigungen für andere Namespaces als den **Cognos** -Namespace. **Systemadministratoren** muss den Schreibberechtigungen für **Verzeichnisadministratoren** erteilen, damit sie Benutzerprofile für den Namespace verwalten können.

Um Benutzerprofile zu verwalten, müssen Sie über die erforderlichen Zugriffsberechtigungen für **IBM Cognos Administration**verfügen.

Weitere Informationen zum Verwalten von Accounts finden Sie unter Kapitel 11, „Benutzer, Gruppen und Rollen”, auf Seite 187.

Zugehörige Konzepte

Serververwaltung

Standardbenutzerprofil bearbeiten

Das Standardbenutzerprofil ist im Namespace von **Cognos** definiert. Sie enthält Einstellungen, die für alle neuen Benutzer gelten. Sie können das Standardbenutzerprofil für Ihre Benutzer bearbeiten, um die Anzahl der Änderungen zu minimieren, die Sie an einzelnen Benutzerprofilen vornehmen müssen.

Nachdem Sie das Standardbenutzerprofil geändert haben, gilt dies nur für Benutzer, die sich zum ersten Mal bei der IBM Cognos -Software anmelden. Die vorhandenen Benutzerprofile anderer Benutzer sind nicht betroffen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Sicherheit** auf **Benutzer, Gruppen und Rollen**.
2. Klicken Sie auf den **Cognos** -Namespace.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche zum Bearbeiten des Standardbenutzerprofils  .
4. Legen Sie das Standardbenutzerprofil fest und klicken Sie auf **OK**.

Ergebnisse

Jeder Benutzer, der sich zum ersten Mal bei der IBM Cognos -Software anmeldet, übernimmt diese Einstellungen automatisch, kann aber später geändert werden.

Benutzerprofil anzeigen oder ändern

Sie können Benutzerprofile anzeigen oder ändern.

Sie können bestimmte Elemente im Profil des Benutzers löschen. Dies kann in den folgenden Situationen nützlich sein:

- Der Inhalt des Benutzers nimmt so viel Speicherplatz auf, dass die Leistung beeinträchtigt wird. Sie möchten einige oder alle Inhalte löschen.
- Sie möchten ein Benutzerprofil anzeigen, bevor Sie es löschen, um sicherzustellen, dass Sie keine wichtigen Inhalte löschen.

Wenn ein Benutzer in Ihrem Authentifizierungsprovider gelöscht wurde, wird der Benutzer nicht mehr in der IBM Cognos -Software angezeigt, und Sie können das Benutzerprofil nicht ändern.

Sie können nur die Profile von Benutzern anzeigen, die mindestens einmal angemeldet sind. Wenn sich die Benutzer anmelden, wird ein Datum in der Spalte **Geändert** angezeigt.

Zum Anzeigen eines Benutzerprofils, zum Löschen von Inhalten oder zum Ändern von Inhalt müssen Sie über Berechtigungen für das Benutzerkonto und alle Ordner verfügen, die den Inhalt des Benutzers enthalten. Sie müssen über Schreibberechtigungen für den Eintrag und über das übergeordnete Element des Eintrags verfügen, den Sie löschen möchten.

Sie können das Benutzerprofil für einzelne Benutzer ändern, jedoch nicht für Gruppen oder Rollen.

Benutzerprofil anzeigen oder ändern

Sie können ein Benutzerprofil anzeigen oder ändern.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Sicherheit** auf **Benutzer, Gruppen und Rollen**.
2. Klicken Sie auf den Namespace, der den Benutzer enthält.
3. Suchen Sie den Benutzer, dessen Vorgaben Sie anzeigen oder ändern möchten.
4. Klicken Sie in der Spalte **Aktionen** auf **Mehr**.
5. Klicken Sie auf **Benutzervorgaben festlegen**.
6. Klicken Sie auf die verschiedenen Registerkarten, um die Einstellungen anzuzeigen oder zu ändern.
7. Klicken Sie auf **Abbrechen** , um den Vorgang zu beenden, ohne Änderungen vorzunehmen, oder klicken Sie auf **OK**.

Inhalt löschen

Sie können bestimmte Elemente im Profil des Benutzers löschen, wie z. B. den Inhalt von "Meine Ordner" oder "Seiten".

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Sicherheit** auf **Benutzer, Gruppen und Rollen**.
2. Wählen Sie den Namespace aus, der den Benutzer enthält.
3. Suchen Sie den Benutzer.
4. Klicken Sie in der Spalte **Name** auf den Benutzernamen.

   Tipp: Wenn der Benutzername kein Link ist, bedeutet dies, dass das Benutzerprofil nicht erstellt wurde. Um das Profil zu erstellen, klicken Sie in der Spalte **Aktionen** auf die Profilschaltfläche dieses Benutzers,  , und fahren Sie mit den übrigen Schritten fort.

   Es wird eine Liste mit den Ordnern des Benutzers angezeigt.
5. Klicken Sie auf einen Ordner, um dessen Inhalt anzuzeigen.
6. Klicken Sie auf das Element, das aus dem Ordner gelöscht werden soll, und klicken Sie auf die Schaltfläche zum Löschen in der Symbolleiste.

   Sie können die Ordner nicht selbst löschen.

Benutzerprofil löschen

Sie können Benutzerprofile aus dem Content Store löschen.

Wenn Sie einen Benutzer in Ihrem Authentifizierungsprovider löschen, können Sie zunächst das Benutzerprofil aus dem Content-Store löschen, damit es nicht mehr Speicherplatz verwendet.

Sie sollten das Benutzerprofil aus der IBM Cognos -Software löschen, bevor Sie den Benutzer in dem zugehörigen Namespace löschen. Nachdem der Benutzer gelöscht wurde, werden die Benutzerinformationen nicht mehr in der IBM Cognos -Software angezeigt, und Sie können das Benutzerprofil in **IBM Cognos Administration**nicht verwalten.

Wenn der Benutzeraccount bereits aus dem zugeordneten Namespace gelöscht wurde, können Sie die Content-Store-Wartung verwenden, um alle zugeordneten Benutzerkontoinformationen aus IBM Cognos -Software zu suchen und optional zu entfernen.

Wenn sich ein Benutzer mit einem gelöschten Benutzerprofil anmeldet, wird ein Account unter Verwendung von Standardwerten erstellt. Wenn ein Benutzer angemeldet ist, während das zugehörige Benutzerprofil gelöscht wird, läuft der Pass des Benutzers ab, und die Anmeldeseite wird angezeigt.

Bevor Sie ein Benutzerprofil löschen, können Sie den Inhalt der Benutzerprofile anzeigen, um sicherzustellen, dass Sie nichts Wichtiges löschen.

Sie können nur mit Profilen von Benutzern arbeiten, die sich mindestens einmal angemeldet haben.

Vorbereitende Schritte

Um ein Benutzerprofil zu löschen, müssen Sie über Schreibberechtigungen für das übergeordnete Objekt verfügen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Sicherheit** auf **Benutzer, Gruppen und Rollen**.
2. Klicken Sie auf den Namespace, der den Benutzer enthält.
3. Suchen Sie den Benutzer, dessen Benutzerprofil Sie löschen möchten. Sie können die Suchfunktion verwenden, um einen Benutzer zu suchen.
4. Klicken Sie in der Spalte **Aktionen** auf **Mehr**.
5. Klicken Sie auf **Das Profil dieses Benutzers löschen**.
6. Klicken Sie auf **OK**.

Benutzerprofile kopieren

Möglicherweise möchten Sie ein Benutzerprofil kopieren.

Das Kopieren eines Benutzerprofils ist in den folgenden Situationen nützlich:

- Ein Benutzer ändert Namen, und Sie setzen ein Konto im neuen Namen ein.
- Ein Benutzer wechselt zu einem anderen Namespace, oder Ihre Organisation ändert Namensbereiche, und Sie müssen neue Konten einrichten.
- Sie erstellen viele neue ähnliche Benutzerkonten.

Wenn Sie planen, den Quellenbenutzer in Ihrem Authentifizierungsprovider zu löschen, kopieren Sie die Benutzerkontoinformationen, bevor Sie ihn löschen. Nachdem Sie den Benutzer gelöscht haben, wird der Benutzer nicht mehr in der IBM Cognos -Software angezeigt, und Sie können die Kontoinformationen des Benutzers nicht kopieren.

Sie können nur mit Profilen von Benutzern arbeiten, die sich mindestens einmal angemeldet haben. Wenn sich die Benutzer anmelden, wird in der Spalte **Geändert** ein Datum angezeigt, und der Benutzername wird in einen Link geändert.

Vorbereitende Schritte

Um Benutzerprofile zu kopieren, müssen Sie über Schreibberechtigungen für die Namespaces sowohl für die Quellen-als auch für die Zielbenutzer verfügen.

Tipp: Wenn Sie ein Benutzerprofil kopieren, werden die vertrauenswürdigen Berechtigungsnachweise nicht kopiert.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Sicherheit** auf **Benutzer, Gruppen und Rollen**.
2. Klicken Sie auf den Namespace, der den Quellenbenutzer enthält (den Benutzer, aus dem kopiert werden soll).

   Tipp: Sie können nur die Namespaces auswählen, auf die Sie Schreibzugriff haben.
3. Suchen Sie den Quellenbenutzer.
4. Klicken Sie in der Spalte **Aktionen** für den Quellenbenutzer auf **Mehr**.
5. Klicken Sie auf der Seite **Aktion ausführen** auf **Profil dieses Benutzers kopieren**.
6. Klicken Sie auf der **Benutzerprofil kopieren** -Seite auf **Zielbenutzer auswählen** und navigieren Sie zu dem Zielbenutzer.
7. Nachdem Sie den Zielbenutzer ausgewählt haben, wählen Sie auf der Seite **Benutzerprofil kopieren** eine oder mehrere der folgenden Profileinstellungen aus, die Sie kopieren möchten: **Vorgaben**, **Portalregisterkarten und Inhalt von persönlichen Ordnern**oder **Inhalt der persönlichen Ordner**.
8. Wählen Sie bei Bedarf das Kontrollkästchen **Löschen Sie das Profil des Quellenbenutzers nach Abschluss der Kopie.** aus.
9. Klicken Sie auf **Kopieren**.

Kapitel 22. Mehrmiet-Umgebungen

Multi-Tenant-Umgebungen bestehen aus mehreren Kunden oder Organisationen, die als Tenants bezeichnet werden. Multitenancy ist die Funktionalität einer Anwendung, mit der mehrere Tenants aus einer einzelnen Implementierung unterstützt werden können. Sie stellt sicher, dass innerhalb der einzelnen Tenantbenutzer nur auf die Daten zugegriffen werden kann, die sie zur Verwendung berechtigt sind. Multitenancy kann die Kosten für die Anwendungswartung reduzieren.

IBM Cognos Analytics stellt integrierte Multitenancy-Funktionen bereit. Vorhandene Implementierungen können inkrementell migriert werden, um Multimieterfunktionen zu implementieren. Die vorhandenen Implementierungen, die keine Multi-Tenant-Funktionalität verwenden, sind nicht betroffen, wenn die Multi-Tenant-Funktionalität aktiviert ist.

Alle Content Manager-Objekte können eine einzelne, optionale Tenant-ID haben. Alle Cognos-Benutzer, einschließlich Administratoren, können über eine optionale Tenant-ID verfügen. Cognos-Benutzer können unabhängig von den Cognos Analytics -Sicherheitsrichtlinien auf ein Content Manager-Objekt zugreifen, wenn sie nicht über eine Tenant-ID verfügen, die mit der Content Manager-Objekt-Tenant-ID übereinstimmt. Content Manager-Objekte, die keine Tenant-ID haben, werden als öffentlich betrachtet und können von jedem Benutzer aufgerufen werden. Benutzer, die keine Tenant-ID haben, können nur auf öffentliche Objekte zugreifen.

Tipp: Der Wert für die Tenant-ID ist eine einfache Zeichenfolge. Die Länge der Tenant-ID ist nicht beschränkt; sie darf jedoch 255 Zeichen nicht überschreiten. Der Grenzwert für die Spalte 'tenantID' im Datenbankschema ist jedoch nicht überschritten.

Das folgende Diagramm zeigt ein Beispiel, wie die Multitenancy-Funktionen von Cognos Analytics den Zugriff auf Objekte in Ihrem Content-Store isolieren. Benutzer können nur auf die Objekte zugreifen, für die sie berechtigt sind, innerhalb jeder Mietergruppierung zuzugreifen.

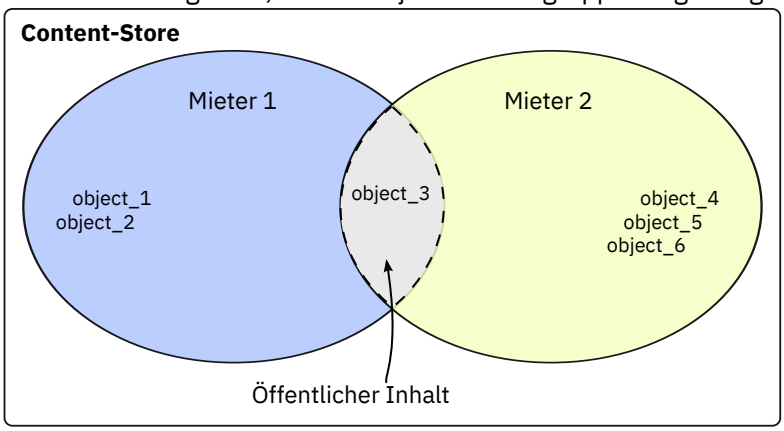


Abbildung 13. Content-Store für die Verwendung der Cognos Analytics -Multitenancy-Funktionalität

In diesem Beispiel haben die Benutzer Zugriff auf die folgenden Objekte:

- Benutzer, die zu Tenant 1 gehören, können auf 'object_1', 'object_2' und 'object_3' zugreifen.
- Benutzer, die zu Tenant 2 gehören, können auf 'object_3', 'object_4', 'object_5' und 'object_6' zugreifen.

Tipp: Der Systemadministrator kann auf alle Objekte im Content Store zugreifen.

Beim Zugriff auf Objekte wird die Objektenanzierung vor Objektzugriffsberechtigungen ausgewertet. Daher sehen Benutzer in einer Multimieteranwendung nur die Objekte, die ihrem Tenant zugeordnet sind, und Objekte, die als öffentlich kategorisiert sind.

Nachdem die Multi-Tenant-Funktionalität aktiviert ist, können Sie Tenantaktivitäten mit einer Prüfprotokolldatenbank aufzeichnen. IBM Cognos Analytics stellt Beispielprüfberichte bereit, in denen gezeigt wird, wie die Informationen zur Tenancy verwendet werden, um bestimmte Benutzeraktivitäten zu überwachen. Informationen zur Verwendung von IBM Cognos Configuration zum Einrichten einer

Protokollierungsdatenbank finden Sie im *IBM Cognos Analytics Installation und Konfiguration*. Informationen zum Einrichten der Beispielprüfberichte finden Sie im Artikel https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ig_smples.doc/c_sampleauditreports.html#SampleAuditReports.

Multitenancy konfigurieren

Um die Multi-Tenant-Funktionalität in Ihrer IBM Cognos Analytics -Installation zu konfigurieren, müssen Sie die Multitenancy-Eigenschaften in der IBM Cognos -Konfiguration angeben.

Die Werte für die Multitenancy-Eigenschaften sind für jede Umgebung unterschiedlich und hängen davon ab, wie Sie die Tenancy-Informationen einzelnen Benutzern in Ihrer Umgebung zuordnen.

Wichtig: Sie sollten in Ihrem Authentifizierungsprovider nichts ändern, um die Multi-Tenant-Funktionalität zu konfigurieren.

Bevor Sie die Multi-Tenant-Funktionalität in IBM Cognos Konfiguration konfigurieren, müssen Sie entscheiden, wie der Benutzeraccount in Ihrem Authentifizierungsprovider dem Tenant zugeordnet werden soll. Sie können zu diesem Zweck die Position eines Benutzers innerhalb der Hierarchie in Ihrem Authentifizierungsprovider oder die Benutzerkontoeigenschaften in Ihrem Authentifizierungsprovider verwenden. Sie können auch einen angepassten Tenantprovider implementieren. Für die letzte Option müssen Sie das IBM Cognos Software Development Kit verwenden. Die Auswahl der besten Implementierungsmethode für Ihre Umgebung erfordert eine sorgfältige Planung und Kenntnis Ihres Authentifizierungsproviders.

Wählen Sie eine der folgenden Methoden aus, um die Mehrantenität zu konfigurieren, je nachdem, wie Sie den Benutzer dem Tenant zuordnen möchten.

- „Multitenancy, die auf einem Hierarchieknoten basiert, konfigurieren“ auf Seite 336
- „Multitenancy konfigurieren, die auf einem Benutzerkontoattribut basiert“ auf Seite 337
- „Multitenancy konfigurieren, die auf einem angepassten Tenantprovider basiert“ auf Seite 339

Sie können die Multi-Tenant-Funktionalität global, auf der **Authentifizierung** -Ebene in IBM Cognos Konfiguration oder für bestimmte Namespaces konfigurieren. Die Multitenancy-Eigenschaften für einen bestimmten Namespace überschreiben alle Multi-Tenant-Eigenschaften, die global gesetzt werden.

Multitenancy, die auf einem Hierarchieknoten basiert, konfigurieren

Sie können die Knotenstrukturinformationen in einer Hierarchie Ihres Authentifizierungsproviders wiederverwenden, wenn Sie Ihren Tenant konfigurieren.

Sie müssen die Hierarchieinformationen der **Zuordnung von Tenant-IDs** > **Muster** -Eigenschaft in IBM Cognos Configuration zuordnen.

Vorbereitende Schritte

Sie können das `Vorfahren` -Benutzeraccountattribut zu diesem Zweck verwenden. Das Attribut `Vorfahren` stellt den hierarchischen Pfad zu einem Benutzeraccount in Form einer Feldgruppe dar. In der folgenden Tabelle wird dargestellt, wie Sie das Attribut der Vorfahren einer Hierarchie zuordnen können, um die Informationen zu den Mietverträgen zu identifizieren:

Tabelle 76. Attribut "Vorfahren", das den Hierarchieinformationen zugeordnet

Informationen zu Vorfahren	**Hierarchie**	**LDAP-Beispiel**
`Vorfahren [0]`	Verzeichnisknoten	
`Vorfahren [1]`	Namespace-ID	`basis-DN`
`Vorfahren [2]`	Mietergruppierung, wie z. B. ein Ordner	`Organisationseinheiten`

Wenn die Benutzer beispielsweise in einem LDAP-Verzeichnis gespeichert sind und die Tenants direkt unter dem Basis-DN (Distinguished Name) als Organisationseinheiten stehen, können Sie den Typ **Muster** auf den folgenden Wert setzen: `~/ancestors [ 2 ]/defaultName`.

Zusätzlich zu `defaultName`können die folgenden `Vorfahren` -Qualifikationsmerkmale Mietinformationen zurückgeben:

- `Name/Ländereinstellung`

  Der Parameter locale in diesem Beispiel basiert auf der Zuordnung in der Namespace-Konfiguration. Wenn keine Ländereinstellung angegeben ist, ist der Name der Titel des Objekts. Sie können beispielsweise Folgendes angeben: `~/ancestors [ 2 ]/name/EN-ca`

- `searchPath/objectID`

  Sie können beispielsweise Folgendes angeben: `~/ancestors [ 2 ]/searchPath/objectId`

Vorgehensweise

1. Öffnen Sie IBM Cognos Konfiguration.
2. Wählen Sie aus, ob die Multi-Tenant-Einstellungen global für alle Namespaces oder für einen bestimmten Namespace konfiguriert werden sollen.
   - Wenn Sie die Multi-Tenant-Funktionalität für alle Namespaces konfigurieren möchten, klicken Sie im Explorer-Fenster für die Kategorie **Sicherheit** auf **Authentifizierung**.
   - Wenn Sie die Multi-Tenant-Funktionalität für einen Namespace konfigurieren möchten, klicken Sie im Explorer-Fenster für die Kategorie **Sicherheit** auf **Authentifizierung**. Klicken Sie anschließend auf den Namespace, den Sie konfigurieren möchten.
3. Klicken Sie in der **Multitenancy** -Gruppe von Eigenschaften auf die Bearbeitungsschaltfläche für die Eigenschaft **Zuordnung von Tenant-IDs** .
4. Geben Sie in dem angezeigten Fenster **Zuordnung von Tenant-IDs** Ihre Zuordnung wie folgt an:
   a) Wählen Sie für **Typ**die Option **Muster**aus.
   b) Geben Sie für **Wert**die Zeichenfolge ein, die Sie auf der Basis der zuvor in diesem Abschnitt beschriebenen Anweisungen erstellt haben. Sie könnten beispielsweise den folgenden Wert angeben: `~/ancestors [ 2 ]/defaultName`.
   c) Klicken Sie auf **OK**.
5. Klicken Sie nur für einen Active Directory-Namespace in der Spalte **Wert** für **Angepasste Eigenschaften** an und klicken Sie auf die Schaltfläche zum Bearbeiten. Fügen Sie die Eigenschaft `MultiDomainTree` hinzu und legen Sie den Wert für `Wahrfest`.
6. Testen Sie Ihre Multi-Tenant-Konfiguration.
   a) Klicken Sie entweder auf **Authentifizierung** oder auf den Namespace (abhängig von Ihrer Auswahl in Schritt 2), und klicken Sie auf **Test**.
   b) Melden Sie sich mit den Berechtigungsnachweisen des Systemadministrators an, und klicken Sie auf **OK**.
   c) Klicken Sie auf die Schaltfläche **Details** und lesen Sie die Informationen, die angezeigt werden.

   Wenn die Multi-Tenant-Funktionalität ordnungsgemäß konfiguriert ist, wird Ihre Tenant-ID in den Details angezeigt. Wenn die Tenant-ID nicht angezeigt wird, aktualisieren und korrigieren Sie die Werte und testen Sie sie erneut.
7. Wenn der Test erfolgreich war, klicken Sie im Menü **Datei** auf **Speichern**.
8. Starten Sie den IBM Cognos -Service erneut, damit die Änderungen wirksam werden.

Multitenancy konfigurieren, die auf einem Benutzerkontoattribut basiert

Sie können ein bestimmtes Benutzeraccountattribut in Ihrem Authentifizierungsprovider festlegen, um dem Tenant zuzuordnen. Nachdem Sie das Benutzeraccountattribut ausgewählt haben, das dem Tenant zugeordnet werden soll, müssen Sie eine angepasste Eigenschaft erstellen und diesem Attribut zuordnen.

Sie müssen das Benutzeraccountattribut der **Zuordnung von Tenant-IDs** > **Muster** -Eigenschaft in der IBM Cognos -Konfiguration zuordnen.

Vorbereitende Schritte

Das Benutzeraccountattribut, das Sie auswählen, um den Nutzer des Benutzers zu identifizieren, sollte nur zu diesem Zweck verwendet werden.

Sie können beispielsweise entscheiden, dass das Attribut `Geschäftseinheit` eines LDAP-Benutzerkontos den Nutzer des Benutzers identifiziert. In diesem Fall legen Sie die Eigenschaft **Muster** type wie im folgenden Beispiel fest: `~/parameters/parameter_name`. Als Nächstes geben Sie eine angepasste Eigenschaft mit dem Namen `Parametername` an und ordnen diese Eigenschaft dem Benutzeraccountattribut `Geschäftseinheit` zu.

Vorgehensweise

1. Öffnen Sie IBM Cognos Konfiguration.
2. Wählen Sie aus, ob die Multi-Tenant-Einstellungen global für alle Namespaces oder für einen bestimmten Namespace konfiguriert werden sollen.
   - Wenn Sie die Multi-Tenant-Funktionalität für alle Namespaces konfigurieren möchten, klicken Sie im Explorer-Fenster für die Kategorie **Sicherheit** auf **Authentifizierung**.
   - Wenn Sie die Multi-Tenant-Funktionalität für einen Namespace konfigurieren möchten, klicken Sie im Explorer-Fenster für die Kategorie **Sicherheit** auf **Authentifizierung**. Klicken Sie anschließend auf den Namespace, den Sie konfigurieren möchten.
3. Klicken Sie in der **Multitenancy** -Gruppe von Eigenschaften auf die Bearbeitungsschaltfläche für die Eigenschaft **Zuordnung von Tenant-IDs** .
4. Geben Sie im Feld **Zuordnung von Tenant-IDs** , das angezeigt wird, Ihre Zuordnung wie folgt an:
   a) Wählen Sie für **Typ**die Option **Muster**aus.
   b) Geben Sie für **Wert**die Zeichenfolge ein, die Sie erstellt haben, die auf den früheren Anweisungen in diesem Abschnitt basiert.

      Geben Sie beispielsweise `~/parameters/`*`Parametername`*ein, wobei `~/parameters` ein konstanter Teil der Syntax ist und *Parametername* der Name der angepassten Eigenschaft ist.
   c) Klicken Sie auf **OK**.
5. Geben Sie in der Gruppe der **Kontozuordnungen (Erweitert)** -Eigenschaften die angepasste Eigenschaft an und ordnen Sie sie dem Accountattribut auf folgende Weise zu:
   a) Klicken Sie in die Spalte **Wert** für **Angepasste Eigenschaften**, und klicken Sie auf die Schaltfläche zum Bearbeiten.
   b) Klicken Sie im Fenster **Wert-Angepasste Eigenschaften** auf **Hinzufügen**.
   c) Geben Sie in der Spalte **Name** den Namen der angepassten Eigenschaft ein. Geben Sie in der Spalte **Wert** den Namen des Attributs ein. Für das Beispiel, das in Schritt 4 verwendet wird, sollte die angepasste Eigenschaft lauten: `Parametername` für **Name** und `Geschäftseinheit` für **Wert**.
   d) Klicken Sie auf **OK**.
6. Testen Sie Ihre Multi-Tenant-Konfiguration.
   a) Klicken Sie entweder mit der rechten Maustaste auf **Authentifizierung** oder auf den Namespace (abhängig von Ihrer Auswahl in Schritt 2) und klicken Sie auf **Test**.
   b) Melden Sie sich mit den Berechtigungsnachweisen des Systemadministrators an, und klicken Sie auf **OK**.
   c) Klicken Sie auf die Schaltfläche **Details** und lesen Sie die Informationen, die angezeigt werden.

   Wenn die Multi-Tenant-Funktionalität ordnungsgemäß konfiguriert ist, wird Ihre Tenant-ID in den Details angezeigt. Wenn die Tenant-ID nicht angezeigt wird, aktualisieren und korrigieren Sie die Werte und testen Sie sie erneut.

7. Wenn der Test erfolgreich war, klicken Sie im Menü **Datei** auf **Speichern**.
8. Starten Sie den IBM Cognos -Service erneut, damit die Änderungen wirksam werden.

Multitenancy konfigurieren, die auf einem angepassten Tenantprovider basiert

Sie können eine angepasste Java-Klasse erstellen und bei der Konfiguration von Multi-Tenant-Funktionalität referenzieren. Sie können diese Methode verwenden, wenn Sie Daten von mehreren Authentifizierungsprovidern oder von einem Authentifizierungsprovider und einer relationalen Datenbank verknüpfen müssen. Für diese Methode müssen Sie das IBM Cognos Software Development Kit verwenden.

Wenn Sie diese Methode verwenden, ordnen Sie die **Zuordnung von Tenant-IDs** > **Anbieterklasse** -Eigenschaft in IBM Cognos Configuration einer angepassten Java -Klasse zu.

Vorbereitende Schritte

Bevor Sie die Multi-Tenant-Funktionalität mit dieser Methode konfigurieren können, müssen Sie die folgenden Tasks ausführen:

- Kompilieren Sie alle erforderlichen angepassten Java -Klassendateien in JAR-Dateien und stellen Sie die Dateien mit allen zugeordneten Dateien in das Verzeichnis *Installationsposition*/webapps/p2pd/WEB-INF/lib , oder aktualisieren Sie die Umgebungsvariable CLASSPATH so, dass sie den Pfad zu diesen Dateien enthält.
- Implementieren Sie die ITenantProvider -Schnittstelle mithilfe des angepassten Authentifizierungsproviders von IBM Cognos und definieren Sie die angepasste Java -Klasse in dieser Schnittstelle. Der angepasste Java-Klassenname kann beispielsweise com.*Beispiel.Klasse*sein. Weitere Informationen finden Sie im *IBM Cognos Software Development Kit Custom Authentication Provider Developer Guide*.

  Tipp: IBM Cognos Der angepasste Authentifizierungsprovider enthält eine angepasste Java-Beispielklasse, die Sie verwenden können. Die Beispieldateien finden Sie im Verzeichnis *Installationsposition*\sdk\java\AuthenticationProvider\MultiTenancyTenantProviderSample .

Vorgehensweise

1. Öffnen Sie IBM Cognos Konfiguration.
2. Wählen Sie aus, ob die Multi-Tenant-Einstellungen global für alle Namespaces oder für einen bestimmten Namespace konfiguriert werden sollen.
   - Wenn Sie die Multi-Tenant-Funktionalität für alle Namespaces konfigurieren möchten, klicken Sie im Explorer-Fenster für die Kategorie **Sicherheit** auf **Authentifizierung**.
   - Wenn Sie die Multi-Tenant-Funktionalität für einen Namespace konfigurieren möchten, klicken Sie im Explorer-Fenster für die Kategorie **Sicherheit** auf **Authentifizierung**. Klicken Sie anschließend auf den Namespace, den Sie konfigurieren möchten.
3. Klicken Sie in der **Multitenancy** -Gruppe von Eigenschaften auf die Bearbeitungsschaltfläche für die Eigenschaft **Zuordnung von Tenant-IDs** .
4. Geben Sie in dem angezeigten Fenster **Zuordnung von Tenant-IDs** Ihre Zuordnung wie folgt an:
   a) Wählen Sie für **Typ**die Option **Anbieterklasse**aus.
   b) Geben Sie für **Wert**den Namen der angepassten Java -Klasse ein, die in der IBoundingSetProvider -Schnittstelle definiert ist, die mit dem angepassten Authentifizierungsprovider von IBM Cognos implementiert wurde. Geben Sie beispielsweise com.*Beispiel.class_name*ein.
   c) Klicken Sie auf **OK**.

5. Wenn Sie eine angepasste Eigenschaft angeben müssen, klicken Sie in der **Kontozuordnungen (Erweitert)** -Gruppe von Eigenschaften auf die Schaltfläche "Bearbeiten" in der Spalte **Wert** der **Angepasste Eigenschaft**und fügen Sie den Eigenschaftsnamen und den Wert nach Bedarf hinzu.
6. Testen Sie Ihre Multi-Tenant-Konfiguration.
   a) Klicken Sie entweder mit der rechten Maustaste auf **Authentifizierung** oder auf den Namespace (abhängig von Ihrer Auswahl in Schritt 2) und klicken Sie auf **Test**.
   b) Melden Sie sich mit den Berechtigungsnachweisen des Systemadministrators an, und klicken Sie auf **OK**.
   c) Klicken Sie auf die Schaltfläche **Details** und lesen Sie die Informationen, die angezeigt werden.

   Wenn die Multi-Tenant-Funktionalität ordnungsgemäß konfiguriert ist, wird Ihre Tenant-ID in den Details angezeigt. Wenn die Tenant-ID nicht angezeigt wird, aktualisieren und korrigieren Sie die Werte und testen Sie sie erneut.
7. Wenn der Test erfolgreich war, klicken Sie im Menü **Datei** auf **Speichern**.
8. Starten Sie den IBM Cognos -Service erneut, damit die Änderungen wirksam werden.

Erweiterte Funktionen für Multi-Tenant-Funktionalität

Die erweiterten Multitenancy-Funktionen können verwendet werden, um die delegierte Tenantverwaltung und die gemeinsame Nutzung von Inhalten zwischen den Mietern einzurichten.

Ein Cognos-Benutzer kann über eine einzelne Tenant-ID verfügen, die der Eigenschaft **Zuordnung von Tenant-IDs** zugeordnet ist. Wenn die Eigenschaft **Zuordnung von Tenant-IDs** definiert ist, können zusätzliche Tenant-IDs mithilfe der Eigenschaft **Zuordnung für Tenantset-Zuordnung** einem Cognos-Benutzer zugeordnet werden.

Content Manager-Objekte können über eine virtuelle Tenant-ID verfügen, die mehrere Tenant-IDs enthalten kann, die als Tenant-ID zugeordnet sind. Auf diese Weise können Benutzer von mehreren Tenants auf allgemeine Inhalte zugreifen, z. B. Ordner oder Berichte.

Virtuelle Tenant-IDs für Content Manager-Objekte und mehrere Tenant-IDs, die für Benutzer mit den Eigenschaften **Zuordnung von Tenant-IDs** und **Zuordnung für Tenantset-Zuordnung** implementiert werden, können zur gleichen Zeit verwendet werden. Diese Funktionen können verwendet werden, um Tenantadministratoren zu ermöglichen, mehrere Tenants zu verwalten, die als delegierte Tenantverwaltung bezeichnet werden, oder Cognos-Benutzer, um auf Content Manager-Objekte für mehrere Tenants zuzugreifen, die als Content-Sharing unter den Tenants bezeichnet werden.

Wenn die delegierte Tenantverwaltung implementiert wird, kann der Systemadministrator bestimmte Tasks, wie z. B. die Verwaltung von Sicherheit, Zeitpläne, Aktivitäten und Ereignisse für einige Tenants, an Mitglieder der Rolle **Mieteradministratoren** delegieren. Die Tenantadministratoren können eine Gruppe von Mietern verwalten, wie sie vom Mieterverwaltungsset des Mieteradministrators definiert werden, zusätzlich zu ihrem eigenen Mieter. Der Systemadministrator behält die volle Kontrolle über die Berechtigungen der Tenantadministratoren bei. Weitere Informationen finden Sie unter „Delegierte Tenantverwaltung“ auf Seite 347.

Wenn der Content-Sharing bei den Mietern implementiert wird, können Nutzer neben dem eigenen Tenants-Content auch auf Inhalte von verschiedenen Mietern zugreifen. Die gemeinsame Nutzung von Inhalten für Benutzer kann mithilfe der folgenden Multitenancy-Features erreicht werden:

- Die Eigenschaft **Zuordnung für Tenantset-Zuordnung** .

  Ein Benutzer kann auf ein Content Manager-Objekt zugreifen, dessen Tenant-ID in den Mieterkennsatz des Benutzers des Benutzers eingeschlossen ist.
- Virtuelle Tenant-IDs

  Ein Content Manager-Objekt, dem die virtuelle Tenant-ID zugeordnet ist, kann von Benutzern von jedem Nutzer, dessen Tenant-ID in die virtuelle Tenant-ID des Objekts eingeschlossen ist, aufgerufen werden.

Weitere Informationen finden Sie im Artikel „Virtuelle Tenants einrichten, um die gemeinsame Nutzung von Inhalten zwischen den Tenants zu ermöglichen“ auf Seite 349.

Konfigurieren der Eigenschaft 'Zuordnung von Tenant-Set' konfigurieren

Der Mieterbounding-Satz ist eine Eigenschaft mit mehreren Werten, die mehrere Tenant-IDs enthalten kann.

Sie konfigurieren diese Eigenschaft in IBM Cognos Konfiguration unter Verwendung einer der folgenden Methoden:

- „Konfigurieren des Mieterbounding-Satzes, der auf einem Benutzerkontoattribut basiert“ auf Seite 341
- „Konfigurieren des Mieterbounding-Sets, das auf einem angepassten Provider basiert“ auf Seite 342

Inaktivierte Tenants sind im Begrenzungsset vorhanden, wenn es sich bei dem Benutzer um einen Systemadministrator handelt. Gelöschte Tenants werden automatisch aus dem Begrenzungsset entfernt.

Sie können diese Einstellung global, auf alle konfigurierten Namespaces oder auf einzelne Namespaces anwenden. Die Multitenancy-Eigenschaften für einen bestimmten Namespace überschreiben alle Multi-Tenant-Eigenschaften, die global festgelegt werden, auf **Authentifizierung** -Ebene in IBM Cognos -Konfiguration.

Tipp: Die **Zuordnung von Tenant-IDs** -und **Zuordnung für Tenantset-Zuordnung** -Eigenschaften können unabhängige Implementierungen haben. Sie können beispielsweise die Position eines Benutzers innerhalb einer Hierarchie verwenden, um die **Zuordnung von Tenant-IDs** -Eigenschaft zu bestimmen und einen angepassten Provider zu verwenden, um die Eigenschaft **Zuordnung für Tenantset-Zuordnung** zu bestimmen. In den meisten Implementierungen sollten jedoch beide Eigenschaften Tenants-IDs desselben Typs enthalten, z. B. Abteilungsnummer.

Konfigurieren des Mieterbounding-Satzes, der auf einem Benutzerkontoattribut basiert

Sie können ein bestimmtes Benutzeraccountattribut in Ihrem Authentifizierungsprovider festlegen, um dem Mieterbounding-Set zuzuordnen. Die Multi-Tenant-Funktionalität muss bereits aktiviert sein.

Sie müssen das Benutzeraccountattribut der **Zuordnung für Tenantset-Zuordnung** > **Muster** -Eigenschaft in der IBM Cognos -Konfiguration zuordnen.

Vorbereitende Schritte

Nachdem Sie in Ihrem Authentifizierungsprovider ein Benutzeraccountattribut ausgewählt haben, das Sie dem Mieterbounding-Set zuordnen möchten, müssen Sie eine angepasste Eigenschaft erstellen und diese dem Benutzeraccountattribut zuordnen.

Sie können das Attribut `Abteilungsnummer` eines LDAP-Benutzerkontos verwenden, um den Manipulationssatz des Benutzers zu identifizieren. In diesem Fall können Sie die Eigenschaft **Zuordnung für Tenantset-Zuordnung**, **Muster** , wie im folgenden Beispiel gezeigt, festlegen: `~/parameters/bounding_set`. Als Nächstes geben Sie eine angepasste Eigenschaft mit dem Namen `Grenzenset` an und ordnen diese Eigenschaft dem Benutzeraccountattribut `Abteilungsnummer` zu.

Vorgehensweise

1. Öffnen Sie IBM Cognos Konfiguration.
2. Wählen Sie aus, ob diese Einstellung global für alle Namespaces oder für einen bestimmten Namespace konfiguriert werden soll.
   - Wenn Sie diese Einstellung für alle Namespaces konfigurieren möchten, klicken Sie im Explorer-Fenster für die Kategorie **Sicherheit** auf **Authentifizierung**.
   - Wenn Sie diese Einstellung für einen Namensbereich konfigurieren möchten, klicken Sie im Explorer-Fenster für die Kategorie **Sicherheit** auf **Authentifizierung**. Klicken Sie anschließend auf den Namespace, den Sie konfigurieren möchten.
3. Klicken Sie in der **Multitenancy** -Gruppe von Eigenschaften auf die Bearbeitungsschaltfläche für die Eigenschaft **Zuordnung für Tenantset-Zuordnung** .

4. Geben Sie im Feld **Zuordnungszuordnung für Mieterbounding** , das angezeigt wird, Ihre Zuordnung wie folgt an:
   a) Wählen Sie für **Typ**die Option **Muster**aus.
   b) Geben Sie für **Wert**die Zeichenfolge ein, die Sie erstellt haben, die auf den früheren Anweisungen in diesem Abschnitt basiert.

      Geben Sie beispielsweise ~/parameters/*Grenzenset*ein, wobei ~/parameters ein konstanter Teil der Syntax ist und *Grenzenset* der Name der angepassten Eigenschaft ist.
   c) Klicken Sie auf **OK**.
5. Geben Sie in der Gruppe der **Kontozuordnungen (Erweitert)** -Eigenschaften die angepasste Eigenschaft an und ordnen Sie sie dem Accountattribut auf folgende Weise zu:
   a) Klicken Sie in die Spalte **Wert** für **Angepasste Eigenschaften**, und klicken Sie auf die Schaltfläche zum Bearbeiten.
   b) Klicken Sie im Fenster **Wert-Angepasste Eigenschaften** auf **Hinzufügen**.
   c) Geben Sie in der Spalte **Name** den Namen der angepassten Eigenschaft ein. Geben Sie in der Spalte **Wert** den Namen des Attributs ein. Für das Beispiel, das in Schritt 4 verwendet wird, sollte die angepasste Eigenschaft lauten: Grenzenset für **Name** und Abteilungsnummer für **Wert**.
   d) Klicken Sie auf **OK**.
6. Testen Sie Ihre Multi-Tenant-Konfiguration.
   a) Klicken Sie entweder mit der rechten Maustaste auf **Authentifizierung** oder auf den Namespace (abhängig von Ihrer Auswahl in Schritt 2) und klicken Sie auf **Test**.
   b) Melden Sie sich mit den Berechtigungsnachweisen des Systemadministrators an, und klicken Sie auf **OK**.
   c) Klicken Sie auf die Schaltfläche **Details** und lesen Sie die Informationen, die angezeigt werden.

   Wenn diese Einstellung ordnungsgemäß konfiguriert ist, wird der Eigenschaftswert **Tenantbounding-Set** in den Details angezeigt. Wenn diese Einstellung nicht angezeigt wird, stellen Sie sicher, dass der Wert korrekt ist, und wiederholen Sie den Test.
7. Wenn der Test erfolgreich war, klicken Sie im Menü **Datei** auf **Speichern**.
8. Starten Sie den IBM Cognos -Service erneut, damit die Änderungen wirksam werden.

Konfigurieren des Mieterbounding-Sets, das auf einem angepassten Provider basiert

Sie können eine angepasste Java-Klasse erstellen, die während des Benutzerauthentifizierungsprozesses gestartet wird, um den Mieterbounding-Satz zu bestimmen. Für diese Methode müssen Sie das IBM Cognos Software Development Kit verwenden.

Wenn Sie diese Methode verwenden, müssen Sie die **Zuordnung für Tenantset-Zuordnung** > **Anbieterklasse** -Eigenschaft in IBM Cognos -Konfiguration einer angepassten Java -Klasse zuordnen.

Vorbereitende Schritte

Bevor Sie den Mieterbounding-Satz mit dieser Methode konfigurieren können, müssen Sie die folgenden Tasks ausführen:

- Kompilieren Sie alle erforderlichen angepassten Java -Klassendateien in JAR-Dateien und stellen Sie die Dateien mit allen zugeordneten Dateien in das Verzeichnis *Installationsposition*/webapps/p2pd/WEB-INF/lib , oder aktualisieren Sie die Umgebungsvariable CLASSPATH so, dass sie den Pfad zu diesen Dateien enthält.
- Implementieren Sie die IBoundingSetProvider -Schnittstelle mithilfe des angepassten Authentifizierungsproviders von IBM Cognos . Definieren Sie in dieser Schnittstelle eine angepasste Java -Klasse, die Sie später verwenden können, wenn Sie die Eigenschaft **Zuordnung für Tenantset-Zuordnung** > **Anbieterklasse** konfigurieren. Der Name kann beispielsweise

com.*Beispiel.Klasse*lauten. Weitere Informationen finden Sie im *IBM Cognos Software Development Kit Custom Authentication Provider Developer Guide*.

Vorgehensweise

1. Öffnen Sie IBM Cognos Konfiguration.
2. Wählen Sie aus, ob diese Einstellung global für alle Namespaces oder für einen bestimmten Namespace konfiguriert werden soll.
   - Wenn Sie diese Einstellung für alle Namespaces konfigurieren möchten, klicken Sie im Explorer-Fenster für die Kategorie **Sicherheit** auf **Authentifizierung**.
   - Wenn Sie diese Einstellung für einen Namensbereich konfigurieren möchten, klicken Sie im Explorer-Fenster für die Kategorie **Sicherheit** auf **Authentifizierung**. Klicken Sie anschließend auf den Namespace, den Sie konfigurieren möchten.
3. Klicken Sie in der **Multitenancy** -Gruppe von Eigenschaften auf die Bearbeitungsschaltfläche für die Eigenschaft **Zuordnung von Tenant-IDs** .
4. Geben Sie im Feld **Zuordnung für Tenantset-Zuordnung** , das angezeigt wird, Ihre Zuordnung wie folgt an:
   a) Wählen Sie für **Typ**die Option **Anbieterklasse**aus.
   b) Geben Sie für **Wert**den Java -Klassennamen ein, den Sie in der `IBoundingSetProvider` -Schnittstelle definiert haben, indem Sie den angepassten Authentifizierungsprovider von IBM Cognos verwenden.

      Geben Sie beispielsweise `~/parameters/`*`Grenzenset`*ein, wobei `~/parameters` ein konstanter Teil der Syntax ist und *Grenzenset* der Name der angepassten Eigenschaft ist.
   c) Klicken Sie auf **OK**.
5. Wenn Sie eine angepasste Eigenschaft angeben müssen, führen Sie in der Gruppe **Kontozuordnungen (Erweitert)** der Eigenschaften die folgenden Aktionen aus:
   a) Klicken Sie in die Spalte **Wert** für **Angepasste Eigenschaften**, und klicken Sie auf die Schaltfläche zum Bearbeiten.
   b) Klicken Sie im Fenster **Wert-Angepasste Eigenschaften** auf **Hinzufügen**.
   c) Geben Sie die Eigenschaft **Name** und **Wert** nach Bedarf an.
   d) Klicken Sie auf **OK**.
6. Testen Sie Ihre Multi-Tenant-Konfiguration.
   a) Klicken Sie entweder mit der rechten Maustaste auf **Authentifizierung** oder auf den Namespace (abhängig von Ihrer Auswahl in Schritt 2) und klicken Sie auf **Test**.
   b) Melden Sie sich mit den Berechtigungsnachweisen des Systemadministrators an, und klicken Sie auf **OK**.
   c) Klicken Sie auf die Schaltfläche **Details** und lesen Sie die Informationen, die angezeigt werden.

   Wenn diese Einstellung ordnungsgemäß konfiguriert ist, wird der **Tenantbounding-Set** in den Details angezeigt. Wenn diese Einstellung nicht angezeigt wird, stellen Sie sicher, dass der Wert korrekt ist, und wiederholen Sie den Test.
7. Wenn der Test erfolgreich war, klicken Sie im Menü **Datei** auf **Speichern**.
8. Starten Sie den IBM Cognos -Service erneut, damit die Änderungen wirksam werden.

Multitenancy inaktivieren

Um die Multi-Tenant-Funktionalität zu inaktivieren, müssen Sie die Authentifizierungseigenschaften für Multitenancy auf allen Content Manager-Computern entfernen, auf denen sie konfiguriert wurden.

Alle Tenant-IDs müssen aus allen Objekten im Content-Store entfernt werden. Wenn alle Tenant-IDs nach der Inaktivierung der Multi-Tenant-Funktionalität nicht entfernt werden, ist das Anwendungsverhalten möglicherweise unvorhersehbar.

Vorgehensweise

1. Öffnen Sie IBM Cognos Konfiguration.
2. Wählen Sie aus, ob die Multitenancy-Einstellungen global für alle Namespaces oder für einen bestimmten Namespace inaktiviert werden sollen.
   - Wenn Sie die Multi-Tenant-Funktionalität für alle Namespaces inaktivieren möchten, klicken Sie im Explorer-Fenster für die Kategorie **Sicherheit** auf **Authentifizierung**.
   - Wenn Sie die Multi-Tenant-Funktionalität für einen Namespace inaktivieren möchten, klicken Sie im Explorer-Fenster für die Kategorie **Sicherheit** auf **Authentifizierung**. Klicken Sie anschließend auf den Namespace, den Sie konfigurieren möchten.
3. Klicken Sie unter **Multitenancy**auf die Bearbeitungsschaltfläche für die Eigenschaft **Zuordnung von Tenant-IDs** .

   Das Feld **Zuordnung von Tenant-IDs** wird angezeigt.
4. Löschen Sie die Werte für die **Muster** oder die **Providerklasse** -Eigenschaft.

   Wenn angepasste Eigenschaften für den Namespace angegeben wurden, müssen Sie sie ebenfalls löschen.
5. Testen Sie Ihre Konfiguration, um zu prüfen, ob die Eigenschaften für die Multitenancy gelöscht werden.
   a) Klicken Sie entweder mit der rechten Maustaste auf **Authentifizierung** oder auf den Namespace (abhängig von Ihrer Auswahl in Schritt 2) und klicken Sie auf **Test**.
   b) Melden Sie sich mit den Berechtigungsnachweisen des Systemadministrators an, und klicken Sie auf **OK**.
   c) Klicken Sie auf die Schaltfläche **Details** und lesen Sie die Informationen, die angezeigt werden.

   Die Tenant-ID sollte nicht angezeigt werden.
6. Klicken Sie im Menü **Datei** auf **Speichern**.
7. Starten Sie den IBM Cognos -Service erneut.

Nächste Schritte

Nachdem die Multi-Tenant-Funktionalität inaktiviert ist, muss der Systemadministrator die Richtlinien für Objekte überprüfen und aktualisieren und anschließend die Tenancy an die Öffentlichkeit aktualisieren.

Mieterverwaltung

Die Aufgaben der Tenantverwaltung werden von Systemadministratoren und delegierten Tenantadministratoren ausgeführt.

Systemadministratoren müssen Mitglieder der **Systemadministratoren** -Rolle im **Cognos** -Namespace sein. Systemadministratoren können alle Objekte im Content-Store anzeigen und ändern. Sie können Tenantverwaltungstasks auch an andere Administratoren delegieren, die Mitglieder der Rolle **Mieteradministratoren** im Namespace von **Cognos** sind.

Mitglieder der Rolle " **Systemadministratoren** " können die folgenden Tasks in einer Umgebung mit mehreren Tenants IBM Cognos Analytics ausführen:

- Mieter-Objekte erstellen, ändern und löschen.
- Ändern Sie die Tenancy-Eigenschaften für ein beliebiges Objekt im Content-Store.
- Tenants verschieben.
- Sitzungen für Tenants beenden.

Die Registerkarte **Multitenancy** in **Verwalten** ist der zentrale Bereich für die Tenantverwaltung. Auf dieser Registerkarte kann der Administrator neue Tenants hinzufügen und alle Tenants verwalten, die in der aktuellen Cognos Analytics -Umgebung registriert sind. Nur Mitglieder der Rolle **Systemadministratoren** können auf die Registerkarte **Multitenancy** zugreifen.

Tipp: Die Registerkarte **Multitenancy** in der IBM Cognos Administration kann auch für die Tenantverwaltung verwendet werden.

Einschlussregeln für Multitenancy

Mehrere Tenants können in einem einzigen Content-Store koexistieren. Die Mieterfassungsregeln gewährleisten die Sicherheit und die Isolation zwischen den Mietern. Diese Regeln diktieren, wie der Inhalt erstellt wird und wo er sich befinden kann.

Jedes Objekt im Content-Store hat einen Tenant-ID-Wert, der angibt, zu welchem Tenant das Objekt gehört. Informationen zum Erstellen von Tenant-IDs finden Sie im Artikel „Mieter erstellen" auf Seite 345.

Die Tenant-ID eines Objekts muss mit der Tenant-ID des übergeordneten Objekts identisch sein, es sei denn, die übergeordnete Tenant-ID ist öffentlich. Wenn die übergeordnete Tenant-ID öffentlich ist, kann die Tenant-ID für das untergeordnete Element in einen beliebigen Wert geändert werden. Weitere Informationen finden Sie unter „Festlegen einer Tenant-ID für ein öffentliches Objekt" auf Seite 346.

Wenn der aktuelle angemeldete Benutzer ein Objekt erstellt, ist die Objekt-Tenant-ID mit der Tenant-ID des Benutzers identisch.

Modell-und ModelView-Objekte übernehmen ihre Tenant-ID aus dem Paket. Zum Beispiel sind Modelle, die zu einem öffentlichen Paket veröffentlicht werden, immer öffentlich.

Systemadministratoren können eine Konsistenzprüfung für den Content-Store ausführen, um Instanzen von Verstößen gegen die Tenanteinschlussregeln zu erkennen. Weitere Informationen finden Sie unter „Konsistenzprüfung für Content Store erstellen und ausführen" auf Seite 357.

Mieter erstellen

Systemadministratoren müssen das Mieterobjekt erstellen und aktivieren, bevor die Tenantbenutzer auf IBM Cognos Analyticszugreifen können.

Vorbereitende Schritte

Die Multi-Tenant-Funktionalität muss bereits in IBM Cognos Configuration aktiviert sein.

Informationen zu diesem Vorgang

Der Systemadministrator erstellt das Tenantobjekt in der Cognos Analytics **Verwalten** -Komponente auf der Registerkarte **Multitenancy** und ordnet dem Objekt eine eindeutige Tenant-ID zu.

Die Tenant-IDs sind im Authentifizierungsprovider definiert, wie z. B. LDAP, Active Directory oder ein angepasster Authentifizierungsprovider. Weitere Informationen finden Sie unter Multitenancy konfigurieren.

Vorgehensweise

1. Wählen Sie in **Verwalten**die Registerkarte **Multitenancy** aus.
2. Wählen Sie das Symbol **Mieter hinzufügen**  aus.
3. Geben Sie die Parameter **Name** und **Mieter-ID** an.

   Stellen Sie sicher, dass Sie eine gültige Tenant-ID angeben, die im Authentifizierungsprovider vorkonfiguriert wurde.

   Andere Parameter auf dieser Seite sind optional.
4. Wählen Sie **Hinzufügen**aus.

Ergebnisse

Der Tenantname wird auf der Registerkarte **Multitenancy** angezeigt. Standardmäßig ist der Tenant  inaktiviert. You can Mieter aktivieren after it is fully configured.

Zuweisen von Tenant-IDs zu vorhandenen Inhalten

Nachdem die Multi-Tenant-Funktionalität aktiviert ist, ordnet der Systemadministrator die Tenant-IDs den vorhandenen Content-Store-Objekten zu. Alle Objekte, die zu einem Tenant gehören, haben dieselbe Tenant-ID.

Wenn sich ein Benutzer aus einem bestimmten Tenant bei IBM Cognos Analyticsanmeldet, oder der Systemverwalter den Mieter verkörpert,das System die Tenant-ID ansieht und den Inhalt filtert.

Mieter können erstellt werden und Tenant-IDs können mit dem Software Development Kit (SDK) zugeordnet werden.

Informationen zu diesem Vorgang

In einer Multi-Tenant-Umgebung sind alle Objekte im Content-Store öffentlich oder gehören zu einem einzelnen Tenant. Als Systemadministrator müssen Sie sicherstellen, dass die vorhandenen Objekte über eine korrekte Tenant-ID verfügen oder öffentlich bleiben sollen. Sie können Tenant-IDs beispielsweise dem Inhalt in einem Ordner zuordnen, aber den Ordner selbst öffentlich verlassen.

Wenn der Tenantinhalt nicht in separaten Ordnern organisiert ist, können Sie für jeden Tenant einen Stammordner erstellen. Dies hilft, die Eindeutigkeit von Namen in der Cognos Analytics -Umgebung zu erhalten.

Sie können Tenant-IDs für einzelne Objekte, wie z. B. Berichte, Dashboards, Datenserververbindungen, Benutzergruppen und Rollen usw., zuordnen.

Vorgehensweise

1. Melden Sie sich bei IBM Cognos Analytics als Systemadministrator an.
2. Suchen Sie in **Teaminhalt**die Containereinträge, wie z. B. Ordner oder Pakete, deren untergeordnete Elemente dieselbe Tenant-ID zugeordnet werden sollen.

   Wenn Sie Tenant-IDs für Objekte, wie z. B. Datenserververbindungen oder Gruppen oder Rollen, zuordnen, suchen Sie die Objekte in dem entsprechenden Bereich in der Verwaltungsschnittstelle.
3. Öffnen Sie die Anzeige **Eigenschaften** für das Objekt, für das Sie die Tenant-ID zuordnen möchten.
4. Klicken Sie auf der Registerkarte **Allgemein** im Abschnitt **Erweitert** auf den Link neben **Mieter**.
5. Wählen Sie eine Tenant-ID aus der Liste der verfügbaren IDs aus, und klicken Sie auf **Anwenden**.

Ergebnisse

Die Tenant-ID wird auf den Eintrag angewendet. Wenn es sich bei dem Eintrag um einen Container handelt, z. B. einen Ordner oder ein Paket, wird die Tenant-ID auf den Eintrag und seine untergeordneten Elemente angewendet.

Der Tenantname wird auf der Registerkarte **Allgemein** , Abschnitt **Erweitert** , auf der Seite mit den Objekteigenschaften angezeigt.

Festlegen einer Tenant-ID für ein öffentliches Objekt

Sie können eine Tenant-ID für Objekte zuordnen, deren übergeordnetes Element öffentlich ist.

Vorgehensweise

1. Öffnen Sie die Anzeige **Eigenschaften** für das Objekt, wie z. B. eine Datenserververbindung, für die Sie die Tenant-ID angeben möchten.

2. Wählen Sie auf der Registerkarte **Allgemein** , Abschnitt **Erweitert** , den Link neben **Mieter**aus.
3. Wählen Sie eine Tenant-ID aus der Liste der verfügbaren IDs aus.
4. Klicken Sie **Anwenden.**

Impersonation eines Mieters

Als Systemadministrator oder Tenantadministrator können Sie einen einzelnen Nutzer impersonieren, um den Inhalt aus der Tenantperspektive anzuzeigen und mit ihm zu interagieren. Wenn Sie einen Tenant verkörpern, können Sie alle Tasks ausführen, die dieser Tenant ausführen darf, und bleiben an dem System angemeldet.

Systemadministratoren können alle Tenants, die im Content Store definiert sind, impersonieren. Tenantadministratoren können nur die Mieter verkörpern, die sie verwalten dürfen.

Vorgehensweise

1. Melden Sie sich bei IBM Cognos Analytics als Systemadministrator oder als Tenantadministrator an. Weitere Informationen finden Sie unter „Mieterverwaltung“ auf Seite 344.
2. Klicken Sie in der Hauptkopfzeile auf das Symbol **Impersonate-Tenant**  .

   Tipp: In **IBM Cognos Administration**können Systemadministratoren die Identität von Tenants auch über die Registerkarte **Multitenancy** starten. Klicken Sie im Dropdown-Menü **Aktionen** für jeden Tenant auf **Impersonate**.

   Der **Mieter-Impersonation** -Header wird angezeigt.
3. Klicken Sie im Auswahlfeld "Tenant" auf das Dropdown-Symbol, und wählen Sie den Tenant aus, den Sie verkörpern möchten.

   Der Tenantname wird in der Auswahlbox angezeigt. Wenn das Kontrollkästchen **Nur den Inhalt des Tenants anzeigen** ausgewählt ist (Standardeinstellung), können Systemadministratoren oder Tenantadministratoren nur den Inhalt anzeigen, der dem ausgewählten Tenant zugeordnet ist. Wenn das Kontrollkästchen **Nur den Inhalt des Tenants anzeigen** abgewählt ist, können Systemadministratoren den Inhalt für alle Tenants im Content-Store anzeigen, und Tenantadministratoren können Inhalte für alle Tenants anzeigen, die sie verwalten können.
4. Führen Sie die Tasks aus, die Sie für den ausgewählten Tenant ausführen möchten.

   Wenn Sie Inhalte für einen anderen Tenant ändern oder erstellen möchten, wählen Sie diesen Nutzer im Auswahlfeld aus.
5. Klicken Sie auf das Symbol **Schließen**  im Header **Mieter-Impersonation** , um die Mieterimpersonationssitzung zu beenden.

Delegierte Tenantverwaltung

Systemadministratoren können Tenantverwaltungstasks an Mitglieder der Rolle **Mieteradministratoren** delegieren.

Wenn die Eigenschaft **Zuordnung für Tenantset-Zuordnung** konfiguriert ist, kann **Mieteradministratoren** nur auf Tenants zugreifen, die in ihrer Begrenzungsgruppe definiert sind. Sie werden durch die Sicherheitsrichtlinien von Cognos Analytics , die dem Inhalt von Systemadministratoren zugeordnet sind, weiter eingeschränkt. In dieser Situation werden **Mieteradministratoren** als begrenzte Tenantadministratoren betrachtet.

Wenn die Eigenschaft **Zuordnung für Tenantset-Zuordnung** nicht konfiguriert ist, wird die Miet-Tenant-Funktionalität von **Mieteradministratoren** nur durch die Sicherheitsrichtlinien von Cognos Analytics , die dem Inhalt von Systemadministratoren zugeordnet sind, umgangen. In dieser Situation gelten **Mieteradministratoren** als ungebundene Tenantadministratoren.

Weitere Informationen zur **Zuordnung für Tenantset-Zuordnung** -Eigenschaft finden Sie in den Informationen zu erweiterten Funktionen für Multitenancy in der *IBM Cognos Analytics Administration and Security Guide*.

Mieteradministratoren kann die Tenantverwaltungstasks ausführen, die der Systemadministrator ihnen zuordnet.

Mieteradministratoren kann die folgenden Tasks nicht ausführen:

- Greifen Sie auf die Registerkarte **Multitenancy** in **Verwalten** und in IBM Cognos Administration zu.
- Sie können Tenants erstellen, löschen, implementieren und inaktivieren.
- Mandantenbenutzerprofile verwaltenBeenden Sie Benutzersitzungen und passen Sie Tenants an.
- Ändern Sie die Tenancy für Objekte im Content-Store.
- Führen Sie Serververwaltungstasks wie die Optimierung und die Ausführung von Speicherauslastungsaufgaben und Konsistenzprüfungen durch.

Tipp: Die Rolle **Mieteradministratoren** ist einer der integrierten Einträge in „Cognos -Namespace” auf Seite 183 .

Informationen zur Rolle von **Systemadministratoren** in einer Multi-Tenant-Umgebung finden Sie unter „Mieterverwaltung” auf Seite 344.

Rolle der Tenantadministratoren einrichten

Im ersten Content-Store hat die Rolle **Mieteradministratoren** keine Mitglieder und nur **Systemadministratoren** verfügen über Zugriffsberechtigungen für diese Rolle. Systemadministratoren müssen Mitglieder hinzufügen und die Anfangszugriffsberechtigungen für diese Rolle ändern, damit sie für die delegierte Tenantverwaltung verwendet werden können.

Informationen zu diesem Vorgang

Wenn Sie der Rolle " **Mieteradministratoren** " Mitglieder hinzufügen, wählen Sie die Benutzer, Gruppen oder Rollen aus den entsprechenden Tenants aus.

Vorgehensweise

Verwenden Sie die folgende Prozedur, um Mitglieder der Rolle **Mieteradministratoren** hinzuzufügen oder zu entfernen.

1. Melden Sie sich bei IBM Cognos Analytics als Systemadministrator an, der Mitglied der Rolle **Systemadministratoren** ist.
2. Wählen Sie in **Verwalten** > **Konten** > **Namensbereiche**den **Cognos** -Namespace aus.
3. Suchen Sie in der Liste der Einträge die Rolle **Mieteradministratoren** und klicken Sie in ihrem Kontextmenü auf **Mitglieder anzeigen**.
4. On the **Mitglieder** tab, select the add member icon, and browse through the hierarchy of your security namespace to select the users, groups or roles that you want to be members of this role.

Ergebnisse

Nachdem Sie die entsprechenden Benutzer, Gruppen oder Rollen zur Rolle **Mieteradministratoren** hinzugefügt haben, können Sie diese Rolle verwenden, um Sicherheitsrichtlinien und -funktionen für Objekte im Content-Store einzurichten.

Informationen zum Festlegen von Zugriffsberechtigungen finden Sie im Artikel „Zugriffsberechtigungen für einen Eintrag festlegen” auf Seite 200. Informationen zum Festlegen von Funktionen finden Sie im Artikel Kapitel 13, „Funktionen”, auf Seite 207.

Virtuelle Tenants einrichten, um die gemeinsame Nutzung von Inhalten zwischen den Tenants zu ermöglichen

Wenn Sie virtuelle Tenants einrichten, kann auf Objekte im Content-Store von Benutzern zugegriffen werden, die zu unterschiedlichen Tenants gehören.

Zu den virtuellen Tenants gehören echte Tenants, die bereits in Cognos Analyticskonfiguriert sind.

Vorbereitende Schritte

Die Multi-Tenant-Funktionalität wird für IBM Cognos Analytics aktiviert, und die Tenants werden in **Verwalten** > **Multitenancy**erstellt. Weitere Informationen finden Sie unter „Mieter erstellen" auf Seite 345.

Informationen zu diesem Vorgang

Wenn Sie auf der Registerkarte **Multitenancy** angezeigt werden, sehen die Einträge für virtuelle Tenants und reale Tenants identisch aus. Um es einfacher zu machen, virtuelle Tenants zu identifizieren, verwenden Sie aussagekräftige Namen, wenn Sie sie erstellen und Beschreibungen angeben.

Sie möchten zum Beispiel die gemeinsame Nutzung von Inhalten für Tenants mit dem Namen Nordamerika, Mittelamerika und Südamerika konfigurieren. Sie erstellen einen virtuellen Tenant mit dem Namen Americas und fügen den drei Tenants diesem Tenant hinzu. Benutzer, die zu einem der drei Mieter gehören, können auf Inhalte des eigenen Mieters, Inhalte der beiden anderen Mieter und öffentliche Inhalte zugreifen.

Wenn Sie einen virtuellen Tenant löschen, werden alle Inhalte, die diesem Tenant zugeordnet sind, ebenfalls gelöscht.

Weitere Informationen finden Sie unter Erweiterte Funktionen für Multi-Tenant-Funktionalität (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ug_cra.doc/c_config_mt_advanced.html).

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen virtuellen Tenant und einen Ordner für den Inhalt des virtuellen Tenants zu erstellen.

1. Melden Sie sich bei IBM Cognos Analytics als Mitglied der Rolle **Systemadministratoren** an.
2. Wählen Sie in **Verwalten**die Registerkarte **Multitenancy** aus.
3. Wählen Sie das Symbol **Mieter hinzufügen** aus.
4. Geben Sie die Parameter **Name** und **Mieter-ID** an.

   Die virtuelle Tenant-ID muss nicht vorkonfiguriert werden. Es kann ein beliebiger Wert sein.

   Geben Sie für eine Beschreibung eine Zeichenfolge (z. B. `Virtueller Tenant`) ein, die Ihnen bei der Identifizierung des Tenants unter anderen Tenants in Cognos Analyticshilft.
5. Wählen Sie **Hinzufügen**aus.

   Der Name des virtuellen Mieters wird in der Liste der Tenants angezeigt, und der Tenant ist standardmäßig inaktiviert. Sie können den Tenant aktivieren, nachdem Sie die Konfiguration abgeschlossen haben.
6. Wählen Sie für den von Ihnen erstellten virtuellen Tenant über das Kontextmenü die Option **Mitglieder anzeigen**aus.
7. On the **Mitglieder** tab, select the add member icon.
8. Wählen Sie die Tenants aus, die Sie dem virtuellen Tenant hinzufügen möchten, und klicken Sie auf **Hinzufügen**.

Tipp: Sie können inaktivierte Tenants hinzufügen. Benutzer können jedoch erst dann auf den Inhalt der inaktivierten Tenants zugreifen, wenn die Tenants aktiviert sind.

9. Erstellen Sie einen neuen Ordner. Der Ordnername sollte dem Namen des virtuellen Mieters für eine einfachere Identifizierung ähnlich sein.
10. Ändern Sie auf der Seite "Ordnereigenschaften" auf der Registerkarte **Allgemein Erweitert** den Wert **Mieter-ID** in die Tenant-ID des virtuellen Tenants, indem Sie die ID aus der Liste der verfügbaren IDs auswählen. Wenn Ihre virtuelle Tenant-ID beispielsweise `Americasist`, wählen Sie diese ID aus der Liste aus, und ordnen Sie sie dem Ordner zu.

Mieternamen in der Cognos Analytics -Benutzerschnittstelle anzeigen

Sie können angeben, ob Benutzer ohne Administratorberechtigungen den Tenantnamen in der Cognos Analytics -Benutzerschnittstelle anzeigen können.

Standardmäßig können nur Systemadministratoren und Tenantadministratoren den Tenantnamen anzeigen, der Objekten zugeordnet ist. Wenn Sie zulassen möchten, dass Benutzer ohne Verwaltungsaufgaben über dieselbe Berechtigung verfügen, ändern Sie die erweiterte Einstellung **portal.showTenantInfoForAllUsers** für den Präsentationsservice in 'true'.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Services konfigurieren” auf Seite 519aus.
2. Geben Sie für den Präsentationsservice die Eigenschaft **portal.showTenantInfoForAllUsers** an, und setzen Sie den Wert auf 'true'.

Mandantenbenutzerprofile verwalten

Jeder Tenant kann ein eigenes Standardbenutzerprofil haben, das von allen Tenantbenutzern gemeinsam genutzt wird.

Informationen zu diesem Vorgang

Der Systemadministrator erstellt das Tenantbenutzerprofil. Dieses Profil basiert auf dem Standardbenutzerprofil, das im Namespace von **Cognos** definiert ist. Das Standardbenutzerprofil kann geändert werden, um für den Tenant relevant zu sein. Das Profil kann z. B. die Produktsprache, die Portalregisterkarten und den Stil der IBM Cognos -Benutzerschnittstelle widerspiegeln, die dem Tenant zugeordnet ist.

Wenn sich ein Tenantbenutzer zum ersten Mal bei der IBM Cognos -Software anmeldet, wird das Benutzerprofil automatisch für den Benutzer erstellt. Das Profil basiert auf dem Tenantbenutzerprofil, sofern vorhanden. Wenn ein Tenantprofil nicht vorhanden ist, wird das Standardbenutzerprofil für den Benutzer angewendet.

Systemadministratoren können das Tenantbenutzerprofil ändern oder löschen. Das Profil kann auch mit anderen Tenantobjekten aus der Quellenumgebung in die Zielumgebung implementiert werden. Bei der Implementierung des Tenants gelten die gleichen Regeln für die Konfliktlösung für Tenantbenutzerprofile wie für andere Tenantobjekte.

Weitere Informationen zu Benutzerprofilen in IBM Cognos Analyticsfinden Sie unter Kapitel 21, „Benutzerprofile verwalten” , auf Seite 331.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf die Registerkarte **Multitenancy** .
2. Wählen Sie die zutreffende Aktion aus:
   - Wenn Sie das Benutzerprofil für einen oder mehrere Tenants erstellen möchten, wählen Sie die Kontrollkästchen für den Tenant aus und klicken Sie in der Symbolleiste auf das Symbol

Standardbenutzerprofil bearbeiten  . Nehmen Sie bei Bedarf Änderungen auf den verschiedenen Registerkarten vor.

- Wenn Sie ein vorhandenes Benutzerprofil für einen Tenant ändern möchten, klicken Sie im Dropdown-Menü des Tenants **Aktionen** auf **Nutzerprofil für Nutzer bearbeiten**, und nehmen Sie die erforderlichen Änderungen auf den verschiedenen Registerkarten vor.
- Wenn Sie das Benutzerprofil für einen oder mehrere Tenants löschen möchten, wählen Sie die Kontrollkästchen "Tenant" aus und klicken Sie in der Symbolleiste auf das Symbol **Mieterbenutzerprofil löschen** . Wenn Sie das Benutzerprofil für einen Tenant löschen möchten, klicken Sie im Dropdown-Menü des Tenants **Aktionen** auf **Mieterbenutzerprofil löschen**.

Implementierung von TenantInhalten

Sie können den Tenantinhalt exportieren und importieren.

Der Tenantinhalt kann allein oder mit dem öffentlichen Inhalt bereitgestellt werden. Öffentliche Inhalte können auch von selbst bereitgestellt werden.

Allgemeine Informationen zur Implementierung in IBM Cognos Analyticsfinden Sie unter Kapitel 19, „Implementierung”, auf Seite 299.

Tenantinhalt in ein Bereitstellungsarchiv exportieren

Sie können den Tenantinhalt aus der Quellenumgebung in ein Bereitstellungsarchiv exportieren. Später können Sie das Archiv in die Zielumgebung importieren.

Vorbereitende Schritte

Nur öffentliche Inhalte und Objekte, die zu den ausgewählten Tenants gehören, werden exportiert. Bevor Sie einen Export starten, müssen Sie die Zuordnung von Tenancy zu Objekten im Content Store abschließen.

Informationen zu diesem Vorgang

Sie können den Inhalt in der folgenden Weise exportieren:

- Inhalt, der zu den ausgewählten Tenants und öffentlichen Inhalten gehört
- Inhalt, der nur zu den ausgewählten Tenants gehört.
- Nur öffentliche Inhalte

Benutzerkontoinformationen, einschließlich öffentlicher Benutzerkonten, können von dem Export eingeschlossen oder ausgeschlossen werden. Beim Exportieren von Tenants mit öffentlichen Inhalten sind die Informationen zum öffentlichen Benutzeraccount standardmäßig ebenfalls enthalten. Wenn Sie die Informationen zum öffentlichen Konto von dieser Art des Exports ausschließen möchten, verwenden Sie die erweiterte Einstellung **`CM.TENANTS_DEPLOYMENT_EXCLUDE_PUBLIC_USER_ACCOUNTS`** . Weitere Informationen finden Sie unter „Informationen zum öffentlichen Benutzeraccount bei der Implementierung von öffentlichem Inhalt ausschließen” auf Seite 354.

Wenn öffentliche Inhalte vom Tenantexport ausgeschlossen werden und ein Mieterobjekt öffentliche Vorfahren hat, werden die öffentlichen Vorfahren in den Export eingeschlossen, sodass die Inhaltsreferenzen im Zielsystem beibehalten werden können. Beispiel: In einer Situation, in der eine Datenquellenverbindung zu einem Tenant gehört, aber die Datenquelle selbst öffentlich ist, wird die Datenquelle exportiert.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf die Registerkarte **Multitenancy** .
2. Klicken Sie in der Symbolleiste auf das Symbol **Neuer Export**  .
   Der Assistent **Neuer Export** wird geöffnet.

3. Geben Sie einen eindeutigen Namen und eine optionale Beschreibung und einen Anzeigentipp für die Implementierungsspezifikation ein. Wählen Sie den Ordner aus, in dem Sie ihn speichern möchten, und klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Implementierungsmethode auswählen** die Option **Tenants auswählen**aus. Falls zutreffend, wählen Sie das Kontrollkästchen **Benutzeraccountinformationen einschließen** ebenfalls aus und klicken Sie auf **Weiter**.
5. Führen Sie auf der **Wählen Sie die Tenants aus** -Seite die folgenden Schritte aus:
   a) Verschieben Sie mithilfe der Pfeilsymbole die entsprechenden Tenants aus dem **Verfügbar** -Feld in das Feld **Ausgewählt** . Stellen Sie sicher, dass sich die richtigen Tenantnamen im Feld **Ausgewählt** befinden.

      Wichtig: Wenn Sie öffentliche Inhalte nur exportieren, muss das Feld **Ausgewählt** leer sein.
   b) Wenn Sie den öffentlichen Inhalt in den Export aufnehmen möchten, wählen Sie das Kontrollkästchen **Öffentliche Inhalte einschließen** aus.
   c) Wählen Sie eine der **Konfliktlösung** -Optionen aus. Diese Optionen werden verwendet, wenn das Bereitstellungsarchiv in die Zielumgebung importiert wird. Mit der Option **Vorhandene Einträge ersetzen** werden Objekte in der Zielumgebung durch Objekte im Bereitstellungsarchiv ersetzt. Mit der Option **Vorhandene Einträge beibehalten** werden Objekte aus dem Bereitstellungsarchiv mit zugeordneten Objekten in der Zielumgebung verknüpft.
   d) Klicken Sie auf **Weiter**.
6. Wählen Sie auf der **Bereitstellungsarchiv angeben** -Seite unter **Bereitstellungsarchiv**ein vorhandenes Bereitstellungsarchiv aus der Liste aus, oder geben Sie einen neuen Namen ein, um einen zu erstellen.

   Wenn Sie einen neuen Namen für das Bereitstellungsarchiv eingeben, verwenden Sie keine Leerzeichen im Namen. Wenn der Name der neuen Implementierungsspezifikation mit dem Namen eines vorhandenen Implementierungsarchivs übereinstimmt, werden die Zeichen _# am Ende des Namens hinzugefügt, wobei # eine Zahl wie 1 ist.
7. Klicken Sie unter **Verschlüsselung**auf **Verschlüsselungskennwort festlegen**, geben Sie das Kennwort ein, und klicken Sie auf **OK**.
8. Überprüfen Sie die Übersichtsdaten, und klicken Sie auf **Weiter**.

   Wenn Sie die Informationen ändern möchten, klicken Sie auf **Zurück** und befolgen Sie die Anweisungen.
9. Legen Sie fest, was mit der Implementierungsspezifikation zu tun ist:
   a) Klicken Sie auf **Speichern und einmal ausführen** , und klicken Sie auf **Fertigstellen**, um es jetzt oder später auszuführen. Geben Sie die Uhrzeit und das Datum für die Ausführung an. Klicken Sie anschließend auf **Ausführen**. Überprüfen Sie die Laufzeit und klicken Sie auf **OK**.
   b) Klicken Sie auf **Speichern und planen** und klicken Sie auf **Fertigstellen**, um den Zeitplan zu einem wiederkehrenden Zeitpunkt zu terminieren. Wählen Sie dann Frequenz und Start-und Enddatum aus. Klicken Sie anschließend auf **OK**.

      Tipp: Wenn Sie den Zeitplan vorübergehend inaktivieren möchten, wählen Sie das Kontrollkästchen **Zeitplan inaktivieren** aus.
   c) Klicken Sie auf **Nur speichern**und klicken Sie dann auf **Fertigstellen**, um das Programm ohne Planung oder Ausführung zu speichern.

Ergebnisse

Die Exportimplementierungsspezifikation wird in IBM Cognos Administration auf der Registerkarte **Konfiguration** in **Inhaltsverwaltung**gespeichert. Von dieser Position aus können Sie die Implementierungsspezifikation aktualisieren und ausführen und das Bereitstellungsarchiv in einen anderen Content-Store verschieben.

Mieterinhalt in eine Zielumgebung importieren

Der Tenantinhalt kann aus dem Bereitstellungsarchiv in die Zielumgebung importiert werden.

Informationen zu diesem Vorgang

Wenn Sie aus dem Bereitstellungsarchiv importieren, wählen Sie die Einträge aus, die exportiert wurden. Wenn die Benutzerkontoinformationen in den öffentlichen Inhalt eingeschlossen wurden, können Sie diese Informationen beibehalten oder ausschließen.

Wenn Sie Inhalte importieren, können Sie den Inhalt in der Zielumgebung durch den Inhalt im Bereitstellungsarchiv ersetzen.

Der gesamte Tenantinhalt in der Zielumgebung wird nicht ersetzt, aber jeder Inhalt in der Zielumgebung, der mit dem Inhalt im Archiv in Konflikt steht, wird ersetzt.

Einige Einträge im Zielinhaltsspeicher können Verweise auf öffentliche Inhalte enthalten, die von der Tenantimplementierung ausgeschlossen wurden. Wenn sich der öffentliche Inhalt nicht bereits im Zielinhaltsspeicher befindet, führt dies zu defekten Referenzen zwischen den Einträgen. Administratoren werden über die unterbrochenen Referenzen über die Implementierungsdetails benachrichtigt. Um die defekten Referenzen zu reparieren, können Sie entweder den öffentlichen Inhalt separat bereitstellen oder den Tenantinhalt mit den im Lieferumfang enthaltenen öffentlichen Inhalten erneut exportieren.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
2. Klicken Sie in der Symbolleiste auf das neue Importsymbol  . Der **Neuer Import** -Assistent wird angezeigt.
3. Wählen Sie im Abschnitt **Bereitstellungsarchiv** das Implementierungsarchiv aus, das Sie importieren möchten.
4. Geben Sie das Kennwort ein, das zum Verschlüsseln des Archivs verwendet wurde, und klicken Sie auf **OK**.
5. Geben Sie einen eindeutigen Namen, eine optionale Beschreibung und eine Anzeigenspitze für die Implementierungsspezifikation ein, wählen Sie den Ordner aus, in dem Sie ihn speichern möchten, und klicken Sie auf **Weiter**.
6. Stellen Sie sicher, dass die Tenant-ID korrekt ist.
7. Wenn die Benutzerkontoinformationen in den öffentlichen Inhalt des Bereitstellungsarchivs eingeschlossen werden, können Sie diese Informationen jetzt einschließen oder ausschließen, indem Sie das Kontrollkästchen **Benutzeraccountinformationen einschließen**auswählen oder löschen. Diese Auswahl ist nicht verfügbar, wenn Benutzerkontoinformationen nicht in das Archiv aufgenommen werden.
8. Wählen Sie eine der **Konfliktlösung** -Optionen aus. Mit der Option **Vorhandene Einträge ersetzen** werden Objekte in der Zielumgebung durch Objekte im Bereitstellungsarchiv ersetzt. Mit der Option **Vorhandene Einträge beibehalten** werden Objekte aus dem Bereitstellungsarchiv mit zugeordneten Objekten in der Zielumgebung verknüpft.
9. Klicken Sie auf **Weiter**.
10. Überprüfen Sie die Übersichtsdaten, und klicken Sie auf **Weiter**.
11. Legen Sie fest, was mit der Importimplementierungsspezifikation ausgeführt werden soll:
    - Klicken Sie auf **Speichern und einmal ausführen**, und klicken Sie auf **Fertigstellen**, um es jetzt oder später auszuführen. Geben Sie die Uhrzeit und das Datum für die Ausführung an. Klicken Sie anschließend auf **Ausführen**. Überprüfen Sie die Laufzeit und klicken Sie auf **OK**.
    - Klicken Sie auf **Speichern und planen** und klicken Sie auf **Fertigstellen**, um den Zeitplan zu einem wiederkehrenden Zeitpunkt zu terminieren. Wählen Sie dann die Häufigkeit und das Start-und Enddatum aus, und klicken Sie auf **OK**.

Tipp: Wenn Sie den Zeitplan vorübergehend inaktivieren möchten, wählen Sie das Kontrollkästchen **Zeitplan inaktivieren** aus. Informationen zum Anzeigen des Zeitplanstatus finden Sie unter Kapitel 17, „Zeitpläne und Aktivitäten", auf Seite 247.

- Klicken Sie auf **Nur speichern**, und klicken Sie auf **Fertigstellen**, um das Programm ohne Planung oder Ausführung zu speichern.

  Wenn Sie den Import ausführen, haben Sie die Möglichkeit, das Upgrade der Berichtsspezifikation zu aktivieren. Wenn Sie die Implementierungsspezifikation zu diesem Zeitpunkt nicht aktualisieren möchten, können Sie das Upgrade später durchführen. Weitere Informationen finden Sie unter „Aktualisieren von Berichtsspezifikationen" auf Seite 321. Außerdem haben Sie die Möglichkeit, die Geschäfts-ID auszuwählen. Wählen Sie **Neue IDs beim Import zuordnen**aus.

12. Wenn Sie den Import ausführen, haben Sie die Möglichkeit, das Upgrade der Berichtsspezifikation zu aktivieren. Wenn Sie die Implementierungsspezifikation zu diesem Zeitpunkt nicht aktualisieren möchten, können Sie das Upgrade später durchführen. Weitere Informationen finden Sie unter „Aktualisieren von Berichtsspezifikationen" auf Seite 321. Sie haben auch die Option, **Geschäfts-IDs**auszuwählen. Wenn Sie einen Import ausführen, werden die Content-Store-IDs gelöscht und es werden neue IDs zugeordnet. Wenn die Content-Store-IDs beibehalten werden müssen, können Sie diese beibehalten. Weitere Informationen finden Sie unter „Inhalt-ID-Zuordnung" auf Seite 321.

Ergebnisse

Die Importimplementierungsspezifikation wird in IBM Cognos Administration auf der Registerkarte **Konfiguration** in **Inhaltsverwaltung**gespeichert. Von dieser Position aus können Sie die Implementierungsspezifikation aktualisieren und ausführen.

Informationen zum öffentlichen Benutzeraccount bei der Implementierung von öffentlichem Inhalt ausschließen

In IBM Cognos Software Version 10.2.0 gab es keine Option, um Benutzerkontoinformationen auszuschließen, wenn öffentliche Inhalte implementiert wurden. Diese Option ist im Produkt, das mit Version 10.2.1 beginnt, vorhanden.

Informationen zu diesem Vorgang

Beim Exportieren von Tenants aus Content Manager 10.2.0 können Sie vor dem Upgrade von Content Manager auf Version 10.2.1 immer noch eine große Anzahl von Benutzerkonten ohne Tenant-IDs haben. Wenn Sie diese Accounts von Ihrer Implementierung ausschließen möchten, verwenden Sie die erweiterte Einstellung **CM.TENANTS_DEPLOYMENT_EXCLUDE_PUBLIC_USER_ACCOUNTS** .

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Services konfigurieren" auf Seite 519aus.
2. Geben Sie für die **ContentManagerService**den folgenden Parameternamen ein: **CM.TENANTS_DEPLOYMENT_EXCLUDE_PUBLIC_USER_ACCOUNTS**.
3. Geben Sie **Wahr** als Wert für diesen Parameter ein und klicken Sie auf **OK**.

Aktive Benutzersitzungen für Tenants beenden

Sie müssen die aktiven Benutzersitzungen des Tenants beenden, bevor Sie einen Tenant löschen, oder bevor Sie einige Tenantwartungsoperationen ausführen.

Vorbereitende Schritte

Bevor Sie die aktiven Benutzersitzungen beenden, inaktivieren Sie den Tenant, damit neue Benutzersitzungen nicht gestartet werden können. Weitere Informationen finden Sie unter „Tenants inaktivieren und aktivieren" auf Seite 355.

Informationen zu diesem Vorgang

Verwenden Sie diese Aktion, um alle aktiven Benutzersitzungen für die angegebenen Tenants zu beenden. Der Zugang für andere Mieter ist nicht betroffen.

Vorgehensweise

1. Suchen Sie in **Verwalten** > **Multitenancy**den entsprechenden Tenant.
2. Klicken Sie im Menü des Tenantkontextmenüs auf **Sitzungen beenden**.

Ergebnisse

Eine Nachricht, die die Anzahl der beendeten Benutzersitzungen angibt, wird angezeigt.

Tenants inaktivieren und aktivieren

Sie können einen Tenant inaktivieren, wenn Sie verhindern möchten, dass die Tenantbenutzer auf IBM Cognos Analytics zugreifen und den Tenantinhalt ändern.

Informationen zu diesem Vorgang

Standardmäßig ist ein neu erstellter Tenant inaktiviert, und Sie müssen ihn aktivieren, nachdem er konfiguriert wurde.

Sie sollten einen Tenant inaktivieren, bevor Sie den Tenant und seinen Inhalt implementieren. Weitere Informationen finden Sie unter „Implementierung von TenantInhalten" auf Seite 351.

Als bewährtes Verfahren sollten Sie auch einen Tenant inaktivieren, bevor Sie seine aktiven Benutzersitzungen beenden. Weitere Informationen finden Sie unter „Aktive Benutzersitzungen für Tenants beenden" auf Seite 354.

Vorgehensweise

1. Suchen Sie in **Verwalten** > **Multitenancy**den erforderlichen Tenant.
2. Klicken Sie im Menü des Tenantkontextmenüs auf **Inaktivieren**.

   Dem Tenantsymbol wird ein Symbol hinzugefügt, das den inaktivierten Status angibt.

   Sie können den Tenant aktivieren, indem Sie **Aktivieren**auswählen.

Löschen von Tenants

Sie können einen Tenant aus IBM Cognos Analyticslöschen. Dies kann erforderlich sein, wenn der Tenant dauerhaft in eine andere Instanz von IBM Cognos Analyticsverschoben wurde.

Vorbereitende Schritte

Bevor Sie einen Tenant löschen, müssen Sie die aktiven Benutzersitzungen des Tenants beenden. Andernfalls können Sie den Tenant nicht löschen. Weitere Informationen finden Sie unter „Aktive Benutzersitzungen für Tenants beenden" auf Seite 354.

Informationen zu diesem Vorgang

Wenn Sie einen Tenant löschen, löschen Sie auch alle Inhalte, die dem Tenant zugeordnet sind, wie z. B. Berichte oder Dashboards.

Vorgehensweise

1. Suchen Sie in **Verwalten** > **Multitenancy**den Tenant, den Sie löschen möchten.

2. Klicken Sie im Menü des Tenantkontextmenüs auf **Löschen**.

Content-Store-Nutzungsaufgaben erstellen und ausführen

Die Tasks zum Speichern von Inhalten geben Einblick in die Content-Store-Nutzung.

Sie können festlegen, wie viele Instanzen jeder Objekttypbenutzer von Ihren Tenants im Content-Store und die Menge an Speicherplatz, die diese Instanzen einnehmen, haben. Sie können auch detailliertere Informationen, wie z. B. die Größe jedes Objekts, ermitteln.

Informationen zu diesem Vorgang

Diese Informationen können für Fakturierungszwecke und Bereitstellungszwecke verwendet werden. Beispielsweise können Abrechnungsentscheidungen auf der Instanzanzahl bestimmter Objekttypen, wie z. B. Berichten, basieren. Bereitstellungsentscheidungen können getroffen werden, indem bestimmt wird, welche Tenants aufgrund der Menge an Speicherplatz, die sie verwenden, in eine andere IBM Cognos -Instanz versetzt werden sollen.

Nach der Erstellung von Content-Store-Nutzungsaufgaben können Sie diese auf Anforderung, zu einem geplanten Zeitpunkt oder auf der Basis eines Triggers ausführen. Die daraus resultierenden CSV-Dateien können als Datenquellen zum Erstellen von Berichten in IBM Cognos Analyticsverwendet werden.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf die Registerkarte **Multitenancy** .
2. Klicken Sie in der Symbolleiste auf das Symbol 'Inhaltsauslastung erstellen'  .
3. Geben Sie den Tasknamen und optional eine Beschreibung und einen Anzeigentipp an.
4. Klicken Sie für die Eigenschaft **Mieter** auf **Festlegen** , um die Tenant-ID auszuwählen, die dieser Task zugeordnet werden soll.

   Wenn Sie den Tenant in diesem Punkt nicht auswählen, wird die Task mit der aktuellen Sitzungs-Tenant-ID erstellt.
5. Wählen Sie den Tenant oder Tenants aus, den Sie in diese Task für die Inhaltsauslastung einschließen möchten, indem Sie die Symbole für Pfeile verwenden, um die Tenants aus dem **Verfügbar** -Feld in das Feld **Ausgewählt** zu verschieben.
6. Geben Sie im Abschnitt **Optionen** an, wie die Informationen nach der Ausführung dieser Task in den Protokolldateien gespeichert werden sollen:
   - Wenn Sie **Eine für alle Mieter**unter **Datei**auswählen, werden die Informationen für alle Tenants in einer einzigen Datei gespeichert. Wenn Sie **Ein pro Mieter**auswählen, werden die Informationen für jeden Tenant in einer separaten Datei gespeichert.
   - Wenn Sie **Nach Objekttyp und Tenant**unter **Granularität**auswählen, wird eine allgemeine Zusammenfassung der Informationen zu jedem Tenant gespeichert. Die Zusammenfassung enthält eine Instanzanzahl und die Gesamtgröße der einzelnen Objekttypen im Content-Store, gruppiert nach Tenant. Wenn Sie **Alle Objekte**auswählen, wird eine detaillierte Zusammenfassung der Informationen zu den einzelnen Objekten im Content-Store gespeichert. Die Zusammenfassung enthält die ObjekttenantID, den Namen, die storeID, die parentStoreID und die Größe.
7. Wählen Sie aus, wie die Task ausgeführt werden soll:
   - Um die Task jetzt oder später auszuführen, klicken Sie auf **Speichern und einmal ausführen**. Geben Sie eine Uhrzeit und ein Datum für die Ausführung an, und klicken Sie auf **Ausführen**.
   - Um die Task zu einer wiederkehrenden Zeit zu planen, klicken Sie auf **Speichern und planen**. Wählen Sie anschließend die Frequenz-, Start-und Enddaten aus, und klicken Sie auf **OK**.
   - Um die Task ohne Planung oder Ausführung zu speichern, klicken Sie auf **Nur speichern**.

Ergebnisse

Die neue Aufgabe wird auf der Registerkarte **Konfiguration** in **Inhaltsverwaltung**angezeigt. Sie können die Task später ändern oder ausführen.

Die Protokolldateien, die aus der Ausführung der Content-Store-Nutzungsaufgaben resultieren, werden im `Protokolle` -Verzeichnis gespeichert, das in IBM Cognos Konfiguration mit den folgenden Namen angegeben ist:

- `cmUtilization_`*`date_stamp`*`.csv` , wenn die Option **Eine für alle Mieter** verwendet wurde.
- `cmUtilization_`*`date_stamp_Tenant_ID`*`.csv` , wenn die Option **Ein pro Mieter** verwendet wurde.

Konsistenzprüfung für Content Store erstellen und ausführen

Sie können eine Konsistenzprüfung ausführen, um Instanzen von Objekten zu erkennen, die gegen die Einschlussregeln für Multitenancy verstoßen. Inhalte, die nicht den Regeln für den Tenanteinschluss folgen, sind möglicherweise für die beabsichtigten Benutzer nicht zugänglich oder werden möglicherweise nicht gelöscht, wenn der Nutzer, zu dem er gehört, gelöscht wird.

Für die Tenant-Einschlussregeln ist es erforderlich, dass die Tenant-ID eines Objekts mit der Tenant-ID des übergeordneten Objekts identisch sein muss, es sei denn, die übergeordnete Tenant-ID ist öffentlich. Weitere Informationen finden Sie unter „Einschlussregeln für Multitenancy“ auf Seite 345.

Vorbereitende Schritte

Sichern Sie den Content Store, bevor Sie eine Konsistenzprüfung für den Content Store ausführen.

Informationen zu diesem Vorgang

Instanzen, bei denen ein Objekt gegen die Tenanteinschlussregeln verstößt, werden automatisch aufgelöst, wenn Sie die Option **Suchen und beheben** verwenden, wenn die Konsistenzprüfungsaufgabe für den Content Store ausgeführt wird. Die inkonsistenten Mieterinkonsistenzen werden durch Zuordnung der übergeordneten Tenant-ID zu dem untergeordneten Objekt, das den Fehler verursacht, behoben. Sie müssen den IBM Cognos -Service nicht für diese Typen von Fehlern starten, die behoben werden sollen. Andere Arten von Inkonsistenzen im Content-Store werden jedoch erst dann behoben, wenn der IBM Cognos -Service gestartet wird. Eine Zusammenfassung jeder Reparatur wird unter der Taskausführungshistorie erstellt.

Wenn Sie die Fälle von Verstößen gegen das Tenanteinschlussregeln überprüfen und manuell beheben möchten, können Sie die Option **Nur suchen** verwenden, wenn Sie die Konsistenzprüfung für den Content Store ausführen. Unter der Annahme, dass der Benutzer, der die Task ausführt, ein Systemadministrator ist, wird unter dem Taskausführungsverlauf eine Zusammenfassung eines jeden Fehlers erstellt. Diese Option ist möglicherweise sicherer, weil sie Ihnen die Zeit gibt, jedes Objekt einzeln zu untersuchen und dem Objekt die richtige Tenant-ID zuzuordnen.

Vorgehensweise

1. Klicken Sie in der IBM Cognos Administration auf der Registerkarte **Konfiguration** auf **Inhaltsverwaltung**.
2. Klicken Sie in der Symbolleiste auf das Symbol für die neue Inhaltsverwaltung  und klicken Sie dann auf **Konsistenzprüfung**.
3. Geben Sie den Tasknamen und optional eine Beschreibung und einen Anzeigentipp ein.
4. Klicken Sie auf **Interne Referenzen** , um den Content-Store auf Inkonsistenzen zu überprüfen.
5. Wählen Sie aus, wie die Task ausgeführt werden soll:
   - Um die Task jetzt oder später auszuführen, klicken Sie auf **Speichern und einmal ausführen**. Geben Sie eine Uhrzeit und ein Datum für die Ausführung an. Klicken Sie auf **Nur suchen** oder **Suchen und beheben**, und klicken Sie dann auf **Ausführen**. Überprüfen Sie die Laufzeit und klicken Sie auf **OK**.

- Um die Task zu einer wiederkehrenden Zeit zu planen, klicken Sie auf **Speichern und planen**. Wählen Sie Frequenz und Start-und Enddatum aus. Klicken Sie auf **Nur suchen** oder **Suchen und beheben** und anschließend auf **OK**.
- Um die Task ohne Planung oder Ausführung zu speichern, klicken Sie auf **Nur speichern**.

Ergebnisse

Die neue Aufgabe wird auf der Registerkarte **Konfiguration** unter **Inhaltsverwaltung**angezeigt. Sie können die Task später ändern oder ausführen. Weitere Informationen zur Verwendung dieser Typen von Tasks in einer IBM Cognos -Umgebung finden Sie unter „Wartungstasks für Content-Store" auf Seite 60.

Zugriff auf interaktive Aktivitäten in einer Multi-Tenant-Umgebung

Der Inhalt der interaktiven Aktivitäten in IBM Cognos Analytics wird nicht von der Tenant-ID gefiltert. Daher sind zusätzliche Maßnahmen erforderlich, um den Zugriff auf interaktive Aktivitäten für Benutzer zu beschränken.

Der Inhalt der Hintergrundaktivitäten wird von der Tenant-ID gefiltert, sodass alle Benutzer diese Aktivitäten anzeigen können.

Hintergrundaktivitäten und interaktive Aktivitäten können in **Eigene Aktivitäten und Zeitpläne**abgerufen werden. Administratoren können die Aktivitäten auf der Registerkarte **Status** in der IBM Cognos Administration anzeigen. Weitere Informationen finden Sie unter Kapitel 17, „Zeitpläne und Aktivitäten", auf Seite 247.

Beschränkung des Zugriffs auf interaktive Aktivitäten für Benutzer

Um das Risiko zu vermeiden, dass der Tenantinhalt unbeabsichtigten Benutzern zugänglich gemacht wird, können Systemadministratoren den Zugriff auf interaktive Aktivitäten einschränken.

Informationen zu diesem Vorgang

Verwenden Sie die erweiterte Einstellung **COGADMIN.restrictInteractiveActivitiesToSystemAdministrators** , um den Zugriff auf interaktive Aktivitäten für Benutzer zu beschränken, so dass nur Systemadministratoren diese Art von Aktivitäten anzeigen können.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Dispatcher konfigurieren" auf Seite 518aus.
2. Geben Sie für den angegebenen Dispatcher in der Spalte **Parameter** den folgenden Namen ein:**COGADMIN.restrictInteractiveActivitiesToSystemAdministrators**
3. Geben Sie einen Wert von `Wahr` für diesen Parameter an und klicken Sie auf **OK**.
4. Starten Sie den IBM Cognos -Service erneut.

Ergebnisse

Nur Systemadministratoren können jetzt interaktive Aktivitäten in der IBM Cognos -Umgebung anzeigen.

Interaktive Aktivitäten unbekannter Benutzer ausblenden

Tenantadministratoren verfügen möglicherweise nicht über die Berechtigungen zum Anzeigen aller Benutzer in der IBM Cognos -Umgebung. Die Administratoren können jedoch immer noch interaktive Aktivitäten aller Benutzer anzeigen, da diese Typen von Aktivitäten nicht von der Tenant-ID gefiltert werden.

Informationen zu diesem Vorgang

Der Systemadministrator kann interaktive Aktivitäten von Benutzern ausblenden, die der Tenantadministrator nicht von seiner Ansicht aus sehen kann.

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Dispatcher konfigurieren" auf Seite 518aus.
2. Geben Sie als **Parameter** name den folgenden Namen ein:**COGADMIN.filterInteractiveActivitiesOfUnknownUsers**
3. Geben Sie einen Wert von `Wahr` für diesen Parameter an und klicken Sie auf **OK**.
4. Starten Sie den IBM Cognos -Service erneut.

Ergebnisse

Tenantadministratoren können jetzt nur die interaktiven Aktivitäten der spezifischen Tenantbenutzer anzeigen.

Kapitel 23. Ressourcenbibliothek

Administratoren importieren, speichern und verwalten wiederverwendbare Ressourcen, wie z. B. Visualisierungen und Benutzerschnittstellenprofile, auf der Registerkarte **Bibliothek** in der IBM Cognos Administration.

Die Registerkarte **Bibliothek** stellt eine zentrale Position für die Verwaltung der Ressourcen bereit.

Um Inhalte auf der Registerkarte **Bibliothek** zu öffnen und zu verwalten, müssen Sie Mitglied der Rolle **Bibliotheksadministratoren** sein. Weitere Informationen finden Sie unter „Vordefinierte Rollen" auf Seite 224.

Administratoren müssen Ressourcen importieren und Zugriffsberechtigungen für die Ressourcen in der Bibliothek festlegen. Benutzer mit den entsprechenden Berechtigungen können dann Ressourcen in Berichten von IBM Cognos verwenden.

Administratoren können auch Ressourcen aus der Bibliothek löschen.

Visualisierungen

Visualisierungen helfen den Verbrauchern, Muster und Ausreißer zu erkennen und Daten zu verstehen. Verwenden Sie die IBM Cognos Analytics -Visualisierungstools, um verschiedene Typen von Visualisierungen und eine größere Interaktivität in die IBM Cognos -Berichte zu integrieren.

Administratoren müssen Visualisierungen aus lokalen Systemen und Dateifreigaben in IBM Cognos Analyticsimportieren.

Eine Vielzahl von sofort einsatzfähigen, anpassbaren Visualisierungen sind in Benutzerdefinierte Visualisierungen, die in den Beispielen verwendet werden verfügbar (https: //community.ibm.com/community/user/businessanalytics/blogs/steven-macko/2016/10/06/ibm-cognos-analytics-custom-visualizations-used-in-the-samples). Sie können die Visualisierungen auswählen, die Ihren Daten entsprechen, und Ihre Geschäftsfrage beantworten, und sie in Ihr Dateisystem oder in die Netzfreigaben herunterladen. Verwenden Sie anschließend die Registerkarte **Bibliothek** , um die Visualisierungen in die Bibliothek zu importieren und sie für die Berichtsersteller verfügbar zu machen.

Visualisierungen sind in einer vollständigen Content-Store-Implementierung enthalten. Bei der Implementierung einer partiellen Content-Store-Implementierung haben Administratoren die Möglichkeit, Visualisierungen zu umfassen. Weitere Informationen finden Sie unter *Implementierung* in der *Verwaltung und Sicherheit*.

Visualisierungen in die Bibliothek importieren

Administratoren importieren Visualisierungen aus lokalen Systemen und Dateifreigaben in die IBM Cognos Analytics -Umgebung. Die importierten Visualisierungen werden dann auf der Registerkarte **Bibliothek** aufgelistet und sind für die Verwendung in Berichten von IBM Cognos verfügbar.

Informationen zu diesem Vorgang

Vorhandene Visualisierungen können erneut importiert werden, wenn sie geändert wurden. Da Änderungen an Visualisierungen nicht rückgängig gemacht werden können, müssen Sie deren Auswirkung auf die zugehörigen Berichte verstehen, bevor Sie die Visualisierungen ersetzen. Andernfalls kann diese Aktion unbeabsichtigte Änderungen an den Berichten zur Folge haben oder verhindern, dass die Berichte ausgeführt werden.

Wenn Sie Visualisierungen erneut importieren, müssen Berichtsersteller die Berichte aktualisieren, die die Visualisierungen in IBM Cognos Analytics - Reporting enthalten, damit die Änderungen wirksam werden. Für die meisten Änderungen reicht es aus, die Berichte in einem neuen Fenster in Reportingerneut zu öffnen. In einigen Fällen sind jedoch Änderungen im Bericht erforderlich. Wenn die

neue Visualisierung beispielsweise Elemente in der Datensatzstruktur des Berichts geändert oder umbenannt hat, muss der Bericht in Reportinggeändert werden.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Bibliothek** auf **Visualisierungen**.
2. Klicken Sie in der Symbolleiste auf das Symbol **Importieren**  .
   Das **Visualisierungen auswählen-Seite 'Neue Darstellung importieren'** wird geöffnet.
3. Klicken Sie auf **Durchsuchen** , um zu der Visualisierungsdatei zu navigieren, die Sie auswählen möchten. Suchen Sie erneut, wenn Sie zusätzliche Visualisierungsdateien auswählen möchten.

   Tipp: Wenn Sie eine Visualisierungsdatei aus der Liste der ausgewählten Visualisierungen entfernen möchten, klicken Sie auf das Symbol **Auswahl entfernen**  .
4. Um eine vorhandene Visualisierung zu ersetzen, wählen Sie das Markierungsfeld **Vorhandene Einträge ersetzen** aus.

   Wenn Sie dieses Kontrollkästchen inaktivieren, während Sie versuchen, eine vorhandene Visualisierung zu importieren, schlägt der Import fehl. Damit soll sichergestellt werden, dass eine vorhandene Visualisierung nicht versehentlich überschrieben wird, was dazu führen könnte, dass die Berichte, die diese Visualisierung verwenden, gebrochen werden. Wenn Sie sich entschließen, eine bestimmte Visualisierung zu ersetzen, importieren Sie die Visualisierung, indem Sie das Markierungsfeld **Vorhandene Einträge ersetzen** auswählen. Aktualisieren Sie anschließend in Reportingdie Berichte, die diese Visualisierung enthalten.
5. Klicken Sie zum Importieren ausgewählter Visualisierungen auf **Importieren**.

Ergebnisse

Die importierten Visualisierungen werden jetzt auf der **Visualisierungen** -Seite aufgelistet. Die Visualisierungen haben Standardzugriffsberechtigungen, die Administratoren ändern können.

Visualisierungen verwalten

Nachdem Sie Visualisierungen in IBM Cognos Administration importiert haben, können Sie diese auf der Registerkarte **Bibliothek** verwalten.

Informationen zu diesem Vorgang

Sie können die folgenden Aktionen ausführen, um die Visualisierungsressourcen zu verwalten:

· **Eigenschaften festlegen**

  Visualisierungen werden, wenn sie importiert werden, Standardeigenschaften, einschließlich Zugriffsberechtigungen, zugeordnet. Bibliotheksadministratoren können die Standardeinstellungen, einschließlich der Zugriffsberechtigungen, für eine Visualisierungsressource ändern.

  Weitere Informationen finden Sie in den Abschnitten Kapitel 16, „Eingabeeigenschaften”, auf Seite 241 und „Zugriffsberechtigungen für einen Eintrag festlegen” auf Seite 200.

  Wichtig: Das Symbol "Eigenschaften festlegen"  in der Symbolleiste wird verwendet, um Eigenschaften, einschließlich Zugriffsberechtigungen, für die Seite **Visualisierungen** in der **Bibliothek**festzulegen.

· **Meine Berechtigungen anzeigen**

  Administratoren können ihre eigenen Berechtigungen für jede Visualisierung anzeigen.

· **Löschen**

  Sie können einzelne oder mehrere Visualisierungen aus der Content Store-Datenbank löschen.

- **Herunterladen**

  Sie können eine vorhandene Visualisierung auf Ihre Festplatte oder Ihren Netzwerkanteil herunterladen, um die Visualisierung zu ändern.

Vorgehensweise

1. Klicken Sie in IBM Cognos Administration auf der Registerkarte **Bibliothek** auf die Seite **Visualisierungen** .
2. In der Visualisierungs-Liste können Sie die folgenden Tasks ausführen:
   - Um eine Visualisierung zu verwalten, klicken Sie auf das entsprechende Dropdown-Aktionsmenü, und klicken Sie auf die ausgewählte Aktion.
   - Wenn Sie mehrere Visualisierungen löschen möchten, wählen Sie die Kontrollkästchen aus, die den ausgewählten Visualisierungen zugeordnet sind, und klicken Sie in der Symbolleiste auf das Symbol **Löschen**  .

Kapitel 24. Berichte und Cubes

Sie können Berichte, Cubes und Dokumente verwenden, um Daten zu analysieren und Ihnen dabei zu helfen, fundierte und rechtzeitige Entscheidungen zu treffen.

In IBM Cognos Analyticskönnen Berichte und Cubes an das Portal veröffentlicht werden, um sicherzustellen, dass jeder in Ihrem Unternehmen genaue und relevante Informationen hat, wenn er dies benötigt.

Arbeiten mit Berichten und Cubes

Ein Bericht kann sich auf die Spezifikation beziehen, die die Informationen definiert, die in einen Bericht aufgenommen werden sollen, oder die Ergebnisse selbst. Berichtsspezifikationen können gespeicherte Ergebnisse haben, oder Sie können einen Bericht ausführen, um neue Ergebnisse zu generieren.

Nachdem ein Bericht für das Portal veröffentlicht wurde, können Sie ihn anzeigen, ausführen oder öffnen oder Berichtsausgabeversionen anzeigen. Sie können den Bericht auch in verschiedenen Formaten anzeigen.

Sie können Berichte verteilen, indem Sie sie speichern, indem Sie sie per E-Mail senden, an IBM Cognos Analytics Mobile Reportssenden, drucken oder platzen lassen. Sie können auch Ausführungsoptionen für die aktuelle Ausführung festlegen und erweiterte Ausführungsoptionen für den aktuellen Testlauf festlegen.

Sie können einen Bericht so terminieren, dass er zu einem späteren Zeitpunkt oder auf einer wiederkehrenden Basis ausgeführt wird. Sie können einen Bericht als Teil eines Jobs oder basierend auf einem Auslöser planen. Sie können den Ausführungsprotokoll für einen Bericht anzeigen. Sie können auch einen Bericht in einen Agenten einschließen.

Sie können sich der Alertliste für einen Bericht hinzufügen, so dass Sie benachrichtigt werden, wenn neue Versionen des Berichts erstellt werden. Sie können auch Überwachungsregeln in gespeicherten HTML-Berichtsausgaben angeben, so dass Sie benachrichtigt werden, wenn die durch die Überwachungsregeln angegebenen Ereignisse erfüllt sind.

Sie können die Auswahl-basierte Features wie Bohren auf und Ab und Drillthrough inaktivieren.

Gemischte Währungen

Gemischte Währungswerte treten auf, wenn Sie Werte mit verschiedenen Währungen berechnen. Wenn Sie eine OLAP-Datenquelle verwenden, verwenden gemischte Währungswerte den Stern (*) als Maßeinheit.

IBM Cognos Aktive Berichte

Sie können IBM Cognos Analytics - Reporting verwenden, um aktive Berichte zu erstellen. IBM Cognos Active Report ist ein Berichtsausgabetyp, der einen hoch interaktiven und easy-to-use verwalteten Bericht bereitstellt. Für Geschäftsbenutzer werden aktive Berichte erstellt, die es ihnen ermöglichen, ihre Daten zu untersuchen und zusätzliche Einblicke abzuleiten.

Berichtsautoren erstellen Berichte, die auf die Bedürfnisse ihrer Benutzer zugeschnitten sind, wobei die Benutzerfreundlichkeit einfach und eingreifend bleibt. Aktive Berichte können von Benutzern, die offline sind, konsumiert werden, wodurch sie zu einer idealen Lösung für ferne Benutzer, wie zum Beispiel die Verkaufskraft, werden.

Aktive Berichte sind eine Erweiterung des traditionellen Berichts von IBM Cognos . Sie können vorhandene Berichte nutzen und sie in aktive Berichte konvertieren, indem Sie ein interaktives Verhalten hinzufügen, indem Sie Endbenutzer über eine benutzerfreundliche Schnittstelle bereitstellen.

Berichtsansichten

Eine Berichtsansicht verwendet dieselbe Berichtsspezifikation wie der Quellenbericht, weist jedoch unterschiedliche Eigenschaften auf, z. B. Eingabeaufforderungswerte, Zeitpläne, Bereitstellungsmethoden, Ausführungsoptionen, Sprachen und Ausgabeformate.

Informationen zu diesem Vorgang

Beim Erstellen einer Berichtsansicht wird der ursprüngliche Bericht nicht geändert. Sie können den Quellenbericht für eine Berichtsansicht ermitteln, indem Sie die zugehörigen Eigenschaften anzeigen. Die Eigenschaften der Berichtsansicht geben auch einen Link zu den Eigenschaften des Quellenberichts an.

Wenn der Quellenbericht an eine andere Position verschoben wird, wird der Link für die Berichtsansicht nicht unterbrochen. Wenn der Quellenbericht gelöscht wird, wird der Link für die Berichtsansicht unterbrochen, und der Eigenschaftslink zum Quellenbericht wird entfernt.

Wenn Sie einen generischen Bericht als zugrunde liegende Struktur für zusätzliche Berichte verwenden möchten, erstellen Sie eine Kopie des Berichts.

Die Berichtsansicht verfügt über dieselben Ausführungsoptionen und Eigenschaften wie der ursprüngliche Eintrag.

Lineage-Informationen für ein Datenelement anzeigen

Abstammungsinformationen werden den Metadaten eines Datenelements in einem HTML-Bericht oder einer Berichtsansicht durch das Paket und die Datenquellen, die von dem Paket verwendet werden, nachverfolgt.

In der Abstammungslinie werden auch alle Datenelementfilter angezeigt, die vom Berichtsersteller hinzugefügt wurden oder die im Datenmodell definiert wurden. Sie können zum Beispiel in einer Kreuztabelle auf eine Zelle klicken, um zu sehen, wie der Zellenwert berechnet wurde.

Sie können keine Abstammungsinformationen anzeigen, wenn Sie einen Bericht von einem mobilen Gerät aus ausführen.

IBM Cognos Analytics kann so konfiguriert werden, dass die Standardlinienlösung verwendet wird, die mit dem Produkt geliefert wird, oder eine angepasste Abstammungslösung. IBM InfoSphere Information Governance Catalog wird ebenfalls unterstützt.

Um in einem Bericht auf Abstammungsinformationen zugreifen zu können, muss ein Administrator die Abstammungslösung konfigurieren, die **Abstammung** -Funktionalität aktivieren und für Sie Leseberechtigungen für den Bericht erteilen.

Weitere Informationen finden Sie unter „Lineage-Lösung konfigurieren” auf Seite 91, Kapitel 13, „Funktionen”, auf Seite 207und Kapitel 14, „Objektfunktionalität”, auf Seite 219.

Die Abstammungslösung von IBM Cognos zeigt die Abstammungslinie für Berichte auf ihrem höchsten Stand an. Die Abstammungslinie ändert sich nach dem Drilldown in einem Bericht nicht. Da der Auswahlkontext, der zum Starten der Abstammung verwendet wird, durch Drilldown-Aktionen beeinflusst werden kann, empfehlen wir, dass Sie die Abstammungslinie immer auf der höchsten Berichtsebene starten, bevor Sie den Bericht in den Bericht einbohren. Andernfalls kann die Abstammungslinie nicht ordnungsgemäß gestartet werden.

Vorgehensweise

1. Öffnen Sie einen HTML-Bericht oder eine Berichtsansicht.
2. Klicken Sie mit der rechten Maustaste auf das gewünschte Datenelement, und klicken Sie auf **Abstammung**.

   Die Lineage-Ansichten werden angezeigt.

Zugriff auf das InfoSphere Business Glossary

Wenn Ihre Organisation IBM InfoSphere Business Glossary verwendet, können Sie auch auf das Glossar in der Cognos-Software, über die IBM Cognos Analytics-Anzeigefunktion und über die Metadatenbaumstruktur in Reporting, Query Studio und Analysis Studio zugreifen.

Vorbereitende Schritte

Bevor Sie auf das Business-Glossar von InfoSphere zugreifen können, müssen Sie über die Berechtigungen für die Funktionalität von **Glossar** verfügen, und der Glossar-URI muss vom Administrator konfiguriert werden.

Weitere Informationen finden Sie unter Kapitel 13, „Funktionen”, auf Seite 207, Kapitel 14, „Objektfunktionalität”, auf Seite 219und „InfoSphere Business Glossary-URI konfigurieren” auf Seite 92.

Vorgehensweise

1. Öffnen Sie eine HTML-Berichts-oder Berichtsansicht in der Cognos Analytics-Anzeigefunktion.
2. Klicken Sie mit der rechten Maustaste auf das gewünschte Datenelement, und klicken Sie auf **Glossar**.

Ergebnisse

Standardmäßig geben die GlossarSuchergebnisse in der Cognos -Software nur Begriffe zurück, die das in der Suche angegebene Schlüsselwort enthalten. Andere Arten von Assets werden nicht zurückgegeben.

Berichtsformate

In IBM Cognos Analyticskönnen Sie Berichte in einem Browser anzeigen, oder Sie können abhängig von Ihren Berechtigungen Berichte in Formaten generieren, die in andere Anwendungen importiert werden können. Administratoren können den Zugriff auf die Funktionen einschränken, die für die Ausführung von Berichten in CSV-, PDF-, Microsoft -oder XML-Formaten (XLS) erforderlich sind.

Standardmäßig verfügen alle Benutzer über Berechtigungen für die folgenden Funktionen:

- CSV-Ausgabe generieren
- PDF-Ausgabe generieren
- XLS-Ausgabe generieren
- XML-Ausgabe generieren

Diese separat gesicherten Funktionen unterstützen die Verwaltung von Systemressourcen. Um die Formate zu steuern, die Benutzer in der Benutzerschnittstelle anzeigen und ausführen können, müssen Sie Zugriffsberechtigungen für diese Funktionen festlegen.

Wenn Ihr Zugriff auf ein Format eingeschränkt ist, können Sie den Inhalt im eingeschränkten Format anzeigen und das eingeschränkte Format in den Eigenschaften eines Berichts angeben.

Um die folgenden Aktionen ausführen zu können, müssen Sie über die Berechtigung "Ausführen" und "traverse" für die entsprechende Funktion verfügen:

- Führen Sie Berichte in einem eingeschränkten Format aus.
- Legen Sie Zeitpläne oder Jobs für Berichte fest, die in einem eingeschränkten Format ausgeführt werden.
- Führen Sie einen Drilldown für Ziele aus, die in einem eingeschränkten Format ausgeführt werden
- Drucken Sie einen PDF-Bericht in einem Cognos Workspace-Widget.

Wenn Sie einen Bericht ausführen, werden nur die Formatoptionen angezeigt, für die Sie die Funktion zum Generieren der Ausgabe haben. Das HTML-Format ist keine gesicherte Funktion.

Die generierten Ausgabefunktionen gelten nicht für PowerPlay-oder aktive Berichte.

Um das Berichtsformat anzugeben, müssen Sie auch Lese-und Schreibberechtigungen für den Bericht haben und Berechtigungen für den Ordner, der den Bericht enthält, traversieren.

Sie können das Standardformat angeben, das verwendet werden soll, wenn ein Bericht ausgeführt wird.

Sie können das Berichtsformat auf der Seite mit den Ausführungsoptionen, in den Berichtseigenschaften oder in Ihren Vorgaben angeben.

HTML-Formate

In IBM Cognos Analyticskönnen Sie das HTML-Ausgabeformat für einen Bericht auswählen.

PDF-Format

Verwenden Sie das PDF-Format, um Berichte in einem Online-Buchformat anzuzeigen und zu verteilen. Um in IBM Cognos AnalyticsBerichtsausgaben im PDF-Format zu generieren, müssen Sie über die Ausführungsberechtigung und die Berechtigung für die **PDF-Ausgabe generieren** -Funktionalität verfügen.

Sie müssen über Administratorrechte verfügen, um die erweiterten PDF-Optionen anzugeben.

Microsoft Excel-Formate

Sie können Ihre Berichtsausgabe in mehrere unterschiedliche Microsoft Excel-Tabellenkalkulationssoftwareformate exportieren.

In IBM Cognos Analyticsmüssen Sie zum Generieren von Berichtsausgaben in Microsoft -Excel-Formaten über die Ausführungsberechtigung und die Berechtigung für die **XLS-Ausgabe generieren** -Funktionalität verfügen.

Die Excel-Formate übergeben die Berichtsausgabe im nativen Excel-XML-Format, auch bekannt als XLSX.

Das **Excel** -Format stellt vollständig formatierte Berichte bereit. Die Ausgabe ist ähnlich wie andere Excel-Formate, mit folgenden Ausnahmen:

- Diagramme werden als statische Bilder wiedergegeben.
- Die Zeilenhöhe kann sich in dem wiedergegebenen Bericht ändern, um eine größere Treue zu erreichen.
- Spaltenbreiten, die explizit in Berichten angegeben werden, werden in Microsoft Excel 2007 ignoriert.
- Zusammengeführte Zellen werden verwendet, um die Darstellung von Berichten zu verbessern.
- Die Standardgröße der Arbeitsblätter beträgt 65 536 Zeilen mit 256 Spalten.

  Ihr IBM Cognos -Administrator kann größere Arbeitsblätter aktivieren und die maximale Anzahl von Zeilen in einem Arbeitsblatt, bis zu maximal 16.384 Spalten nach 1.048.576 Zeilen ändern, indem erweiterte Servereigenschaften verwendet werden.

Excel-Daten stellt Daten mit minimaler Formatierung zur Verfügung. Die Standarddatenformatierung wird auf die Daten auf der Basis des Datentyps angewendet und geht davon aus, dass jede Spalte einen einzelnen Datentyp aufweist.

Die Ausgabe ist ähnlich wie andere Excel-Formate, mit folgenden Ausnahmen:

- Die generierte Ausgabe enthält nur die erste Listenabfrage in dem Bericht. Wenn ein Bericht mehrere Abfragen enthält und die erste Abfrage eine mehrdimensionale Abfrage für eine Kreuztabelle oder für ein Diagramm ist, wird bei der Ausführung des Berichts eine Fehlernachricht angezeigt.
- Verschachtelte Rahmen und Master-Detail-Links werden nicht unterstützt.
- Zellen in der Microsoft Excel-Datei haben eine Standardbreite und -höhe. Sie müssen die Spaltenbreite und -höhe anpassen, wenn die Daten größer als die Standardgröße sind.
- Stilspezifikationen werden nicht wiedergegeben, einschließlich Farbe, Hintergrundfarbe und Schriftarten.
- Grenzen werden nicht wiedergegeben.

- Die benutzerdefinierte Datenformatierung in der Berichtsspezifikation wird nicht angewendet, einschließlich der Hervorhebung von Ausnahmebedingungen und der Farbregeln für negative Zahlen.

CSV-Format

Berichte, die im CSV-Format (CSV-Format) gespeichert wurden, werden in der Anwendung geöffnet, die dem Dateityp ".csv" zugeordnet ist.

Sie müssen über die Berechtigung "Ausführen" und "traverse" für die Funktion " **CSV-Ausgabe generieren** " verfügen, um Berichtsausgaben im CSV-Format zu generieren.

Im CSV-Format gespeicherte Berichte

- sind für die Unterstützung von Unicode-Daten über viele Clientbetriebssysteme ausgelegt.
- sind UTF-16-Little-Endian-Daten-codiert
- Fügen Sie am Anfang der Datei ein BOM (Byte Order Mark) ein.
- Durch Tabulatoren begrenzt
- Zeichenfolgen in Anführungszeichen nicht einschließen
- Verwenden eines neuen Zeilenzeichens zum Begrenzen von Zeilen
- Zeigt nur die Ergebnisse einer Berichtsabfrage an. Seitenlayoutelemente, wie z. B. Titel, Bilder und Parameterwerte, werden in der CSV-Ausgabe nicht angezeigt.

Berichtssprachen

Sie können die Sprache für einen Bericht auswählen.

Sie können die Berichtssprache in den Berichtseigenschaften oder in Ihren Vorgaben angeben. Wenn Sie einen Bericht ausführen, wird die in den Berichtseigenschaften angegebene Sprache verwendet. Wenn sie in den Berichtseigenschaften nicht angegeben ist, wird die Sprache in Ihren Vorgaben verwendet.

Wenn Sie eine Sprache für Ihren Bericht auswählen, wird die Sprache, die im Portal verwendet wird, nicht geändert. Sie können die Sprache, die in der Portalschnittstelle verwendet wird, in Ihren Vorgaben ändern.

Wenn ein Bericht ausgeführt wird, stellt der Berichtsserver eine Verbindung zu der zugrunde liegenden Datenquelle her, um Daten abzurufen. Wenn der SAP BW-Server die Sprache, die der Ländereinstellung Ihres Inhalts zugeordnet ist, nicht unterstützt, überprüft IBM Cognos Analytics bei Verwendung einer SAP BW-Datenquelle eine Ländereinstellungszuordnung für eine entsprechende Ländereinstellung. Wenn der SAP BW-Server die Sprache für die entsprechende Ländereinstellung unterstützt, wird diese Sprache verwendet. Andernfalls wird der Bericht mit der Standardsprache ausgeführt, die auf dem SAP BW-Server installiert ist.

Um die Berichtssprache anzugeben, müssen Sie über Lese-und Schreibberechtigungen für den Bericht verfügen und die Berechtigungen für den Ordner, der den Bericht enthält, traversieren.

Das zum Erstellen des Berichts verwendete Paket muss mehrsprachige Daten enthalten, bevor die Berichtsausgaben in den ausgewählten Sprachen angezeigt werden.

Geben Sie die Sprache für einen Bericht an.

Wenn Sie die Sprache für einen Bericht angeben möchten, ändern Sie die Berichtseigenschaften.

Geben Sie die Standardaufforderungswerte für einen Bericht an.

Wenn ein Bericht Eingabeaufforderungen enthält, müssen Sie standardmäßig die Werte jedes Mal auswählen, wenn der Bericht ausgeführt wird. Sie können das Eingabeaufforderungsverhalten in den Berichtseigenschaften ändern.

Informationen zu diesem Vorgang

Wenn Sie Standardwerte für Eingabeaufforderungen festlegen möchten, müssen Sie über Lese-und Schreibberechtigungen für den Bericht verfügen und die Berechtigungen für den Ordner, der den Bericht enthält, lesen oder traversieren.

Wenn Sie der Berichtsersteller sind, können Sie Standardwerte für Eingabeaufforderungswerte für einen Bericht erstellen. Wenn der Bericht ausgeführt wird, werden die Daten basierend auf den von Ihnen angegebenen Eingabeaufforderungswerten automatisch gefiltert. Der Benutzer muss keine Eingabeaufforderungswerte angeben, wenn der Bericht ausgeführt wird. Dies ist hilfreich, wenn die meisten Benutzer bei jeder Ausführung eines Berichts die gleichen Eingabeaufforderungswerte verwenden.

Wenn Sie über Schreibzugriff auf einen Bericht verfügen und die Eingabeaufforderungswerte ändern, werden diese Werte für alle gespeichert, die den Bericht nach der Ausführung des Berichts ausführen. Wenn Sie Eingabeaufforderungswerte konsistent verwenden, die sich von der Mehrheit der Benutzer unterscheiden, erstellen Sie eine Berichtsansicht des Berichts.

Berichtsausgabe wird gespeichert

Sie wählen die Option zum Speichern von Berichtskopien als Bereitstellungsoption aus.

Alle Berichtsausgaben werden in IBM Cognos Analyticsautomatisch gespeichert. Sie können auch Kopien von Berichten in anderen Dateipositionen speichern:

- in IBM Cognos Analytics , so dass es erneut und zu Archivierungszwecken verwendet werden kann
- Außerhalb von IBM Cognos Analytics für die Verwendung in externen Anwendungen wie Websites und für die Verwendung durch Personen, die keinen Zugriff auf IBM Cognos Analytics haben

Sie können auch auswählen, wie ein Bericht gespeichert werden soll, wenn Sie ihn terminieren.

Vorbereitende Schritte

Bevor Sie die Berichtsausgabe an Dateipositionen speichern können, muss Ihr Administrator die Positionen einrichten.

Weitere Informationen zum Einrichten von Dateipositionen finden Sie unter „Gespeicherte Berichtsausgabe" auf Seite 87.

Vorgehensweise

1. Klicken Sie in einem Ordner oder einer Subskriptionsliste für den Bericht, den Sie ausführen möchten, auf die Schaltfläche "Mehr"  und dann auf **Ausführen als** oder **Einmal ausführen**.
2. Wählen Sie ein Ausgabeformat aus.
3. Wählen Sie bei Bedarf **Im Hintergrund ausführen**aus, klicken Sie auf **Erweitert**, und führen Sie anschließend die folgenden Schritte aus:
   a) Wählen Sie **Jetzt** aus oder wählen Sie **Später** aus, und geben Sie an, wann der Bericht ausgeführt werden soll.
   b) Wählen Sie in das Feld **Sprachen** eine oder mehrere Ausgabesprachen aus.
   c) Wählen Sie im Feld **Zustellung** aus, ob der Bericht wie folgt lauten soll:
      - als Anhang oder Link in einer E-Mail gesendet
      - an einen Drucker gesendet
      - als lokale Datei gespeichert
      - als externe Datei gespeichert

      Tipp: Die Option **Bericht als externe Datei speichern** ist nur verfügbar, wenn Sie eine Dateisystemposition für externe Dateien konfiguriert haben. Weitere Informationen finden Sie unter „Berichtsausgabedateien außerhalb von IBM Cognos -Software speichern" auf Seite 88.

d) Sie können auch ändern, wie der Dateikonflikt aufgelöst wird. Klicken Sie auf **Vorhandene beibehalten** , um vorhandene Dateien nicht zu überschreiben, oder **Ersetzen** , um vorhandene Dateien zu überschreiben. Klicken Sie auf **Zeitmarke** oder **Versionsnummer** , um zu verhindern, dass vorhandene Dateien überschrieben werden, indem Sie neue Dateien mit eindeutigen Zeitmarken oder Folgenummern erstellen.

e) Wenn mehr als eine Dateiposition definiert ist, wählen Sie die Position aus, an der Sie in der Liste **Position** speichern möchten.

4. Klicken Sie auf **Fertig**.

Angeben, wie lange Berichtsausgabeversionen aufbewahrt werden sollen

In den Berichtseigenschaften können Sie die Anzahl der Berichtsausgabeversionen angeben, die beibehalten werden sollen, und die Anzahl der Tage oder Monate, die beibehalten werden sollen.

Angeben, wie lange Berichtsausgabedaten beibehalten werden sollen

Sie können die Berichtsausgabe für eine bestimmte Anzahl von Ausführungen oder für eine bestimmte Anzahl von Tagen oder Monaten beibehalten.

Sie können beispielsweise die Berichtsausgabe für die zehn letzten Vorkommen beibehalten oder Sie können die Berichtsausgabe für die 2 Tage oder 6 Monate beibehalten.

Informationen zu diesem Vorgang

Sie müssen Lese-und Schreibberechtigungen für den Eintrag und die Lese-oder Transitberechtigungen für den Ordner, der den Eintrag enthält, haben.

Datenquellen mit benannten Sets können zu unvorhersehbaren Ergebnissen führen

Wenn Ihre dimensionalen Datenquellen benannte Gruppen enthalten, bei denen es sich um Gruppen von Membern oder um definierte Ausdrücke handelt, die für die Wiederverwendung erstellt werden, sind die Datenergebnisse in Query Studio unvorhersehbar, wenn sie mit Filterung und Verschachtelungsstufe kombiniert werden.

Wenn Ihre Datenquellen mehrere benannte Gruppen enthalten, sind die Datenergebnisse in Analysis Studio bei der Zusammenfassung unvorhersehbar.

Es wird daher empfohlen, Query Studio-und Analysis Studio-Benutzern das Aussetzen von benannten Gruppen oder benannten Gruppen auf mehreren Ebenen zu vermeiden.

Das Arbeiten mit benannten Gruppen kann auch zu unvorhersehbaren Ergebnissen in Reportingführen. Weitere Informationen finden Sie im IBM Cognos Analytics - Reporting *Benutzerhandbuch*.

Serie 7-Berichte in IBM Cognos Analytics

PowerPlay 7.3 oder höher kann für die Verwendung von IBM Cognos Analytics und nicht als Upfront als Portal konfiguriert werden. Wenn Sie jedoch auf Inhalte aus anderen IBM Cognos -Anwendungen oder -Versionen vor PowerPlay 7.3 zugreifen, kann der Administrator weiterhin vom Upfront-Portal abhängig sein.

Serie 7 PowerPlay Berichte und Cubes

Nach der Veröffentlichung von Berichten und Cubes von Series 7 PowerPlay in IBM Cognos Analytics können Sie PowerPlay -Authoring-Tools verwenden, um Series 7- PowerPlay -Berichte zu erstellen und zu bearbeiten.

Weitere Informationen zu PowerPlay -Authoring-Tools finden Sie im PowerPlay Web *Benutzerhandbuch*.

Sie können die Standardlaufoptionen von Series 7 PowerPlay -Berichten und -Würfeln ändern und mehrsprachige Eigenschaften auswählen.

Die Berichte und Cubes der Serie 7 PowerPlay funktionieren anders als in anderen Berichten. Die folgenden Aktionen gelten nicht für Berichte und Cubes der Serie 7 PowerPlay :

· Anzeigen der Ausführungsprotokoll-und Berichtsausgabeversionen.

· Angeben, wie lange Berichtsausgaben und -geschichten aufbewahrt werden sollen.

· Berichte werden storniert und ausgesetzt.

· Angeben von Eingabeaufforderungswerten für andere Berichtsformate als PDF.

· Geben Sie die Sprache für den Inhalt von Berichten an.

· Einen Bericht als Eigner ausführen.

· Planungsberichte.

· Berichte verteilen.

Single Signon

Mit der Einzelanmeldung wird sichergestellt, dass Benutzer, die bei einer IBM Cognos -Anwendung angemeldet sind, nicht zur Authentifizierung aufgefordert werden, wenn sie eine andere IBM Cognos -Anwendung ausführen.

Sie können sicherstellen, dass Ihre Benutzer von der Einzelanmeldung profitieren, indem Sie sicherstellen, dass sowohl IBM Cognos Analytics als auch PowerPlay denselben Series 7-Namespace wie ihre Authentifizierungsquelle verwenden. Alternativ können Sie sicherstellen, dass die Authentifizierungsnamensbereiche, die sowohl für IBM Cognos Analytics als auch für PowerPlay verwendet werden, für die Verwendung eines externen SSO-Mechanismus (Single Sign-on) für die Authentifizierung konfiguriert sind, wie z. B. Betriebssystemsignonen für Series 7 PowerPlay oder LDAP-Provider mit externer Identitätszuordnung in IBM Cognos Analytics.

Anweisungen zum Einrichten der Einzelanmeldung Series 7 finden Sie im Access Manager *Administratorhandbuch*.

Anweisungen zum Einrichten der Einzelanmeldung für das Berichterstellungsprodukt von IBM Cognos finden Sie im *Installations-und Konfigurationshandbuch*.

Ändern Sie die Standardwerte für einen Series 7-Bericht von PowerPlay

Sie können die Standardwerte für die Berichte von Series 7 PowerPlay ändern.

Wenn ein Bericht ausgeführt wird, können Sie eine der folgenden Standardaktionen auswählen:

· Führen Sie den Bericht im PDF-Format aus (Standard).

· Öffnen Sie den Bericht mit PowerPlay Web Explorer.

Für HTML-Formatberichte können Sie auswählen, ob der Bericht im Entwurfsmodus (ohne Daten) geöffnet werden soll. Das Öffnen eines Berichts im Entwurfsmodus ist nützlich, um die Struktur des Berichts schnell zu sehen.

Für Berichte im PDF-Format können Sie angeben, dass Sie zur Eingabe von Werten aufgefordert werden, die das in einem Bericht enthaltene Datenangebot filtern. Sie können beispielsweise einen Datumsbereich angeben, bei dem es sich um eine Untergruppe der im Bericht verfügbaren Daten handelt.

Wenn der Bericht "Series 7 PowerPlay " mit Eingabeaufforderungswerten erstellt wurde, werden Sie aufgefordert, Werte einzugeben, wenn der Bericht ausgeführt wird.

Mehrsprachige Eigenschaften für Serie 7 Berichte und Cubes

In IBM Cognos Analytics können Sie die mehrsprachigen Eigenschaften eines Series 7-Berichts oder -Würfels auswählen.

Die Einstellungen in IBM Cognos Analytics wirken sich nicht auf Inhalt, Daten, Kategoriebezeichnungen und andere Bezeichnungen aus. Die Sprache für diese Elemente wird vom PowerPlay -Administrator festgelegt, der den Bericht oder den Cube erstellt.

Kapitel 25. Menschliche Aufgaben verwalten

Es gibt drei Typen von Benutzertasks, die Sie in **Mein Posteingang**sehen können: Genehmigungsanforderungen, Ad-hoc-Tasks und Benachrichtigungsanforderungen.

Sie öffnen **Mein Posteingang** von Ihrem **Persönliches Menü** auf der Begrüßungsseite.

Tasks können erstellt werden aus

- Event Studio (Benachrichtigungsanforderungen und Genehmigungsanforderungen)

  Weitere Informationen finden Sie in Event Studio *Benutzerhandbuch*.
- **Mein Posteingang** (Benachrichtigungsanforderungen und Ad-hoc-Tasks).
- Eine Überwachungsregel, die für einen Bericht eingerichtet wurde (nur Benachrichtigungsanforderungen).

Genehmigungsanforderungen und Ad-hoc-Aufgaben

Sie können Genehmigungsanforderungen mit Event Studio erstellen.

Weitere Informationen finden Sie in Event Studio *Benutzerhandbuch*.

Sie können Ad-hoc-Tasks aus dem Taskeingang erstellen. Weitere Informationen finden Sie unter „Eine Ad-hoc-Aufgabe erstellen" auf Seite 376.

Eine Genehmigungsanforderung oder eine Ad-hoc-Task kann verschiedene Empfänger haben:

- Ein Taskeigner-ein bestimmter Benutzer
- Potenzielle Eigentümer-mehrere Benutzer, Gruppen, Rollen oder Verteilerlisten
- Interessenvertreter-eine oder mehrere Interessenten, die keine potenziellen Eigentümer sind

Wenn eine Task nur über einen potenziellen Eigner verfügt, wird dieser Benutzer automatisch zum Taskeigner. Wenn eine Task mehrere Eigner hat, wird der Benutzer, der die Task beansprucht, zum Aufgabeneigentümer.

Es ist möglich, eine Task mit einem oder mehreren Stakeholdern zu erstellen, aber keinen Eigentümer oder potenzielle Eigentümer. In diesem Fall können Stakeholder potenzielle Eigentümer nach der Erstellung zuordnen.

Taskstatus

Der Status einer Genehmigungsanforderung oder einer Ad-hoc-Task kann einer der folgenden sein:

- Nicht gestartet-die Task wartet darauf, gestartet zu werden.
- Gestartet-Die Task verfügt über einen Eigner und ist in Bearbeitung.
- Abgeschlossen-Der Eigner hat die Task abgeschlossen.
- Abgebrochen-die Task wurde von einem Empfänger abgebrochen.

Kommentare anzeigen

Sie können Kommentare anzeigen, die von anderen Empfängern hinzugefügt wurden, sowie Kommentare zu Prüfprotokolldaten, die vom System aufgezeichnet wurden.

Sie können auch Ihre eigenen Kommentare zu einer Aufgabe hinzufügen. Weitere Informationen finden Sie unter „Kommentare zu einer Aufgabe hinzufügen" auf Seite 380.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.

2. Wählen Sie die Task aus, für die Sie Kommentare anzeigen möchten, und klicken Sie anschließend in der Leseeinheit auf die Registerkarte **Diskussion** .

   Standardmäßig werden nur Benutzerkommentare angezeigt.
3. Wählen Sie in der Dropdown-Liste Kommentare den Typ der Kommentare aus, die angezeigt werden sollen.

   Sie können alle Benutzer-und Prüfkommentare anzeigen, oder Sie können die Anzeige nach Kommentartyp filtern.

E-Mail-Benachrichtigungen abonnieren

Wenn die Task erstellt wird, werden die Standardbenachrichtigungsoptionen eingerichtet. Sie können Ihre Subskriptionen für eine Task mit dem Status 'Nicht gestartet' oder 'Gestartet' ändern.

Sie können Benachrichtigungen empfangen oder empfangen, wenn

· Eine Aufgabe wird nicht mit dem Startdatum gestartet

· Eine Aufgabe wird bis zum Fälligkeitsdatum nicht abgeschlossen

· Der Status einer Taskänderung (gestartet, abgeschlossen oder abgebrochen)

· Der Eigner einer Taskänderung

· Ein Benutzerkommentar wird zu einer Task hinzugefügt.

Anmerkung:

· Benachrichtigungen werden an den Taskeigner gesendet und an alle Beteiligten kopiert.

· Der Empfänger, der den Status oder Eigner einer Task ändert oder einen Benutzerkommentar hinzufügt, empfängt die zugeordnete Benachrichtigung nicht.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die Task aus, für die Sie Ihre Benachrichtigungssubskriptionen ändern möchten, und klicken Sie anschließend in der Leseeinheit auf die Registerkarte **Benachrichtigungsoptionen** .
3. Wählen Sie die entsprechenden Kontrollkästchen für die Benachrichtigungen aus, die Sie empfangen möchten, und löschen Sie die Kontrollkästchen für die Benachrichtigungen, die nicht erforderlich sind.
4. Klicken Sie auf **Speichern**.

Eine Ad-hoc-Aufgabe erstellen

Erstellen Sie eine Ad-hoc-Task, um eine Task an den Taskeingang der von Ihnen angegebenen Empfänger zu senden.

Sie können zu einer Ad-hoc-Task Fristen hinzufügen, wenn Sie sie erstellen. Alternativ können potenzielle Eigentümer oder Stakeholder Fristen zu einem späteren Zeitpunkt hinzufügen, indem sie die Task aus ihrem Taskeingang aktualisieren.

Sie können Benachrichtigungsoptionen für den Taskeigner einrichten, um E-Mails zu empfangen, wenn

· Eine Ad-hoc-Aufgabe wird bis zum Fälligkeitsdatum nicht abgeschlossen

· Eine Ad-hoc-Task wird nicht mit dem Startdatum gestartet.

Anmerkung: Die Stakeholder werden auch auf diese E-Mails kopiert.

Darüber hinaus können Sie Benachrichtigungsoptionen für den Taskeigner und alle Stakeholder einrichten, um E-Mails zu empfangen, wenn

· Der Status einer Ad-hoc-Taskänderung (gestartet, abgeschlossen oder abgebrochen)

· Der Eigner einer Ad-hoc-Taskänderung

· Ein Kommentar wird zu einer Ad-hoc-Task hinzugefügt.

Anmerkung: Potenzielle Eigentümer und Stakeholder können sich nicht subskribieren, indem sie bestimmte Benachrichtigungen empfangen, indem sie die Task aus ihrem Taskeingang aktualisieren.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie in der Dropdown-Liste "Task" die Option **Neue Aufgabe**  aus.
3. Klicken Sie im Lesebereich auf **Empfänger hinzufügen/entfernen**.

   Die Seite **Empfänger auswählen** wird angezeigt.
4. Wählen Sie die erforderlichen Benutzer, Gruppen, Rollen und Verteilerlisten aus, die als potenzielle Eigentümer und Stakeholder hinzugefügt werden sollen.

   · Wenn Sie aus aufgelisteten Einträgen auswählen möchten, klicken Sie auf den entsprechenden Namespace, und wählen Sie anschließend die Kontrollkästchen neben den Benutzern, Gruppen, Rollen oder Verteilerlisten aus.

   Tipp: Um die Benutzereinträge sichtbar zu machen, klicken Sie auf **Benutzer anzeigen** in der Liste.

   · Um nach Einträgen zu suchen, klicken Sie auf **Suchen** und geben Sie in das Feld **Suchbegriff** den Ausdruck ein, nach dem gesucht werden soll. Klicken Sie für Suchoptionen auf **Bearbeiten**. Suchen und klicken Sie auf den gewünschten Eintrag.

   · Wenn Sie den Namen der Einträge eingeben möchten, die hinzugefügt werden sollen, klicken Sie auf **Typ** , und geben Sie die Namen der Gruppen, Rollen oder Benutzer ein. Verwenden Sie dabei das folgende Format, wobei ein Semikolon (;) jeden Eintrag trennt:*namespace/group_name*;*namespace/role_name*;*namespace/user_name*;

   Im Folgenden sehen Sie ein Beispiel:

   Cognos/Authors; LDAP/scarter;
5. Klicken Sie auf die **Potenzieller Eigner** -oder **Stakeholder** -Pfeilschaltfläche, um die **Ausgewählte Einträge** -Liste zu aktualisieren, und klicken Sie auf **OK**.

   Tipp: Wenn Sie Einträge aus der Liste **Ausgewählte Einträge** entfernen möchten, wählen Sie sie aus und klicken Sie auf **Entfernen**. Wenn Sie alle Einträge in der Liste auswählen möchten, wählen Sie das Kontrollkästchen für die Liste aus.
6. Klicken Sie auf **OK**.
7. Geben Sie in das Feld **Betreff** den Betreff der Task ein.
8. Fügen Sie bei Bedarf eine Fertigstellungsfrist für die Task in der **Fälligkeitsdatum** -Box hinzu.
9. Fügen Sie bei Bedarf eine Startzeit für die Task in der **Starten von** -Box hinzu.
10. Wählen Sie die Priorität in der Liste **Priorität** aus.
11. Geben Sie in das Feld **Nachricht** direkt Text ein.
12. Klicken Sie zum Hinzufügen von Links auf **Links hinzufügen**, wählen Sie die gewünschten Einträge aus, klicken Sie auf die Pfeilschaltfläche, um die **Ausgewählte Einträge** -Liste zu aktualisieren, und klicken Sie auf **OK**.

    Tipp: Um Links zu entfernen, wählen Sie sie aus und klicken Sie auf **Links entfernen**.
13. Wenn Sie Benachrichtigungsoptionen einrichten möchten, klicken Sie auf **Erweitert**, andernfalls fahren Sie mit Schritt 16 fort.
14. Wählen Sie die Optionen für die Taskerstellung und die Endterminbenachrichtigung wie erforderlich aus:

    · **Benachrichtigung senden, wenn nicht mit dem Startdatum gestartet wird**

    · **Benachrichtigung senden, wenn nicht bis zu Fälligkeitsdatum abgeschlossen**
15. Wählen Sie die Optionen für die Benachrichtigungsanforderung für Genehmigungsanforderung wie erforderlich aus:

    · **Gestartet**

- **Kommentar**
- **Eigner geändert**
- **Abgeschlossen**
- **Abgebrochen**

16. Klicken Sie auf **Speichern**.

Aktionen, die Sie für Genehmigungsanforderungen und Ad-hoc-Tasks ausführen können

Die Aktionen, die Sie für eine Genehmigungsanforderung oder eine Ad-hoc-Task ausführen können, unterscheiden sich abhängig von Ihrem Empfängertyp.

In der folgenden Tabelle werden die Aktionen zusammengefasst, die von jedem Empfängertyp ausgeführt werden können.

Tabelle 77. Genehmigungsanforderung und Ad-hoc-Aktionen nach Empfängertyp

Aktion	Potenzieller Eigner	Eigner	Stakeholder
Eigentumsrecht an einer Aufgabe übernehmen	X		
Empfänger für eine Task ändern	X	X	X
Eigentumsrecht für eine Task widerrufen		X	
Fristen für eine Aufgabe festlegen	X	X	X
Priorität einer Task ändern	X	X	X
Kommentare zu einer Task hinzufügen	X	X	X
Task starten oder stoppen		X	
Eine Task abschließen		X	
Task abbrechen		X	X

Task anfordern

Wenn Sie ein potenzieller Eigner einer Aufgabe sind, die nicht beansprucht wird, können Sie die Task anfordern. Die Aufgabe ist dann Eigentum von Ihnen.

Wenn Sie der einzige potenzielle Eigner einer Task sind, wird die Task automatisch Eigentum von Ihnen. In diesem Fall ist es nicht erforderlich, die Aufgabe zu beanspruchen.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.

2. Wählen Sie die Aufgabe aus, die Sie beanspruchen möchten, und klicken Sie dann im Lesebereich auf **Machen Sie mich zum Eigentümer** .

Empfänger für eine Aufgabe ändern

Jeder Taskempfänger kann den aktuellen Eigner einer Task ändern.

Darüber hinaus können sie potenzielle Eigentümer und Stakeholder für eine Aufgabe hinzufügen oder entfernen. Der Status der Task muss nicht gestartet oder gestartet sein.

Anmerkung: Wenn Sie der Eigner einer Task sind, können Sie das Eigentumsrecht für die Task „Eigentumsrecht für eine Aufgabe widerrufen" auf Seite 380widerrufen.

Eigner des Aktuell s ändern

Sie können den aktuellen Eigner ändern.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die Task aus, für die Sie den aktuellen Eigner ändern möchten, und klicken Sie anschließend in der Leseeinheit auf **Eigner ändern** .

   Die Seite **Benutzer auswählen** wird angezeigt.
3. Wählen Sie den Benutzer aus.
   - Wenn Sie aus aufgelisteten Einträgen auswählen möchten, klicken Sie auf den entsprechenden Namespace und wählen Sie dann den erforderlichen Benutzer aus.
   - Um nach einem Eintrag zu suchen, klicken Sie auf **Suchen** und geben Sie in das Feld **Suchbegriff** den Ausdruck ein, nach dem gesucht werden soll. Klicken Sie für Suchoptionen auf **Bearbeiten**. Suchen und klicken Sie auf den gewünschten Eintrag.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Speichern**.

Potenzielle Eigentümer und Interessenträger ändern

Sie können die potenziellen Eigentümer und Stakeholder ändern.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die Task aus, für die Sie potenzielle Eigentümer und Stakeholder ändern möchten, und klicken Sie anschließend in der Leseeinheit auf **Empfänger hinzufügen/entfernen** .

   Die Seite **Empfänger auswählen** wird angezeigt.
3. Wählen Sie die erforderlichen Benutzer, Gruppen, Rollen und Verteilerlisten aus.
   - Wenn Sie aus aufgelisteten Einträgen auswählen möchten, klicken Sie auf den entsprechenden Namespace, und wählen Sie anschließend die Kontrollkästchen neben den Benutzern, Gruppen, Rollen oder Verteilerlisten aus.

     Tipp: Um die Benutzereinträge sichtbar zu machen, klicken Sie auf **Benutzer anzeigen** in der Liste.
   - Um nach Einträgen zu suchen, klicken Sie auf **Suchen** und geben Sie in das Feld **Suchbegriff** den Ausdruck ein, nach dem gesucht werden soll. Klicken Sie für Suchoptionen auf **Bearbeiten**. Suchen und klicken Sie auf den gewünschten Eintrag.
   - Wenn Sie den Namen der Einträge eingeben möchten, die hinzugefügt werden sollen, klicken Sie auf **Typ** , und geben Sie die Namen von Gruppen, Rollen oder Benutzern ein. Verwenden Sie dabei das folgende Format, wobei ein Semikolon (;) jeden Eintrag trennt:

     namespace/group_name;*namespace/role_name*;*namespace/user_name*;

Im Folgenden sehen Sie ein Beispiel:

Cognos/Authors; LDAP/scarter;

4. Klicken Sie auf die **Potenzieller Eigner** -oder **Stakeholder** -Pfeilschaltfläche, um die **Ausgewählte Einträge** -Liste zu aktualisieren, und klicken Sie auf **OK**.

   Tipp: Wenn Sie Einträge aus der Liste **Ausgewählte Einträge** entfernen möchten, wählen Sie sie aus und klicken Sie auf **Entfernen**. Wenn Sie alle Einträge in der Liste auswählen möchten, wählen Sie das Kontrollkästchen für die Liste aus.
5. Klicken Sie auf **OK**.
6. Klicken Sie auf **Speichern**.

Eigentumsrecht für eine Aufgabe widerrufen

Wenn Sie der Eigentümer einer Aufgabe sind, können Sie sich selbst als Aufgabeneigentümer entfernen.

Dadurch wird der Eigner in 'Nicht beansprucht' und der Status der Task in 'Nicht gestartet' geändert.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die Task aus, die widerrufen werden soll, und klicken Sie anschließend im Lesebereich auf **Mich als Eigentümer entfernen** .

Fristen für eine Aufgabe festlegen

Jeder Taskempfänger kann ein Startdatum oder ein Fälligkeitsdatum für eine Genehmigungsanforderung oder eine Ad-hoc-Task mit dem Status 'Nicht gestartet' oder 'Gestartet' hinzufügen. Sie können auch bestehende Fristen ändern.

Wenn Benachrichtigungen eingerichtet werden, wenn eine Aufgabe nicht durch die erforderliche Zeit gestartet oder abgeschlossen wird, werden E-Mail-Benachrichtigungen gesendet, die alle potenziellen Eigner und Stakeholder subskribieren. Weitere Informationen zu Benachrichtigungen finden Sie unter „E-Mail-Benachrichtigungen abonnieren” auf Seite 376.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die Task aus, für die Sie die Fristen aktualisieren möchten.
3. Fügen Sie bei Bedarf eine Fertigstellungsfrist für die Task in der **Fälligkeitsdatum** -Box hinzu.
4. Fügen Sie bei Bedarf eine Startzeit für die Task in der **Starten von** -Box hinzu.
5. Klicken Sie auf **Speichern**.

Priorität einer Aufgabe ändern

Die Priorität einer Task wird festgelegt, wenn die Task erstellt wird. Jeder Taskempfänger kann die Priorität einer Task mit dem Status 'Nicht gestartet' oder 'Gestartet' ändern.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die Task aus, für die Sie die Priorität ändern möchten, und wählen Sie anschließend die Priorität aus der Liste **Priorität** in der Leseeinheit aus.
3. Klicken Sie auf **Speichern**.

Kommentare zu einer Aufgabe hinzufügen

Jeder Taskempfänger kann Kommentare zu einer Task hinzufügen.

Informationen zum Anzeigen von Kommentaren, die einer Task hinzugefügt wurden, finden Sie unter „Kommentare anzeigen“ auf Seite 375.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die Task aus, für die Sie einen Kommentar hinzufügen möchten, und klicken Sie anschließend in der Leseeinheit auf die Registerkarte **Diskussion** .
3. Klicken Sie auf **Kommentar hinzufügen**  , geben Sie Ihre Kommentare in das Fenster ein, das angezeigt wird, und klicken Sie dann auf **OK**.
4. Klicken Sie auf **Speichern**.

Task starten oder stoppen

Wenn Sie der Eigner einer Task sind, die noch nicht gestartet wurde, können Sie die Task starten.

Dadurch wird der Status 'Gestartet' geändert, so dass andere Taskempfänger den Fortschritt Ihrer Task anzeigen können.

Ein potenzieller Eigner kann auch eine nicht beanspruchte Task starten. Der Benutzer wird dann zum Eigner dieser Task.

Wenn Sie eine Task besitzen, die bereits gestartet wurde, können Sie die Task stoppen. Dadurch wird der Status in 'Nicht gestartet' geändert.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die Task aus, die gestartet werden soll, und wählen Sie anschließend **Task starten** in der Dropdown-Liste **Status** im Lesebereich aus.

   Tipp: Wenn Sie eine Task stoppen möchten, die gestartet wurde, wählen Sie **Nicht gestartet** in der Dropdown-Liste **Status** aus.
3. Klicken Sie auf **Speichern**.

Aufgabe abschließen

Wenn Sie der Eigner einer Task mit dem Status "Nicht gestartet" oder "Gestartet" sind, können Sie die Task ausführen, indem Sie die erforderliche Aktion ausführen.

Die erforderliche Aktion ist je nach Tasktyp unterschiedlich. Für Ad-hoc-Tasks müssen Sie die Task als abgeschlossen markieren.

Für Genehmigungsanforderungsaufgaben hängt die Aktion davon ab, wie der Task-Ersteller die Task konfiguriert hat. Sie müssen eine der folgenden Aktionen ausführen:

- die Anforderung genehmigen oder zurückweisen

  Für diesen Typ der Genehmigungsanforderung müssen Sie die Anforderung von Ihrem Taskeingang genehmigen oder zurückweisen, um die Task abzuschließen.

  Je nachdem, wie die Task eingerichtet wurde, kann die Beendigung der Task dazu führen, dass eine andere Aktion ausgeführt wird. Wenn Sie z. B. eine Anforderung zum Verteilen eines Berichts genehmigen, wenn die Task abgeschlossen ist, kann der Bericht automatisch verteilt werden. Wenn die Anforderung zurückgewiesen wird, werden keine weiteren Aktionen ausgeführt.
- Geben Sie die verbleibenden Tasks für die Genehmigung und Ausführung an.

  Dieser Typ der Genehmigungsanforderung enthält eine oder mehrere Tasks, die nach Abschluss der Task ausgeführt werden sollen. Sie müssen auswählen, welche Tasks ausgeführt werden sollen.

Eine Ad-Hoc-Task abschließen

Die Prozedur zum Ausführen einer Ad-hoc-Task ist wie folgt.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die Task aus, die abgeschlossen werden soll, und klicken Sie dann auf **Als abgeschlossen markieren**.

   Der Status der Task ändert sich in "Abgeschlossen".

Anforderung genehmigen oder zurückweisen

Die Prozedur zum Genehmigen oder Zurückweisen einer Anforderung ist wie folgt.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die Task aus, die Sie ausführen möchten, und zeigen Sie die Details im Lesebereich an.
3. Fügen Sie bei Bedarf einen Kommentar hinzu, um Ihre Entscheidung in der **Kommentar** -Box zu erläutern.
4. Klicken Sie auf **Genehmigen** oder **Zurückweisen** , um die Task abzuschließen.

   Anmerkung: Genehmigen und **Zurückweisen** sind die Standardschaltflächennamen. Der Benutzer, der die Task erstellt hat, hat möglicherweise angepasste Schaltflächennamen verwendet, die sich von der Standardeinstellung unterscheiden.

   Der Status der Task ändert sich in "Abgeschlossen".

Geben Sie die verbleibenden Tasks an, die Genehmigt und ausgeführt werden sollen

Sie können die verbleibenden Tasks angeben, die genehmigt und ausgeführt werden sollen.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die Task aus, die Sie ausführen möchten, und zeigen Sie die Details im Lesebereich an.
3. Wählen Sie die verbleibenden Tasks aus, die genehmigt werden sollen, und klicken Sie auf **Übergeben**.

   Anmerkung: Übergeben ist der Standardschaltflächenname. Der Benutzer, der die Task erstellt hat, hat möglicherweise einen angepassten Button-Namen verwendet, der sich von der Standardeinstellung unterscheidet.

   Der Status der Task ändert sich in "Abgeschlossen".

Task abbrechen

Ein Taskeigner oder Stakeholder kann eine Genehmigungsanforderung oder eine Ad-hoc-Task mit dem Status 'Nicht gestartet' oder 'Gestartet' abbrechen.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die Task aus, die Sie abbrechen möchten, und klicken Sie anschließend in der Leseeinheit auf **Als abgebrochen markieren** .

   Der Status der Task ändert sich in "Storniert".

Benachrichtigungsanforderungen

Sie können eine Benachrichtigungsanforderung mit einer Option für Empfänger erstellen, um die Anforderung zu bestätigen. Sie können auch Fristen für Bestätigungen angeben.

Eine Benachrichtigungsanforderung kann verschiedene Empfänger haben:

- Benutzer, Gruppen, Rollen und Verteilerlisten, an die die Anforderung gesendet wird (Empfängerlistenempfänger)
- Stakeholder, an die die Anforderung kopiert wird (Empfänger von CC-Listen)

Der Status einer Benachrichtigungsanforderung kann

- Ungelesst-die Anforderung wurde von einem Empfänger nicht geöffnet
- Lesen-Die Anforderung wurde von einem Empfänger geöffnet
- Bestätigt-die Anforderung wurde von einem Empfänger bestätigt, der auf der To-Liste enthalten ist.

Benachrichtigungen können auch in IBM Cognos Event Studio erstellt werden. Weitere Informationen finden Sie in Event Studio *Benutzerhandbuch*.

Danksagungen

Wenn eine Benachrichtigungsanforderung erstellt wird, können Sie von jedem Empfänger, der in der Liste "To" enthalten ist, eine Bestätigung anfordern.

Anmerkung: Interessenvertreter (Empfänger von CC-Listen) haben nicht die Möglichkeit, Benachrichtigungsanforderungen zu bestätigen.

Fristen

Wenn eine Benachrichtigungsanforderung erstellt wird, können Sie eine Bestätigungsfrist angeben. Sie können auch angeben, dass eine E-Mail an jeden Empfänger in der To-Liste gesendet wird, der eine Benachrichtigungsanforderung nicht bis zum Endtermin bestätigt. Zum Stichtag wird eine separate E-Mail an die Stakeholder in der Liste CC gesendet, in der sie darüber informiert werden, dass einige Empfänger in der Liste "To" die Benachrichtigungsanforderung nicht bestätigt haben.

Tipp: Ein Stakeholder kann prüfen, wer eine Benachrichtigungsanforderung bestätigt hat, indem er E-Mails oder die Prüftabellen überprüft.

Wenn alle Empfänger der To-Liste die Anforderung bestätigt haben, wird die Frist abgebrochen.

Benachrichtigungsanforderung erstellen

Fügen Sie eine Benachrichtigungsanforderung zu einem Agenten hinzu, um eine sichere Benachrichtigung über ein Ereignis an den von Ihnen angegebenen Posteingang zu senden.

Sie können eine Bestätigung anfordern und eine Bestätigungsfrist hinzufügen.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie **Neue Benachrichtigung**  in der Task-Dropdown-Liste aus.
3. Klicken Sie in der Leseeinheit auf **Empfänger hinzufügen/entfernen** .

   Die Seite **Empfänger auswählen** wird angezeigt.
4. Wählen Sie die erforderlichen Benutzer, Gruppen, Rollen und Verteilerlisten aus, die als Empfänger hinzugefügt werden sollen.
   - Wenn Sie aus aufgelisteten Einträgen auswählen möchten, klicken Sie auf den entsprechenden Namespace, und wählen Sie anschließend die Kontrollkästchen neben den Benutzern, Gruppen, Rollen oder Verteilerlisten aus.

Tipp: Um die Benutzereinträge sichtbar zu machen, klicken Sie auf **Benutzer anzeigen** in der Liste.

- Um nach Einträgen zu suchen, klicken Sie auf **Suchen** und geben Sie in das Feld **Suchbegriff** den Ausdruck ein, nach dem gesucht werden soll. Klicken Sie für Suchoptionen auf **Bearbeiten**. Suchen und klicken Sie auf den gewünschten Eintrag.
- Wenn Sie den Namen der Einträge eingeben möchten, die hinzugefügt werden sollen, klicken Sie auf **Typ** , und geben Sie die Namen von Gruppen, Rollen oder Benutzern ein. Verwenden Sie dabei das folgende Format, wobei ein Semikolon (;) jeden Eintrag trennt:

  namespace/group_name;*namespace/role_name*;*namespace/user_name*;

  Im Folgenden sehen Sie ein Beispiel:

  Cognos/Authors; LDAP/scarter;

5. Klicken Sie auf die **Bis** -oder **Cc** -Pfeilschaltfläche, um die **Ausgewählte Einträge** -Liste zu aktualisieren, und klicken Sie auf **OK**.

   Tipp: Wenn Sie Einträge aus der Liste **Ausgewählte Einträge** entfernen möchten, wählen Sie sie aus und klicken Sie auf **Entfernen**. Wenn Sie alle Einträge in der Liste auswählen möchten, wählen Sie das Kontrollkästchen für die Liste aus.
6. Klicken Sie auf **OK**.
7. Geben Sie in das Feld **Betreff** den Betreff der Benachrichtigungsanforderung ein.
8. Geben Sie in das Feld **Nachricht** direkt Text ein.
9. Klicken Sie zum Hinzufügen von Links auf **Links hinzufügen**, wählen Sie die gewünschten Einträge aus, klicken Sie auf die Pfeilschaltfläche, um die **Ausgewählte Einträge** -Liste zu aktualisieren, und klicken Sie auf **OK**.

   Tipp: Um Links zu entfernen, wählen Sie sie aus und klicken Sie auf **Links entfernen**.
10. Wenn Sie Benachrichtigungsoptionen einrichten möchten, klicken Sie auf **Erweitert**, andernfalls fahren Sie mit Schritt 13 fort.
11. Wählen Sie das Feld **Bestätigung anfordern** aus, um eine Bestätigung von jedem Empfänger in der Liste "Bis" anzufordern.
12. Wenn Sie eine E-Mail-Benachrichtigung an Empfänger senden möchten, die die Anforderung nicht bis zu einem Endtermin bestätigen, wählen Sie das Feld **Benachrichtigung senden, wenn bis zum Datum nicht bestätigt** aus und wählen Sie dann das erforderliche Datum aus.
13. Klicken Sie auf **Speichern**.

Benachrichtigungsanforderung lesen und bestätigen

Neue Benachrichtigungsanforderungen in Ihrem Task-Posteingang haben den Status Ungelesen.

Sie können die Benachrichtigungsanforderung lesen und bestätigen, wenn diese Option für Sie verfügbar ist.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die ungelesene Benachrichtigungsanforderung aus, die Sie lesen möchten, und zeigen Sie die Details in der Leseeinheit an.

   Der Status der Benachrichtigungsanforderung ändert sich in "Lesen".
3. Wenn Ihr Benutzername in der Liste **Bis** angezeigt wird und eine Bestätigung erforderlich ist, klicken Sie auf **Bestätigen**.

   Der Status der Benachrichtigungsanforderung ändert sich in 'Bestätigt'.

   Anmerkung: Wenn Ihr Benutzername in der Liste **Bis** angezeigt wird, handelt es sich um einen Empfänger der Benachrichtigungsanforderung. Wenn sie in der Liste **CC** angezeigt wird, werden Sie ein Stakeholder, der auf die Anforderung kopiert wurde. Wenn für die Benachrichtigungsanforderung eine Frist festgelegt wurde, wird sie in der **Frist** -Box angezeigt.

Archivierungsaufgaben

Bei der Archivierung handelt es sich um eine Methode, um unerwünschte Aufgaben aus Ihrem Posteingang zu entfernen.

Wenn Sie eine Task archivieren, bleibt sie in IBM Cognos Analyticsaktiv, und andere Taskempfänger können weiterhin mit ihr arbeiten. Alle Benachrichtigungen, die einer archivierten Task zugeordnet sind, bleiben ebenfalls aktiv.

Tasks, die aus Ihrem Archiv gelöscht werden, bleiben ebenfalls aktiv, aber Sie können sie nicht mehr anzeigen.

Vorgehensweise

1. Zeigen Sie Ihren Taskeingang an.
2. Wählen Sie die Tasks aus, die archiviert werden sollen, und klicken Sie anschließend in der Dropdown-Liste **Verschieben nach** auf **Archiv**  .

Taskarchiv anzeigen

Sie können eine Liste der Tasks anzeigen, die Sie archiviert haben.

Vorgehensweise

Zeigen Sie Ihren Taskeingang an, und klicken Sie anschließend auf die Registerkarte **Archiv** .

Nächste Schritte

Sie können die Details einer Task anzeigen, indem Sie sie auswählen. Die Taskdetails werden in der Leseeinheit angezeigt. Wenn die Task einen Anhang enthält, z. B. einen Bericht, können Sie doppelt darauf klicken, um sie anzuzeigen.

Tipp:

- Wenn Sie das Fälligkeitsdatum für Tasks anstelle des empfangenen Datums anzeigen möchten, wählen Sie **Fälligkeitsdatum anzeigen** in der Dropdown-Liste **Anzeigedatum empfangen** aus.
- Um zu Ihrem Taskeingang zurückzukehren, klicken Sie auf die Registerkarte **Eingang** .
- Wenn Sie unerwünschte Tasks löschen möchten, wählen Sie sie aus und klicken Sie dann auf **Löschen**  .

Kapitel 26. Drillthrough-Zugriff

Drillthrough-Anwendungen sind ein Netzwerk von verlinkten Berichten, die Benutzer navigieren können, indem sie ihren Kontext und ihren Fokus behalten, um Informationen zu untersuchen und zu analysieren.

Der Drillthrough-Zugriff hilft Ihnen, Anwendungen zu erstellen, die größer als ein einzelner Bericht sind.

Beispiel: Sie verfügen über einen Analysis Studio-Bericht, in dem die Einnahmen angezeigt werden, und Sie möchten in der Lage sein, einen Drillthrough zu einem Reporting -Bericht durchzuführen, in dem Details zu geplanten und tatsächlichen Einnahmen angezeigt werden.

Ein weiteres Beispiel ist ein Analysis Studio-Bericht, in dem die Top 10-Rabatte des Einzelhändlers aufgelistet werden und Sie in der Lage sein möchten, einen Drillthrough zu einem Reporting -Bericht durchzuführen, der die Umsatzerlöse für Werbeaktionen anzeigt.

Drillthrough-Zugriff funktioniert, indem Informationen von der Quelle an das Zielobjekt übergeben werden, in der Regel ein Bericht. Sie definieren, was aus dem Quellenbericht übergeben wird, indem Sie die Systemübereinstimmungsinformationen aus dem Auswahlkontext des Quellenberichts auf den Inhalt des Ziels (dynamischer Drillthrough) oder durch Definieren von Parametern im Ziel (parametrisierter Drillthrough) angeben. Sie definieren Drillthrough-Zugriff für die Quelle, entweder auf der Paketebene oder auf der Berichtsebene. In einem Paket steuern Sie den Umfang der Daten, für die Drillthrough-Zugriff in der Drillthrough-Definition verfügbar ist. In einem Bericht definieren Sie den Drillthrough-Zugriff für ein Berichtselement.

Was Sie wissen sollten

Für einen Drillthrough-Link zur Arbeit ist es erforderlich, Folgendes zu wissen:

- was der Quellenbericht ist oder sein wird
- was der Zielbericht ist oder sein wird
- ob die Benutzer des Drillthrough-Links im Quellenbericht über die entsprechenden Berechtigungen zum Anzeigen oder Ausführen des Zielberichts verfügen.
- wie die Daten in den beiden Berichten miteinander verknüpft sind

  Abhängig von den zugrunde liegenden Daten können Sie eine Drillthrough-Definition (dynamischer Drillthrough) erstellen oder die Quellenmetadaten den Parametern zuordnen, die im Zielbericht oder im Zielpaket definiert sind (parametrisierter Drillthrough).
- Angabe, ob der Zielbericht ausgeführt oder geöffnet werden soll

  Das Ziel des Drillthrough-Zugriffs ist in der Regel eine gespeicherte Berichtsdefinition. Der Bericht kann in Reporting, PowerPlay Studio, Query Studio oder Analysis Studio erstellt werden. Das Ziel des Drillthrough-Zugriffs kann auch ein Paket sein, das einen PowerCube enthält. In diesem Fall wird eine Standardansicht des PowerCubes erstellt.
- Wenn das Ziel ausgeführt wird, in welchem Format es ausgeführt werden soll und welche Filter für die Ausführung verwendet werden sollen

  Wenn Sie den Zielbericht nicht bedarfsgerecht ausführen möchten, können Sie stattdessen eine Verknüpfung mit einem Lesezeichen in der gespeicherten Ausgabe herstellen.

Quellen und Ziele

Es gibt viele verschiedene Kombinationen von Quelle und Ziel. Beispiel: Sie können einen Drillthrough durchführen.

- zwischen Berichten, die in verschiedenen Paketen für unterschiedliche Datenquellentypen erstellt wurden, wie z. B. aus einer Analyse für einen Cube zu einem detaillierten Bericht für eine relationale

Datenquelle. Weitere Informationen zum Erstellen eines Drillthrough-Zugriffs in Paketen finden Sie im Artikel „Drillthrough-Zugriff in Paketen einrichten" auf Seite 394.

- von einem vorhandenen Bericht zu einem anderen Bericht mit Reporting. Weitere Informationen zum Erstellen eines Drillthrough-Zugriffs in einem Bericht finden Sie unter „Drillthrough-Zugriff in einem Bericht einrichten" auf Seite 401 .
- zwischen IBM Cognos Viewer-Berichten, die in Reporting, Query Studio, PowerPlay Studio und Analysis Studio verfasst wurden
- aus Series 7 PowerPlay Webcubes zu IBM Cognos Analytics -Berichten.

Verstehen von Drillthrough-Konzepten

Bevor Sie den Drillthrough-Zugriff einrichten, müssen Sie die Schlüsselkonzepte zum Durchbohren verstehen. Die Kenntnis dieser Konzepte wird Ihnen helfen, Fehler zu vermeiden, damit die Konsumenten so effizient wie möglich bohren können.

Drillthrough-Pfade

Sie können einen Drillthrough-Pfad in einem Quellenbericht erstellen oder Drillthrough-Definitionen verwenden. Ein Drillthrough-Pfad ist die Definition des Pfads, der ausgeführt wird, wenn von einem Bericht in einen anderen verschoben wird, einschließlich der Art und Weise, wie die Datenwerte zwischen den Berichten übergeben werden.

Mit **Drillthrough-Definitionen**können Sie einen Drillthrough-Pfad aus einem beliebigen Bericht im Quellenpaket zu einem beliebigen Zielbericht in einem anderen Paket erstellen. Diese Art der Drillthrough-Definition wird im Quellenpaket gespeichert.

Für jeden Zielbericht, der Parameter enthält, sollten Sie die Zielparameter den richtigen Metadaten im Drillthrough-Pfad zuordnen. Dadurch wird sichergestellt, dass die Werte aus dem Quellenbericht an die richtigen Parameterwerte übergeben werden und dass der Zielbericht korrekt gefiltert wird. Wenn Sie keine Parameter zuordnen, werden die Benutzer möglicherweise zur Eingabe von Werten aufgefordert, wenn der Zielbericht ausgeführt wird.

Ein berichtspfadbasierter Drillthrough-Pfad verweist auf einen Pfad, der in einem Quellenbericht erstellt und gespeichert wird. Diese Art des Drillthrough-Pfads wird auch als autorisierte Drillthrough-Funktion bezeichnet. Der Pfad wird einer bestimmten Datenspalte, einem bestimmten Diagramm oder einer bestimmten Kreuztabelle im Quellenbericht zugeordnet und ist nur verfügbar, wenn Benutzer den betreffenden Bereich des Berichts auswählen. Wenn eine autorisierte Drillthrough-Definition verfügbar ist, wird ein Hyperlink in dem Quellenbericht angezeigt, wenn er ausgeführt wird.

Der Bericht-basierte Drillthrough ist auf Berichtsquellenberichte und alle Zielberichte beschränkt. Verwenden Sie diesen Drillthrough-Typ, wenn Sie Datenelementwerte oder -parameter aus einem Quellenbericht an den Zielbericht übergeben möchten, die Ergebnisse eines Berichtsausdrucks an einen Zielbericht übergeben oder einen URL-Link als Teil der Drillthrough-Definition verwenden möchten.

Auswahlkontexte

Der Auswahlkontext stellt die Struktur der Werte dar, die vom Benutzer in der Quelle ausgewählt wurden.

In IBM Cognos Analysis Studio umfasst dies den Kontextbereich. Wenn eine Drillthrough-Definition für Pakete verwendet wird, wird der Auswahlkontext verwendet, um Werte für zugeordnete Parameter (parametrisierter Drillthrough) anzugeben oder auch die entsprechenden Datenelemente und Werte zuzuordnen.

Drillthrough-Links können auch definiert werden, um das Zielobjekt bei einem Lesezeichen zu öffnen. Der Inhalt dieses Lesezeichens kann auch durch den Auswahlkontext angegeben werden.

Ein Drillthrough-Zugriff ist zwischen den meisten Kombinationen aus den IBM Cognos Analytics -Studios möglich. Jedes Studio ist optimiert für die Ziele und Fähigkeiten des Publikums, das es nutzt, und in einigen Fällen für den Typ der Datenquelle, für die es entworfen wurde. Daher müssen Sie möglicherweise überlegen, wie die verschiedenen Studios den Auswahlkontext verwalten, wenn Sie einen Drillthrough

zwischen Objekten durchführen, die in verschiedenen Studios erstellt wurden, und wie die Datenquellen zusammengebildet werden. Während des Tests oder Debuggings können Sie sehen, wie Quellenwerte in verschiedenen Kontexten mithilfe des Drillthrough-Assistenten zugeordnet werden.

Drillthrough zu verschiedenen Berichtsformaten

Die Einstellungen in der Drillthrough-Definition bestimmen das Format, in dem die Benutzer die Berichtsergebnisse sehen.

For example, the users may see the reports in IBM Cognos Viewer as an HTML Web page, or the reports may open in IBM Cognos Query Studio, IBM Cognos PowerPlay Studio, or IBM Cognos Analysis Studio. Wenn Ihre Benutzer PowerPlay Studio haben, können sie auch die Standardansicht eines PowerCubes anzeigen.

Berichte können als HTML-Seiten oder als PDF-, XML-, CSV-oder Microsoft Excel-Tabellenkalkulationssoftware-Formate geöffnet werden. Wenn Sie einen Drillthrough-Pfad definieren, können Sie das Ausgabeformat auswählen. Dies kann nützlich sein, wenn die erwartete Verwendung des Zielberichts etwas anderes ist als das Onlineanzeigen. Wenn der Bericht gedruckt wird, wird er als PDF ausgegeben; wenn er für die weitere Verarbeitung in Excel exportiert wird, wird er als Excel-oder CSV-Ausgabe ausgegeben usw.

Zum Ausführen von Berichten oder zum Drillup von Zielen, die Berichte im CSV-, PDF-, Microsoft Excel-Tabellenkalkulationsprogramm (XLS) oder in XML-Ausgabeformaten ausführen, benötigen Benutzer die Funktion zur Generierung von Ausgabefunktionen für das bestimmte Format.

Anmerkung: Der PDF-Drillthrough wird nur in Internet Explorer mit dem Adobe PDF-Plug-in unterstützt.

Wenn Sie einen Drillthrough-Pfad zu einem Bericht definieren, der in Analysis Studio, PowerPlay Studio oder Query Studio erstellt wird, können die Konsumenten den Bericht in seinem Studio anstatt in IBM Cognos Viewer öffnen. Dies kann nützlich sein, wenn Sie erwarten, dass ein Konsument den Drillthrough-Zielbericht als Beginn einer Analyse-oder Abfragesitzung verwendet, um weitere Informationen zu finden.

Wenn eine Anwendung beispielsweise einen Dashboard-Style-Bericht mit hochrangigen Daten enthält, können Sie einen Drillthrough-Link zu Analysis Studio definieren, um die interessierenden Elemente zu untersuchen. Die Analyse-Studio-Ansicht kann anschließend in einen PDF-Bericht für den Druck durchgebohrt werden.

Anmerkung: IBM Cognos Analytics - Reporting zeigt keine Datenergebnisse an.

Zugehörige Konzepte

Berichtsformate

Bohren zwischen Paketen

Sie können einen Drillthrough-Zugriff zwischen den Paketen einrichten.

Die beiden Pakete können auf unterschiedlichen Typen von Datenquellen basieren, aber es gibt einige Einschränkungen. In der folgenden Tabelle sind die Datenquellenzuordnungen aufgeführt, die den Drillthrough-Zugriff unterstützen.

Tabelle 78. Datenquellenzuordnungen, die den Drillthrough-Zugriff unterstützen

Quellendatenquelle	**Zieldatenquelle**
OLAP	OLAP **Hinweis:** OLAP zu OLAP-Drillthrough wird nur unterstützt, wenn der Datenquellentyp identisch ist, z. B. SSAS zu SSAS.
OLAP	Dimensional modellierte relationale Daten

Tabelle 78. Datenquellenzuordnungen, die den Drillthrough-Zugriff unterstützen (Forts.)	
Quellendatenquelle	**Zieldatenquelle**
OLAP	Relationale Daten **Hinweis:** Weitere Informationen finden Sie im Artikel „Geschäftsschlüssel" auf Seite 392.
Dimensional modellierte relationale Daten	Dimensional modellierte relationale Daten
Dimensional modellierte relationale Daten	Relationale Daten
Relationale Daten	Relationale Daten

Lesezeichen für Lesezeichen

Wenn Sie einen Drillthrough durchführen, werden die Werte, die Sie übergeben, in der Regel, aber nicht immer, zum Filtern des Berichts verwendet.

IBM Cognos Analytics unterstützt Lesezeichen in gespeicherten PDF-und HTML-Berichten, sodass ein Benutzer einen Bericht scrollen kann, um das relevante Teil auf der Basis eines URL-Parameters anzuzeigen.

Beispiel: Sie verfügen über einen umfangreichen Bestandsbericht, der aufgrund von Ressourcenüberlegungen täglich oder wöchentlich während der Dauer ausgeführt werden soll. Möglicherweise möchten Ihre Benutzer diesen Bericht als Ziel anzeigen, da er detaillierte Informationen enthält. Sie möchten jedoch, dass die Benutzer die gespeicherte Ausgabe anzeigen, anstatt diesen großen Bericht auszuführen. Mit dieser Aktionsoption und den Einstellungen für Lesezeichen können Benutzer von einer anderen Quellenposition ausgehend von Produkten Drillthrough durchführen, um den gespeicherten Bericht auf der Seite zu öffnen, auf der das Produkt angezeigt wird, auf das sie sich konzentrieren möchten.

Wenn ein Lesezeichen im Quellenbericht in einer Drillthrough-Definition verwendet wird, stellt es den Wert für den URL-Parameter bereit. Wenn Sie mithilfe dieser Definition einen Drillthrough-Bericht für Konsumenten erstellen, sehen sie den entsprechenden Abschnitt des Zielberichts.

Anmerkung: PDF-Drillthrough wird nur in Internet Explorer mit dem Adobe PDF-Plug-in unterstützt.

Lesezeichenverweise sind auf zuvor ausgeführten Berichte beschränkt, die als PDF oder HTML ausgegeben werden und Lesezeichenobjekte enthalten.

Mitglieder und Werte

Dimensional modellierte Daten, ob in Cubes gespeichert oder als dimensional modellierte relationale Daten (DMR) gespeichert, werden Daten in Dimensionen organisiert. Diese Dimensionen enthalten Hierarchien. Die Hierarchien enthalten Ebenen. Und die Ebenen enthalten Mitglieder.

Ein Beispiel für eine Dimension ist "Standorte". Eine Dimension "Orte" kann zwei Hierarchien enthalten: Standorte nach Organisationsstruktur und Standorte nach Geographie. Jede dieser Hierarchien kann Ebenen wie Land oder Region und Stadt enthalten.

Mitglieder sind die Instanzen in einer Ebene. Zum Beispiel sind New York und London Mitglieder in der City-Ebene. Ein Mitglied kann mehrere Eigenschaften haben, z. B. "Population", "Latitude" und "Longitude". Intern wird ein Member durch einen Member Unique Name (MUN) identifiziert. Die Methode, mit der ein MUN abgeleitet wird, hängt von dem Cube-Anbieter ab.

Relationale Datenmodelle bestehen aus Datensubjekten, wie z. B. Mitarbeitern, die aus Datenelementen wie Name oder Erweiterung bestehen. Diese Datenelemente haben Werte, z. B. Peter Schmidt.

In IBM Cognos Analyticssind die Methoden für das Durchbohren verfügbar.

· Dimensional (Mitglied) zu Dimensional (Mitglied)

· Dimensionales (Mitglied) zu relationalem Element (Datenelementwert)

· Relationaler (Datenelementwert) für relationale Daten (Datenelementwert)

Wenn der Zielparameter ein Member ist, muss die Quelle ein Member sein. Die Quelle und das Ziel sollten in der Regel aus einer konformierten Dimension stammen. Wenn die Daten diese Unterstützung unterstützen, können Sie jedoch auch eine Zuordnung mit unterschiedlichen Eigenschaften des Quellenmetadatenelements definieren.

Wenn der Zielparameter ein Wert ist, kann es sich bei der Quelle um einen Wert oder um ein Member handeln. Wenn es sich bei der Quelle um ein Dimensionselement handelt, müssen Sie sicherstellen, dass die Ebene oder Dimension dem Zieldatenelement in der Drillthrough-Definition korrekt zugeordnet ist. Der Geschäftsschlüssel, aus dem das Member stammt, sollte in der Regel mit dem relationalen Zielwert übereinstimmen, der am häufigsten der Geschäftsschlüssel ist. Wenn die Daten diese Unterstützung unterstützen, können Sie jedoch auch eine Zuordnung aus der Beschriftung des Quellenmetadatenelements definieren.

Konformierte Dimensionen

Wenn Sie mit mehr als einer dimensionalen Datenquelle arbeiten, können Sie feststellen, dass einige Dimensionen gleich strukturiert sind, und einige sind es nicht.

Der Grund dafür, dass Dimensionen unterschiedlich strukturiert werden können, ist, dass die Datenquellen verschiedenen Zwecken dienen können.

Beispiel: Eine Kundendimension wird in einem Umsatzdatenspeicher angezeigt, jedoch nicht in einem Bestandsdatenspeicher. Die Dimension "Products" und die Dimension "Time" werden jedoch in beiden Datenspeichern angezeigt.

Dimensionen, die in mehreren Datenspeichern angezeigt werden, werden konformiert, wenn ihre Struktur für alle der folgenden Elemente identisch ist:

· Hierarchie-

· Ebenennamen

· Rangordnung

· Interne Schlüssel

Das Durchbohren ist zwischen verschiedenen Dimensionsdatenspeichern nur möglich, wenn die Dimensionen übereinstimmen, und wenn der Dimensionsdatenspeicher denselben Anbietertyp hat, wie z. B. IBM Cognos PowerCube als Quelle und Ziel. Beispiel: In zwei Datenspeichern für Umsatz und Lager, die Produkte und Zeitdimensionen enthalten, ist es möglich, die Dimensionen 'Produkte' und 'Zeit' für jeden Datenspeicher unterschiedlich zu definieren. Bei der Ausführung von Drillthrough zwischen den Dimensionen 'Products' und 'Time' müssen die Strukturen jedoch in jedem Datenspeicher identisch sein.

Wenn Sie sich nicht sicher sind, ob Ihre Dimensionen definiert sind, sollten Sie mit dem Datenmodellierer überprüfen, ob die Bohrung aussagekräftige Ergebnisse liefern wird.

IBM Cognos Analytics unterstützt keine konformen Dimensionen, die von IBM Cognos Framework Manager für SAP BW-Datenquellen generiert werden.

Dimensionally modeled Relational Data Sources

Stellen Sie sicher, dass jede Ebene einen Geschäftsschlüssel enthält, der Werte enthält, die mit Ihrem PowerCube oder anderen DMR-Modellen übereinstimmen. Außerdem müssen Sie sicherstellen, dass die Eigenschaft **Stammgeschäftschlüssel** definiert ist und den Geschäftsschlüssel der ersten Ebene in der Hierarchie verwendet. Auf diese Weise können Sie sicherstellen, dass Sie einen eindeutigen Namen für die Teildatei haben, wenn Sie versuchen, mithilfe von Membern aus dieser Dimension einen Drillthrough durchzuführen.

Geschäftsschlüssel

Wenn ein Drillthrough-Zugriff von einem Member auf einen relationalen Wert definiert ist, wird der Geschäftsschlüssel des Members standardmäßig übergeben.

Dies bedeutet, dass Ihr relationaler Zielparameter mithilfe des Datenelements mit einem übereinstimmenden Wert eingerichtet werden muss, bei dem es sich am häufigsten um das Geschäftsschlüsseldatenelement handelt. Sie können auch auswählen, dass die Beschriftung des Quellenmetadatenelements übergeben wird.

Mitarbeiter werden beispielsweise in der Regel durch eine Mitarbeiterzahl eindeutig identifiziert, nicht durch ihren Namen, weil ihr Name nicht unbedingt eindeutig ist. Wenn Sie einen Drillthrough von einem dimensionalen Member zu einem relationalen Datenelement durchführen, ist der angegebene Wert der Geschäftsschlüssel. Daher muss der Parameter im Zielbericht so definiert werden, dass er einen Geschäftsschlüsselwert akzeptiert. Die genaue Logik, die zum Definieren des angegebenen Geschäftsschlüsselwerts verwendet wird, hängt vom Cube-Anbieter ab. Für IBM Cognos PowerCubes ist der Geschäftsschlüsselwert die **Quelle** -Eigenschaft, die für die Ebene in IBM Cognos Transformer definiert ist. IBM Cognos Series 7 Transformer PowerCubes übergeben den Quellenwert, wenn das Drillthrough-Flag aktiviert wurde, bevor der Cube erstellt wurde. Andernfalls wird der Kategoriecode verwendet.

In IBM Cognos Analytics - Reportingkönnen Sie bestimmen, was der Membergeschäftsschlüssel mit einem Ausdruck wie `roleValue ('_businessKey', [Campingausrüstung])`verwendet. Bei diesem Ausdruck muss die Groß-/Kleinschreibung beachtet werden.

SSAS 2005 mehrteilige Geschäftsschlüssel werden in Drillthrough-Operationen nicht unterstützt.

Tipp: Wenn andere Benutzer Ihren Drillthrough-Bericht ausführen, möchten Sie möglicherweise nicht, dass sie zur Eingabe eines Geschäftsschlüssels aufgefordert werden. In Reportingkönnen Sie eine Eingabeaufforderungsseite mit einem Text erstellen, der den Benutzern vertraut ist, aber auf den Geschäftsschlüssel filtert. Ihr IBM Cognos Framework Manager-Modellierer kann auch die Option **Artikelverweis anzeigen** für die Eigenschaft **Informationen zur Eingabeaufforderung** festlegen, um den Geschäftsschlüssel zu verwenden, wenn das Datenelement in einer Eingabeaufforderung verwendet wird.

Geltungsbereich

Der Geltungsbereich ist für Drillthrough-Definitionen spezifisch, die mithilfe von Drillthrough-Definitionen erstellt wurden (Paketdrillthrough-Definitionen). Der Bereich, den Sie festlegen, definiert, wann der Zielbericht den Benutzern angezeigt wird, basierend auf den Elementen, die sie im Quellenbericht haben.

In der Regel definieren Sie den Bereich eines Drillthrough-Pfads, der mit einem Parameter übereinstimmt, den er übergibt. Wenn beispielsweise ein Zielbericht eine Liste von Mitarbeitern enthält, wird der Bericht in der Regel nur dann als verfügbare Drillthrough-Auswahl angezeigt, wenn ein Benutzer Mitarbeiternamen in einem Quellenbericht anzeigt. Wenn sich Mitarbeiternamen nicht im Quellenbericht befinden und der Geltungsbereich in der Drillthrough-Definition auf den Mitarbeiternamen gesetzt wurde, wird der Mitarbeiterbericht nicht in der Liste der verfügbaren Drillthrough-Zielberichte auf der **Gehe zu** -Seite angezeigt. Sie können den Geltungsbereich auf eine Kennzahl oder auf einen Artikel in dem Bericht festlegen.

Bei einem berichtsbasierten Drillthrough-Zugriff, bei dem der Drillthrough-Pfad einer bestimmten Berichtsspalte zugeordnet ist, dient die Spalte als Geltungsbereich.

Zugeordnete Parameter

Drillthrough-Ziele können vorhandene Parameter enthalten, oder Sie können Parameter zum Ziel hinzufügen, um die Steuerung über den Drillthrough-Link zu erweitern.

In der Regel ordnen Sie alle Parameter in einem Drillthrough-Ziel den Elementen aus der Quelle zu.

Wenn Sie Quellenelemente, die OLAP-oder DMR-Member sind, auf Zielparameter zuordnen, können Sie aus einer Gruppe zusammengehöriger Mitgliedseigenschaften auswählen, um die Anforderungen des Zielparameters zu erfüllen. Bei einem dimensionalen Ziel verwendet ein dimensionales Quellenelement

standardmäßig den eindeutigen Membernamen. Für ein relationales Ziel verwendet ein dimensionales Quellenelement standardmäßig den Geschäftsschlüssel.

Sie könnten beispielsweise die Eigenschaft des Quellenelements, die für eine Zuordnung verwendet wird, an die Mitgliedskaption anstelle des Geschäftsschlüssels ändern, um mit dem Parameter in einem relationalen Ziel übereinstimmen zu können. Für ein dimensionales Ziel können Sie einen Parameter definieren, der eine bestimmte Eigenschaft akzeptiert (z. B. Geschäftsschlüssel oder eindeutiger Name des übergeordneten Elements), und dann die entsprechende Quelleneigenschaft übergeben, um dieses Ziel zu erfüllen.

Anmerkung: Wenn Sie einen Drillthrough zwischen nicht konformierten Dimensionen definieren, sollten Sie sorgfältig prüfen, ob die Ergebnisse wie erwartet verhalten werden.

Wenn Sie keine Parameterzuordnungen angeben, werden Sie standardmäßig zur Eingabe von Parametern aufgefordert, die für das Ziel erforderlich sind, wenn Sie den Drillthrough-Link verwenden. Um dieses Verhalten anzupassen, verwenden Sie die Einstellung "Eingabeaufforderungsseiten anzeigen".

Wenn die Aktion auf **Führen Sie den Bericht mit dynamischer Filterung aus.**gesetzt ist, wird die zusätzliche Filterung angewendet, wenn Namen aus dem Kontext im Quellenbericht mit den Namen von Elementen im Ziel übereinstimmen. Verwenden Sie diese Aktion auch, wenn im Ziel keine Parameter definiert sind.

Wenn Parameter nicht korrekt zugeordnet werden, erhalten Sie möglicherweise einen leeren Bericht, die falschen Ergebnisse oder eine Fehlernachricht.

Die Quelle und das Ziel können keine identischen Parameternamen enthalten, wenn sie aus verschiedenen Paketen stammen, selbst wenn die Datenstruktur gebildet wird. Wenn die Quelle und das Ziel aus dem gleichen Paket stammen, gibt es keine Einschränkung.

Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie den Drillthrough-Assistenten verwenden, um zu prüfen, welche Quellenparameter übergeben werden und welche Zielparameter für einen gegebenen Drillthrough-Link zugeordnet werden.

Sie können das Verhalten des dynamischen Drillthrough-Filters ändern, wenn Sie einen Drillthrough durchführen möchten, um einen Filter mit dem Member Business Key anstelle der Standardmitgliedskaption zu generieren. Weitere Informationen finden Sie im Abschnitt Drill-Through-Filter-Verhalten in der *IBM Cognos Administration and Security Guide*.

Drillthrough für Daten zwischen PowerCubes und relationalen Paketen

Die übliche Methode zum Durchbohren von OLAP-zu relationalen Paketen erfordert, dass der Parameter für den Zielbericht mit dem Geschäftsschlüssel in den relationalen Daten festgelegt wird, was für Datumsangaben nicht gut funktioniert.

OLAP-Datenquellen betrachten Daten in der Regel als Mitglieder, wie z. B. Quartal 1 2012, während relationale Datenquellen Datumsangaben als Bereiche anzeigen, z. B. 1/Jan/2012 bis 31 /March/2012.

Eine spezielle Funktion besteht zum Durchbohren zwischen PowerCubes und relationalen Paketen. Stellen Sie sicher, dass der Parameter für den Zielberichtsparameter mit `in_Bereich`konfiguriert ist. Der Parameter muss vom Typ "date-time" und nicht "integer" sein.

Es folgt ein Beispiel:

```
[gosales_goretailers].[Orders].[Order date] in_range ?Date?
```

Stellen Sie außerdem sicher, dass die Drillthrough-Definition den Parameter auf der Dimensionsebene zuordnet und dass die Datumsebene des PowerCube nicht zum Unterdrücken von leeren Kategorien festgelegt ist. Wenn Sie die Option aktivieren, um leere Kategorien im Transformer-Modell zu unterdrücken, bevor Sie den Cube erstellen, kann die Drillthrough-Operation für Datumsangaben nicht erfolgreich sein. Dies liegt daran, dass im Bereich fehlende Werte vorhanden sind.

Drillthrough-Zugriff in Paketen einrichten

Eine Drillthrough-Definition gibt ein Ziel für den Drillthrough-Zugriff, die Bedingungen, unter denen das Ziel verfügbar ist (wie z. B. den Geltungsbereich), und das Ausführen oder Öffnen und das Filtern des Ziels.

In IBM Cognos Analytics ist eine Drillthrough-Definition einem Quellenpaket zugeordnet. Der Drillthrough-Pfad, der in der Drillthrough-Definition definiert ist, ist für jeden Bericht verfügbar, der auf dem Quellenpaket basiert, dem es zugeordnet ist. Das Ziel kann auf einem beliebigen Zielpaket basieren und überall gespeichert werden. Beispielsweise können alle Berichte, die im Beispielpaket GO Data Warehouse (analysis) oder in einem mit diesem Paket verknüpften Ordner erstellt wurden, auf jede Drillthrough-Definition zugreifen, die in diesem Paket erstellt wurde.

Anmerkung: Sie können Drillthrough-Zugriff in bestimmten Berichten definieren, indem Sie die Drillthrough-Definition in dem Bericht anstatt im Paket einrichten oder den Drillthrough-Zugriff durch Ändern von Berichtseinstellungen beschränken, sodass der Bericht als Drillthrough-Ziel nicht verfügbar ist.

Sie können Drillthrough-Definitionen zwischen Berichten definieren, die in den verschiedenen Studios erstellt wurden, und Berichte, die auf verschiedenen Paketen und Datenquellen basieren.

Der Zielbericht muss vorhanden sein, bevor Sie mit der Erstellung der Drillthrough-Definition beginnen. Drillthrough-Ziele können Berichte, Analysen, Berichtsansichten, PowerCube-Pakete und Abfragen sein.

Drillthrough-Definitionen unterstützen sowohl dimensionale als auch relationale Pakete.

Vorbereitende Schritte

Zum Ausführen von Berichten oder zum Ausführen von Drills für Ziele, die Berichte im CSV-, PDF-, Microsoft Excel-Tabellenkalkulationsprogramm (XLS) oder in XML-Ausgabeformaten ausführen, ist die Generierung der Ausgabefunktion für das bestimmte Format erforderlich.

Vorgehensweise

1. Überprüfen Sie das Drillthrough-Ziel:
   - Bestätigen Sie, dass die Drillthrough-Benutzer Zugriff auf das Ziel haben.
   - Verdecken Sie das Ziel vor dem direkten Zugriff, wenn Sie möchten.
   - Falls erforderlich, prüfen Sie, welche Parameter im Ziel vorhanden sind.

     Wenn eine Drillthrough-Definition Objekte in verschiedenen Paketen verknüpft, müssen Sie die Datentypen berücksichtigen, die sowohl in der Quelle als auch in dem Zielobjekt verwendet werden. Überprüfen Sie die Struktur und die Werte der Daten, die Sie im Drillthrough übergeben möchten, und stellen Sie sicher, dass die erstellten Parameter für Ihr Szenario geeignet sind, wenn Sie Parameter definiert haben oder dass eine dynamische Drillthrough-Funktion erfolgreich ausgeführt werden kann.
2. Starten Sie **Drillthrough-Definitionen**.
3. Navigieren Sie zu dem Paket, für das Sie die Drillthrough-Definition erstellen möchten.
4. Klicken Sie in der Symbolleiste auf das Symbol **Neue Drillthrough-Definition** .

   Tipp: Wenn das Symbol **Neue Drillthrough-Definition** nicht angezeigt wird, bestätigen Sie, dass Sie sich auf der Paketebene befinden und nicht in einem Ordner in dem Paket. Drillthrough-Definitionen müssen auf der Paketebene gespeichert werden.
5. Geben Sie einen Namen für die Drillthrough-Definition ein.
6. Wenn Sie möchten, geben Sie eine Beschreibung und eine Anzeigenspitze ein, und klicken Sie dann auf **Weiter**.
7. Befolgen Sie die Anweisungen auf dem Bildschirm:
   - Wenn Sie möchten, schränken Sie den Geltungsbereich auf ein Abfrageelement oder eine Kennzahl in der Quelle ein.

Wenn das Ziel Parameter enthält, sollten Sie den Geltungsbereich auf die Parameter festlegen, die dem Zielbericht zugeordnet sind.

- Wählen Sie das Ziel aus jedem Paket aus.

  Wenn PowerPlay -Ziele verfügbar sind, müssen Sie auswählen, ob das Ziel als Bericht oder als PowerCube festgelegt werden soll.

- Klicken Sie auf **Weiter**.

8. Geben Sie im Abschnitt **Aktion** an, wie das Zielobjekt geöffnet werden soll, wenn der Drillthrough-Link ausgeführt wird. Wenn Sie den Bericht ausführen wollen, geben Sie im Abschnitt **Format** das Format an, in dem der Bericht ausgeführt werden soll.

   Anmerkung: Benutzer können die Einstellungen für **Aktion** möglicherweise ändern, wenn sie den Drillthrough-Link verwenden. Wenn Sie Lesezeichen im Ziel verwenden, müssen Sie die Aktion **Letzten Bericht anzeigen**auswählen.

9. Geben Sie in der Tabelle **Parameterwerte** an, wie die Quellenmetadaten allen Parametern zugeordnet werden sollen, die im Zielbericht oder in dem Zielobjekt vorhanden sind.

   Wenn Sie z. B. Drillthrough zwischen OLAP-Datenquellen durchführen, werden die Member einander zugeordnet. Wenn Sie einen Drillthrough von einer OLAP-zu einer relationalen Datenquelle durchführen, wird der Quellenwert (Member) dem Abfrageelementnamen (Wert) zugeordnet.

   Normalerweise sollte jeder Parameter, der in dem Ziel vorhanden ist, den Quellenmetadaten zugeordnet werden. Ist dies nicht der Fall, kann der Berichtsbenutzer bei der Verwendung der Drillthrough-Verknüpfung für fehlende Werte aufgefordert werden.

10. Klicken Sie auf **Metadaten zuordnen**, oder klicken Sie auf die Bearbeitungsschaltfläche  .

    - Wählen Sie in der Anzeige, die angezeigt wird, die Metadaten aus der Quelle aus, die dem Zielparameter zugeordnet werden sollen.
    - Wenn das Quellenpaket dimensionell ist, können Sie auswählen, welche Eigenschaft des Quellenmetadatenelements in der Zuordnung verwendet werden soll. Standardmäßig wird der Geschäftsschlüssel für ein relationales Ziel verwendet, und der eindeutige Membername wird für ein dimensionales Ziel verwendet.
    - Wiederholen Sie den Vorgang für jeden Parameter in der Liste.

11. Geben Sie im Abschnitt **Eingabeaufforderungsseiten anzeigen** an, wann die Eingabeaufforderungsseiten angezeigt werden sollen.

    - Wählen Sie in der Anzeige, die angezeigt wird, die Metadaten aus der Quelle aus, die dem Zielparameter zugeordnet werden sollen.
    - Wenn das Quellenpaket dimensionell ist, können Sie auswählen, welche Eigenschaft des Quellenmetadatenelements in der Zuordnung verwendet werden soll. Standardmäßig wird der Geschäftsschlüssel für ein relationales Ziel verwendet, und der eindeutige Membername wird für ein dimensionales Ziel verwendet.
    - Wiederholen Sie den Vorgang für jeden Parameter in der Liste.

    Sie können diese Aktion nur festlegen, wenn Parameter im Zielbericht vorhanden sind und der Zielbericht ausgeführt wird. Wenn Sie die Aktion in **Letzten Bericht anzeigen**ändern, z. B. für Lesezeichenverweise, ist die Eigenschaft **Eingabeaufforderungsseiten anzeigen** inaktiviert, da Sie einen zuvor ausgeführten Bericht verwenden. Wenn Sie den Bericht direkt in Analysis Studio öffnen, ist die Eigenschaft **Eingabeaufforderungsseiten anzeigen** ebenfalls inaktiviert.

    Sie geben Eingabeaufforderungseinstellungen in **Berichtseigenschaften**, **Eingabeaufforderung für Werte**an.

12. Klicken Sie auf **Fertigstellen**.
13. Führen Sie einen Bericht aus dem Quellenpaket aus, und testen Sie den Drillthrough-Link.

    Anmerkung: Die Drillthrough-Definition wird mit der Quelle verknüpft und gespeichert. Fehler, die sich auf das Ziel beziehen, werden nur generiert, wenn Sie die Drillthrough-Links ausführen, und nicht, wenn Sie die Drillthrough-Definition speichern.

Zugehörige Konzepte
Berichtsformate

Vorhandene Drillthrough-Definitionen bearbeiten

Sie können vorhandene Drillthrough-Definitionen bearbeiten.

Vorgehensweise

1. Klicken Sie auf der Begrüßungsseite von IBM Cognos Analytics auf **Neu** > **Sonstige** > **Drillthrough-Definitionen**.
2. Klicken Sie auf einen Paketnamen, um seine Drillthrough-Definitionen anzuzeigen.
3. Klicken Sie für die Drillthrough-Definition, die Sie ändern möchten, in der Spalte **Aktionen** auf das Symbol **Eigenschaften festlegen**  .

   Tipp: Wenn Sie die Drillthrough-Definitionen nicht sehen, überprüfen Sie, ob Sie sich nicht in einem Ordner im Paket befinden. Drillthrough-Definitionen werden alle auf der Stammebene des Pakets gespeichert. Wenn eine bestimmte Drillthrough-Definition nicht angezeigt wird, bestätigen Sie, dass Sie über die korrekten Berechtigungen verfügen.
4. Klicken Sie auf die Registerkarte **Ziel** .
5. Nehmen Sie die erforderlichen Änderungen vor, und klicken Sie auf **OK**.
6. Führen Sie einen Bericht aus dem Quellenpaket aus, und testen Sie den Drillthrough-Link.

   Anmerkung: Die Drillthrough-Definition wird mit der Quelle verknüpft und gespeichert. Fehler, die sich auf das Ziel beziehen, werden nur generiert, wenn Sie die Drillthrough-Links ausführen, und nicht, wenn Sie die Drillthrough-Definition speichern.

Einrichten von Parametern für einen Drillthrough-Bericht

Für eine größere Kontrolle über den Drillthrough-Zugriff können Sie Parameter im Zielbericht definieren.

Parameter für einen Drillthrough-Bericht konfigurieren

Für eine größere Kontrolle über den Drillthrough-Zugriff können Sie Parameter im Zielbericht definieren.

Vorgehensweise

1. Öffnen Sie den Zielbericht.
2. Stellen Sie sicher, dass der Bericht für einen Drillthrough-Zugriff verfügbar ist:
   - Wählen Sie im Menü **Daten** die Option **Drillverhalten**aus.
   - Wählen Sie auf der Registerkarte **Basis** die Option **Dynamische Filter akzeptieren, wenn es sich bei diesem Bericht um ein Drillthrough-Ziel handelt** aus, und klicken Sie anschließend auf OK.
3. Erstellen Sie einen Parameter, der als Drillthrough-Spalte verwendet wird, oder der zum Filtern des Berichts verwendet wird. (**Daten** -Menü, **Filter**).

   Beispiel: Zum Durchbohren oder Filtern von Produktlinien erstellen Sie einen Parameter, der wie folgt aussieht:

   ```
   [Produktreihe] = ?prodline_p?
   ```

   Tipp: Verwenden Sie die Operatoren `In` oder `in_Bereich` , wenn Sie möchten, dass der Zielbericht mehrere Werte oder einen Wertebereich akzeptiert.
4. Geben Sie im Feld **Verwendung** an, welche Schritte ausgeführt werden sollen, wenn ein Wert für den Zielparameter nicht als Teil eines Drillthrough-Werts übergeben wird:
   - Wenn Sie angeben möchten, dass Benutzer im Quellenbericht auf einen Wert klicken müssen, klicken Sie auf **Erforderlich**.

Wenn kein Wert für den Zielparameter übergeben wird, werden die Benutzer aufgefordert, einen Wert auszuwählen.

- Wenn Sie angeben möchten, dass Benutzer im Quellenbericht nicht auf einen Wert klicken müssen, klicken Sie auf **Optional**.

  Benutzer werden nicht aufgefordert, einen Wert auszuwählen, und daher wird der Wert nicht gefiltert.

- Um anzugeben, dass der Parameter nicht verwendet werden soll, klicken Sie auf **Inaktiviert**.

  Der Parameter wird im Bericht nicht verwendet und ist daher für Drillthrough-Definitionen nicht verfügbar. Weitere Informationen zum Definieren von Berichtsparametern finden Sie im Reporting *Benutzerhandbuch*.

  Tipp: Wenn der Parameter aus anderen Gründen in dem Bericht benötigt wird, können Sie auch angeben, dass er nicht in der Drillthrough-Definition verwendet werden soll (**Parameter** -Tabelle, **Methode**, **Parameter nicht verwenden**).

Ergebnisse

Die Drillthrough-Definition steuert, wann Eingabeaufforderungsseiten oder -parameter angezeigt werden.

Definieren von Parametern für einen Drillthrough-Bericht in Query Studio

Für eine größere Kontrolle über den Drillthrough-Zugriff können Sie Parameter im Zielbericht in Query Studio definieren.

Vorgehensweise

1. Öffnen Sie den Zielbericht in Query Studio.
2. Bestätigen Sie, dass der Bericht für Drillthrough-Zugriff verfügbar ist:
   - Wählen Sie im Menü **Bericht ausführen**, **Erweiterte Optionen**aus.
   - Wählen Sie **Drillthrough von einem Paket in der Berichtsausgabe aktivieren** aus, und klicken Sie auf OK.
3. Erstellen Sie einen Filter, der als Drillthrough-Parameter verwendet wird oder der zum Filtern des Berichts verwendet werden soll.
   - Wählen Sie die Spalte aus, nach der gefiltert werden soll, und klicken Sie auf die Filterschaltfläche.
   - Ändern Sie die Einstellungen nach Bedarf, und klicken Sie auf OK.

Legen Sie Parameter für ein Drillthrough-Ziel in Analysis Studio fest

Sie können eine Drillthrough-Zielanalyse erstellen und Zielparameter in der Analyse hinzufügen, indem Sie eine Dimension als "Gehe zu" -Parameter festlegen.

Wenn Sie eine Drillthrough-Definition für die Analyse erstellen, wird dieser Parameter in der Zielparameterliste angezeigt.

Um das Bohren in der Dimension zu unterstützen und anschließend durchzubohren, ordnen Sie die Dimension in den Quellenmetadaten der Zieldimension zu. Die Mitglieder oder Mitglieder, die sich derzeit in Ihrer Ansicht befinden, werden als Filterwerte an die Zielanalyse übergeben. Dies gilt für alle Abfragen, Berichte oder Analysen, die in Drillthrough-Aktionen verwendet werden. Wenn Sie das Bohren direkt von einer bestimmten Ebene aus unterstützen möchten, ordnen Sie diese Ebene in den Quellenmetadaten der Zieldimension zu.

Sie können mehrere Parameter in einem Analyseziel festlegen. Die Mitglieder können jedoch nicht innerhalb einer Auswahlgruppe in Analysis Studio übergeben werden.

Vorgehensweise

1. Erstellen Sie in Analysis Studio mithilfe des Pakets, das für die Drillthrough-Analyse eingerichtet wurde, eine Kreuzladungsanalyse.
2. Wenn Sie möchten, fügen Sie als Zeile oder Spalte das Datenelement hinzu, das Sie als Eingabeaufforderung verwenden möchten.
3. Verschieben oder fügen Sie die Dimension oder Ebene, die als Zielparameter verwendet werden soll, in den Bereich **Kontext** ein.

   Anmerkung: Mitglieder können nicht innerhalb einer Auswahlgruppe in Analysis Studio übergeben werden.
4. Zeigen Sie die Liste für das Element im Bereich **Kontext** an, und klicken Sie auf **Als "Wechseln zu" -Parameter verwenden**.
5. Speichern Sie diese Analyse als Zielbericht.

   Sie können nun die Drillthrough-Definition unter einem Quellenpaket erstellen.

Ergebnisse

Wenn Sie die Drillthrough-Definition erstellen und die Kreuzladenanalyse als Ziel verwenden, wird das **Gehe zu** -Parameterelement in der Analyse als Drillthrough-Parameter angezeigt.

Debug für eine Drillthrough-Definition durchführen

IBM Cognos Analytics enthält eine Debugging-Funktionalität, die Sie verwenden können, um Probleme mit Ihren Drillthrough-Definitionen zu finden und Drillthrough-Fehler zu korrigieren.

Sie können auch helfen, zu verstehen, wie die Drillthrough-Funktionalität funktioniert, insbesondere über verschiedene Arten von Datenquellen. Diese Funktionalität wird auch als Drillthrough-Assistent bezeichnet. Sie können auch Drillthrough-Definitionen debuggen, die in einem PowerCube erstellt und in IBM Cognos Analytics migriert wurden.

Wenn Ihr Zielbericht keine Parameter empfängt, überprüfen Sie die Zuordnung in Ihrer Drillthrough-Definition, und stellen Sie sicher, dass Ihre Parameter für Ihren Drillthrough-Szenario mit dem richtigen Datentyp erstellt wurden. Wenn Sie beispielsweise eine Drillthrough-Definition aus einem OLAP-Paket zu einem Zielbericht erstellen möchten, der auf einem relationalen Paket basiert, müssen Ihre Zielparameter auf ein Abfrageelement gesetzt werden, das denselben Wert wie der OLAP-Geschäftsschlüssel oder die Memberunterschrift hat. Weitere Informationen finden Sie unter „Mitglieder und Werte“ auf Seite 390.

Wenn Ihr Zielbericht mit den falschen Werten gefiltert wird, überprüfen Sie die Werte, die von der Quelle zum Ziel zugeordnet werden.

Sie müssen über die erforderlichen Berechtigungen verfügen, um den Drillthrough-Assistenten zu verwenden. Die Informationen, die der Drillthrough-Assistent bereitstellt, sind auf der **Gehe zu** -Seite verfügbar, wenn Sie die Drillthrough-Operation ausführen. Der Drillthrough-Assistent stellt die folgenden Informationen bereit.

Übergebene Quellenwerte

Die Quellenwerte sind die Werte aus dem Auswahlkontext, die für die Übergabe an den Zielbericht verfügbar sind, wenn der Benutzer für den Drillthrough zum Zielbericht oder zum Zielobjekt auswählt. Wenn Sie beispielsweise einen Drillthrough von einer Quelle in Analysis Studio durchführen, sehen Sie die Werte an der Schnittmenge, die Sie vor der Drillthrough-Aktion ausgewählt haben, sowie alle Werte im Kontextbereich.

Die Werte in der Debugliste sind die Werte in dem Quellenbericht, die durch eine Drillthrough-Operation transformiert wurden.

· Anzeigewert

Zeigt den Wert an, den Benutzer bei der Verwendung dieses Datenelements oder dieses Members sehen. Bei OLAP-Membern handelt es sich um die Mitgliedskaption oder -beschriftung. Beispiel: `Telefon` ist ein Mitglied aus der Dimension `Bestellmethode` .

· Wert verwenden

Zeigt den Wert an, den IBM Cognos beim Abrufen des Datenelements oder des Members verwendet und analysiert. Für OLAP-Member ist dies der eindeutige Membername (MUN). Beispiel: `[große_outdoors_company].[Bestellmethode].[Bestellmethode].[Order Method1]->:[PC]. [@MEMBER]. [2]` ist die MUN für das `Telefon` -Member in der `Bestellmethode` -Dimension.

Zielzuordnung

Wenn Sie sich für die Verwendung von Parametern im Ziel entschieden haben, zeigt die Zielzuordnung den Namen jedes Parameters an, der in der Drillthrough-Definition zugeordnet wurde, und die Werte, die von der Quelle versucht werden, an diesen Parameter zu übergeben.

· Parametername

Zeigt eine Liste der gültigen Zielparameter an, die in der Drillthrough-Definition zugeordnet sind, um Informationen aus dem Abfrageelement, der Ebene oder der Hierarchie zu empfangen, auf denen Sie die Drillthrough-Aktion ausgeführt haben.

Es können nur Parameter angezeigt werden, für die eine gültige Zuordnung und nur die Namen der Parameter vorhanden sind. Wenn der Zielbericht beispielsweise einen Parameter für `Produkttyp` enthält und die Drillthrough-Definition diesen Zielparameter den Metadaten der `Produkttyp` -Quellenebene zuordnet, wird dieser Zielparameter nur angezeigt, wenn Sie versuchen, im Quellenbericht eine Drillthrough-Operation auf der `Produkttyp` -Ebene durchzuführen. Durch das Durchbohren auf der `Produktlinie` -Ebene wird dieses Parameterziel nicht angezeigt.

Sie müssen sicherstellen, dass die Zielparameter in Ihren Drillthrough-Definitionen korrekt zugeordnet werden. Falsch zugeordnete Parameter können Informationen aus den falschen Quellenmetadaten empfangen, insbesondere dann, wenn Sie Datenwerte haben, die nicht eindeutig sind. Wenn keine Zielparameter oder Parameter angezeigt werden können, die in der Liste **Zielzuordnung anzeigen** angezeigt werden sollen, überprüfen Sie die Parameterzuordnung in der Drillthrough-Definition.

· Anzeigewert

Zeigt den Wert an, den Benutzer bei der Verwendung eines Datenelements oder Mitglieds anzeigen. Bei OLAP-Membern handelt es sich um die Mitgliedskaption oder -beschriftung. Beispiel: `Telefon` ist ein Mitglied aus der Dimension `Bestellmethode` .

· Wert verwenden

Zeigt den transformierten Wert an, den die Drillthrough-Definition verwendet, wenn ein Datenelementwert oder ein Member an den Zielparameter übergeben wird.

OLAP-Mitglieder, die an die Parameter für relationale Zielparameter übergeben werden, erhalten den Geschäftsschlüssel von den Membern der Member MUN und übergeben nur den Geschäftsschlüssel. Mit dem Beispiel des `Telefon` -Members in `Bestellmethode`nist der Geschäftsschlüssel 2. Wenn Sie sich unsicher sind, was der Geschäftsschlüssel für ein Mitglied ist, können Sie einen Ausdruck wie `roleValue ('_businessKey', [member])`schreiben. Dieser Wert wird an den Zielparameter übergeben.

OLAP-Member, die auf der Basis eines anderen OLAP-Pakets desselben OLAP-Typs an einen Zielparameter übergeben wurden, zeigen eine transformierte MUN an. Mit dem Beispiel `Bestellmethode`n wird die MUN nun transformiert und die Drillthrough-Definition verwendet den Wert von `[great_outdoors_company].[Bestellmethode].[Bestellmethode].[Order Method1]-> [Order Method1]. [2]: [PC]. [@MEMBER]. [2]`. Der mittlere Abschnitt von `[Bestellmethod1] [2]` ist der Ort, an dem die Drillthrough-Definition das richtige Member im Ziel findet, wenn die OLAP-Datenquellen unterschiedlich sind. Um die MUN für ein bestimmtes Member

anzuzeigen, können Sie sich die Eigenschaften des Mitglieds in Reporting ansehen und sich die Eigenschaft `Eindeutiger Mitgliedsname` ansehen.

Zugriff auf den Drill-through-Assistenten

Sie können den Drillthrough-Assistenten für Debugging-Zwecke verwenden, wenn Sie mit Drillthrough-Definitionen arbeiten.

Vorbereitende Schritte

Um diese Funktionalität zu verwenden, müssen Sie über die erforderlichen Berechtigungen für die geschützte **Drillthrough-Assistent** -Funktion in IBM Cognos Administration verfügen.

Vorgehensweise

1. Wählen Sie einen Link in Ihrem Quellenbericht aus, klicken Sie mit der rechten Maustaste auf den Link und wählen Sie **Gehe zu**aus, oder klicken Sie in PowerPlay Studio auf den Drillthrough-Knopf.

   Die Seite **Zugehörige Links** wird angezeigt, in der die Liste der verfügbaren Zielberichte angezeigt wird. Wenn Ihr Zielbericht nicht angezeigt wird, überprüfen Sie die Bereichseinstellungen in Ihrer Drillthrough-Definition.

   Tipp: Wenn nur ein Ziel verfügbar ist, wird bei Auswahl von **Zugehörige Links**das Ziel geöffnet, ohne dass die Seite **Gehe zu** angezeigt wird.
2. Klicken Sie auf **Übergebene Quellenwerte anzeigen** , um die Werte anzuzeigen, die für die Übergabe durch den Quellenbericht verfügbar sind.
3. Klicken Sie neben dem Zielbericht auf den Abwärtspfeil und wählen Sie **Zielzuordnung anzeigen**aus.

   Es wird eine Liste der gültigen zugeordneten Daten angezeigt, in der die verfügbaren Quellenwerte sowie die Werte für die Verwendung und die Anzeige angezeigt werden.
4. Klicken Sie für eine Gruppe von Werten auf **Weitere Informationen** , um die XML für den Auswahlkontext (übergebene Quelle) oder die Drillthrough-Spezifikation (Zielzuordnung) anzuzeigen.

Beispiel-Debugging einer Drillthrough-Definition

Im Folgenden sehen Sie ein Beispiel für das Debugging einer Drillthrough-Definition.

Ihre OLAP-Quelle verfügt über eine Dimension 'Products' mit den Ebenen 'Line', 'Type' und 'Name'. Sie haben einen Parameter in Ihrem relationalen Ziel so definiert, dass er jeder Ebene dieser OLAP-Quellendimension entspricht. Sie können eine Situation haben, in der alle Zielparameter aus einer einzelnen Dimension angezeigt werden, die in der Liste Zugeordnete Zielliste angezeigt wird. Dies ist wahrscheinlich, weil die einzelnen Zielparameter in der Drillthrough-Definition, in diesem Fall der Dimension 'Products', einer einzigen Dimension zugeordnet werden. In Ihrer OLAP-Datenquelle haben Sie einen Geschäftsschlüsselwert oder den Quellenwert, der zum Erstellen der Member verwendet wird, der in allen drei Ebenen dupliziert wird, wie in der folgenden Tabelle dargestellt.

Tabelle 79. Beispiel für eine problematische Parameterzuordnung für Drillthrough-Definition

Parametername	**Anzeigewert**	**Wert verwenden**
Prod-Zeilenparameter	Campingausrüstung	1
Produktart-Parameter	Kochgerät	1
Produktname-Parameter	Trail Chef Water Bag	1

Alle drei Parameter, die der Dimension 'Products' zugeordnet sind, sind korrekt, wenn die Nutzungswerte in der Dimension nicht dupliziert werden. In der vorhergehenden Tabelle haben die Mitglieder aus allen drei Ebenen den gleichen Nutzungswert. In diesem Fall kann die Drillthrough-Operation nicht feststellen, welche Ebene die richtige ist, da das Szenario angibt, dass alle Ebenen gültig sind. In dieser Situation wird die erste Ebene, die mit einem gültigen Geschäftsschlüssel oder einem gültigen Wert für die Verwendung festgestellt wurde, von der Drillthrough-Definition erfüllt. Dies kann zu einem unerwarteten Verhalten führen.

Dieses Beispiel zeigt, warum es wichtig ist, immer sicherzustellen, dass Ihre Data Warehouses und OLAP-Quellen mit eindeutigen Geschäftsschlüsseln oder Quellenwerten entworfen werden. Um diese Situation zu korrigieren, muss die Drillthrough-Definition jedem einzelnen Zielparameter zugeordnet sein, der jeder zugeordneten Ebene in den Quellenmetadaten und nicht in der Dimension zugeordnet ist.

Drillthrough-Zugriff in einem Bericht einrichten

Verwenden Sie Reporting , um einen Quellen-Drillthrough-Bericht zu erstellen, um zwei Berichte, die zugehörige Informationen enthalten, zu verknüpfen. Sie können dann auf zugehörige oder detailliertere Informationen in einem Bericht zugreifen, indem Sie einen Wert oder mehrere Werte im Quellenbericht auswählen. Sie können auch innerhalb des gleichen Berichts Drillthrough-Elemente durchführen, indem Sie Lesezeichen erstellen.

Vorbereitende Schritte

Tipp: Wenn Sie einen Bericht als Quelle in einer Drillthrough-Definition verwenden möchten, muss die Option **Paketbasierte Drillthrough zulassen** ausgewählt sein (Menü**Daten** , **Drillverhalten**). Diese Option ist standardmäßig ausgewählt.

Vorgehensweise

1. Öffnen Sie den Zielbericht.
2. Erstellen Sie einen Parameter, der als Drillthrough-Spalte dienen soll oder den Bericht filtern soll.

   Erstellen Sie beispielsweise den folgenden Parameter, um die Produktlinie zu durchbohren oder zu filtern:

   [Produktreihe]=?prodline_p?

   Tipp: Verwenden Sie die Operatoren `In`oder `in_Bereich`, um den Zielbericht zu aktivieren, um mehrere Werte oder einen Wertebereich zu akzeptieren.
3. Geben Sie im Feld **Verwendung** an, welche Schritte ausgeführt werden sollen, wenn ein Wert für den Zielparameter nicht als Teil eines Drillthrough übergeben wird:

   - Wenn Sie angeben möchten, dass Benutzer einen Wert auswählen müssen, klicken Sie auf **Erforderlich**.

     Wenn kein Wert für den Zielparameter übergeben wird, werden die Benutzer aufgefordert, einen Wert auszuwählen.
   - Wenn Sie angeben möchten, dass Benutzer keinen Wert auswählen müssen, klicken Sie auf **Optional**.

     Benutzer werden nicht aufgefordert, einen Wert auszuwählen, und daher wird der Wert nicht gefiltert.
   - Um anzugeben, dass der Parameter nicht verwendet werden soll, klicken Sie auf **Inaktiviert**.

     Der Parameter wird während der Drillthrough-Operation nicht verwendet. Sie wird auch nicht für andere Zwecke im Bericht verwendet.

     Tipp: Wenn der Parameter aus anderen Gründen in dem Bericht benötigt wird, können Sie auch angeben, dass er nicht in der Drillthrough-Definition verwendet werden soll (**Parameter** -Tabelle, **Methode**, **Parameter nicht verwenden**).

Ergebnisse

Der Drillthrough-Text wird als blauer Hyperlink in Textelementen in den Nicht-Diagrammbereichen des Berichts angezeigt. Darüber hinaus können Berichtskonsumenten die Drillthrough-Aktion starten, indem Sie auf die Schaltfläche **Gehe zu** klicken oder indem Sie mit der rechten Maustaste auf das Element klicken und auf **Gehe zu**, **Zugehörige Links**klicken. Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie mit dem Drillthrough-Assistenten anzeigen, welche Parameter von der Quelle übergeben wurden und wie sie im Zielobjekt von der **Gehe zu** -Seite zugeordnet werden.

Geben Sie den Drillthrough-Text an

Sie können den Drillthrough-Text angeben, der angezeigt wird, wenn Benutzer einen Drillthrough zu mehr als einem Ziel durchführen können.

Wenn zum Beispiel Benutzer aus verschiedenen Regionen den Bericht anzeigen, können Sie Text in einer anderen Sprache für jede Region anzeigen.

Vorgehensweise

1. Klicken Sie auf das Drillthrough-Objekt, und klicken Sie anschließend im Teilfenster **Eigenschaften** auf **Drillthrough-Definitionen**.
2. Wenn für das Objekt mehr als eine Drillthrough-Definition vorhanden ist, klicken Sie im Feld **Drillthrough-Definitionen** auf eine Drillthrough-Definition.
3. Klicken Sie auf die Registerkarte **Bezeichnung** .
4. Gehen Sie wie folgt vor, um die Beschriftung mit einer Bedingung in der **Bedingung** -Box zu verknüpfen:
   - Klicken Sie auf **Variable** , und klicken Sie auf eine vorhandene Variable oder erstellen Sie eine neue Variable.
   - Klicken Sie auf **Wert** , und klicken Sie auf einen der möglichen Werte für die Variable.
5. Klicken Sie in der **Quellentyp** -Box auf den zu verwendenden Quellentyp.
6. Wenn der Quellentyp **Text**ist, klicken Sie auf die Schaltfläche mit den Auslassungspunkten, die dem Feld **Text** entspricht, und geben Sie Text ein.
7. Wenn der Quellentyp **Datenelementwert** oder **Datenelementbeschriftung**ist, klicken Sie auf **Datenelement** , und klicken Sie auf ein Datenelement.
8. Wenn der Quellentyp **Berichtsausdruck**ist, klicken Sie auf die Schaltfläche mit den Auslassungspunkten, die dem **Berichtsausdruck** -Feld entspricht, und definieren Sie den Ausdruck.
9. Wenn die Beschriftung mit einer Bedingung verknüpft ist, wiederholen Sie die Schritte 5 bis 8 für die verbleibenden möglichen Werte.

Ergebnisse

Wenn Benutzer den Quellenbericht ausführen und auf einen Drillthrough-Link klicken, wird die Seite **Gehe zu** angezeigt. Der Drillthrough-Text, den Sie angegeben haben, wird für jedes Ziel angezeigt. Wenn Sie den Drillthrough-Text für ein Ziel nicht angegeben haben, wird der Drillthrough-Name verwendet.

Kapitel 27. Arbeitsbereich ' IBM Cognos '

IBM Cognos Workspace ist ein webbasiertes Tool, mit dem Sie IBM Cognos -Inhalte und externe Datenquellen zum Erstellen anspruchsvoller, interaktiver Arbeitsbereiche verwenden können. For more information about IBM Cognos Workspace, see the IBM Cognos Workspace *Benutzerhandbuch*.

Um Cognos Workspace zu starten, klicken Sie auf der **Begrüßung** -Seite auf **Neu** > **Sonstige** > **Arbeitsbereich**.

HTML-Markup aus RSS-Feed-Details entfernen

In IBM Cognos Workspace kann ein Benutzer ein RSS-Widget aus der Toolbox einfügen. Nach der Konfiguration des RSS-Feeds zeigt das RSS-Feed-Widget die HTML-Markup an, wenn die Feeddetails aktiviert sind.

Sie können die HTML-Markup ausblenden, wenn die Option **Feed-Details anzeigen** aktiviert ist, indem Sie die erweiterte Einstellung **`CPSRssAllowUnsafeCharacters`** auf dem Dispatcher angeben. Sie müssen den Parameter für jeden Dispatcher festlegen. Bei mehreren Dispatchern können Sie den Parameter global festlegen.

Vorgehensweise

1. Klicken Sie in der IBM Cognos Administration auf **Konfiguration** > **Dispatcher und Services**.
2. Gehen Sie wie folgt vor, um die Einstellung **`CPSRssAllowUnsafeCharacters`** für einen einzelnen Dispatcher anzugeben:
   a) Klicken Sie in der Spalte **Name** auf einen Dispatcher, und klicken Sie auf **Eigenschaften festlegen**.
   b) Rufen Sie die **PresentationService**auf und klicken Sie auf **Eigenschaften festlegen**.
   c) Klicken Sie auf die Registerkarte **Einstellungen** , und klicken Sie für **Umwelt**, **Erweiterte Einstellungen**auf **Bearbeiten**.
   d) Klicken Sie auf **Über den übergeordneten Eintrag erfasste Einstellungen außer Kraft setzen**. Fahren Sie mit Schritt 4 fort.
3. Gehen Sie wie folgt vor, um den globalen Parameter **`CPSRssAllowUnsafeCharacters`** für mehrere Dispatcher anzugeben:
   a) Klicken Sie in der Symbolleiste von **Konfiguration** auf **Eigenschaften festlegen-Konfiguration**.
   b) Klicken Sie auf die Registerkarte **Einstellungen** , und klicken Sie für **Umwelt**, **Erweiterte Einstellungen**auf **Bearbeiten**.
4. Geben Sie **`CPSRssAllowUnsafeCharacters`**in das Feld **Parameter** ein und geben Sie im Feld **Wert** den Wert **`Wahr`**ein.
5. Klicken Sie auf **OK**.

Ergebnisse

HTML-Markup wird in den RSS-Feed-Details nicht angezeigt.

Kapitel 28. Verwaltung von Cognos Analytics Mobile Reports

IBM Cognos Analytics Mobile Reports erweitert die Funktionalität Ihrer vorhandenen IBM Cognos Analytics -Installation auf mobile Geräte, sodass Benutzer die Cognos Analytics -Inhalte auf ihren Tablets oder Smartphones anzeigen und mit ihnen interagieren können.

Mit dem Rich Client von Cognos Analytics Mobile Reports können Benutzer die aktiven Berichte von Cognos Analytics-Reporting und den Arbeitsbereichen aus dem Arbeitsbereich von Cognos auf ihren mobilen Geräten anzeigen. Die aktiven Berichte müssen auf dem Server als gespeicherte Ausgaben vorhanden sein oder an den Cognos Analytics Mobile Reports -Benutzer zugestellt werden. Aktive Berichte müssen auf dem Server ausgeführt werden, nicht auf dem Client.

Die Eingabeaufforderungsfunktionen und die Zeitplanungsmechanismen von Cognos Analytics werden verwendet, um angepasste Berichte zeitnah zu liefern. Cognos Analytics -Sicherheit und verschiedene, herstellerspezifische Sicherheitsmechanismen, einschließlich einheitenbasierter und serverbasierter Sicherheit, werden zum Schutz des Berichts und des Arbeitsbereichsinhalts verwendet.

Viele der gerätespezifischen Management-Server und Verwaltungstools, die von Cognos Analytics Mobile Reports verwendet werden, bieten die Möglichkeit, Inhalte über Fernzugriff von einer Einheit zu entfernen oder die Einheit vollständig zu inaktivieren. Wenn eine Einheit beispielsweise verloren geht oder gestohlen wird, kann der Cognos Analytics -Administrator diese Funktionalität zum Schutz sensibler Inhalte auf dem Gerät verwenden. Der Cognos Analytics -Administrator kann auch ein Ablaufdatum für einen Bericht festlegen, nach dem der Bericht bis zum erneuten Authentifizieren des Benutzers unzugänglich wird.

Cognos Analytics Mobile Reports unterstützt Anforderungen zwischen dem mobilen Gerät und der Serverumgebung für die folgenden Produktfunktionen:

- Suchen
- Durchsuchen
- Ausführen

Auf der Registerkarte **Mobil** in der IBM Cognos Administration werden zentrale Verwaltungsfunktionen für Cognos Analytics Mobile Reportsbereitgestellt. Um auf diese Registerkarte zugreifen zu können, muss der Administrator über die erforderlichen Zugriffsberechtigungen für die Funktionalität von **Mobile Administration** verfügen. **Mobile Administratoren**, eine der vordefinierten Rollen im Namespace von **Cognos** , kann verwendet werden, um Zugriffsberechtigungen für diese Funktion anzugeben.

Cognos Analytics Mobile Reports verwendet dieselbe Gruppe von Benutzern wie Cognos Analytics. Weitere Informationen zur Verwaltung von Cognos Analyticsfinden Sie in den Abschnitten zu den anderen Abschnitten in der *IBM Cognos Analytics Administration and Security Guide*.

Native Cognos Analytics Mobile Reports -Apps für Benutzer vorkonfigurieren

Konfigurieren Sie die Anwendung IBM Cognos Analytics Mobile Reports , um die Konfiguration für Benutzer zu optimieren und zu steuern, wie die Anwendung auf iOS-und Android-Geräten funktioniert.

Informationen zu diesem Vorgang

Sie können Konfigurationseinstellungen in einer URL codieren und generieren, um Benutzer von Cognos Analytics Mobile Reportse in einer E-Mail-Nachricht, einem Chat oder mit anderen Methoden zu verteilen. Mit dieser URL können die Benutzer die Anwendung automatisch auf ihren mobilen Endgeräten konfigurieren.

Die Cognos -Server-URL ist in der Konfiguration enthalten, damit die Benutzer bei der Konfiguration der Anwendung nicht die URL auf ihren mobilen Einheiten eingeben müssen.

Als zusätzliche Sicherheitsmaßnahme kann ein Kennwort auch in die Konfiguration aufgenommen werden. Das Kennwort für die mobile Konfiguration stellt eine fälschungssichere Abdichtung zur Verfügung, um die Integrität der Konfigurations-URL zu gewährleisten, und bestätigt, dass die Quelle der URL gültig ist. Die Konfigurations-URL und das Kennwort sollten niemals zusammen mit demselben Medium, wie z. B. E-Mail oder Chat, zusammen übertragen werden. Benutzer müssen dieses Kennwort nur einmal eingeben, wenn sie die Konfigurations-URL öffnen.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf die Registerkarte **Mobil** .
2. Klicken Sie auf **Ferne Konfiguration**.
3. Geben Sie für **IBM Cognos-Server-URL**Ihren IBM Cognos Analytics -Server-URL ein: `http://`*`Servername`*`:`*`Portnummer`*`/bi/v1/disp`
4. Aktivieren oder inaktivieren Sie die folgenden Einstellungen:

   Pass-Through-Authentifizierung
   Aktivieren Sie diese Einstellung, damit Benutzer über die verschiedenen dazwischenliegenden Webseiten, die für sie angezeigt werden, zum Cognos Analytics -Server navigieren können.

   Standardmäßig ist für Cognos Analytics Mobile Reports eine direkte Konnektivität mit dem IBM Cognos Analytics -Server erforderlich. Wenn eine direkte Konnektivität wegen der intervenierenden Sicherheitsprodukte nicht möglich ist, muss diese Einstellung aktiviert sein. Zu den intervenierenden Produkten gehören CA SiteMinder, Tivoli Access Manager, Microsoft ISA Server oder Landing-Pages in öffentlichen WiFi-Netzen.

   Automatische Downloads
   Aktivieren Sie diese Einstellung für die Cognos Analytics Mobile Reports -Apps, um neue Berichtsausgaben automatisch aus dem Posteingang des Benutzers und aus Berichten, die an den Benutzer übertragen wurden, herunterzuladen. Diese Einstellung sollte aktiviert werden, es sei denn, die Bandbreite ist ein Anliegen.

   Beispielserver anzeigen
   Aktivieren Sie diese Einstellung für die Cognos Analytics Mobile Reports -Apps, um auf den Cognos Analytics Mobile Reports -Beispielserver zuzugreifen. Der Beispielserver enthält Beispiele für IBM Cognos -Berichte, die die Funktionen der IBM Cognos -Software veranschaulichen. Die Beispielberichte sind für die Verwendung in Cognos Analytics Mobile Reportsoptimiert.

   Anwendungsstatus verwalten
   Aktivieren Sie diese Einstellung, damit die Anwendung nach dem Neustart der Anwendung den neuesten Inhaltsbereich wiederherstellen kann. Wenn die Anwendung beispielsweise während der Anzeige eines Berichts im Inhaltsbereich "Eigene Berichte" geschlossen wird, öffnet die Anwendung den Inhaltsbereich "Meine Berichte" nach einem Neustart erneut. Wenn diese Einstellung inaktiviert ist, zeigt die Anwendung die Hauptanzeige nach einem Neustart an.

   Standardwert: **Aus**
5. Optional: Wählen Sie das Markierungsfeld **Kennwort für mobile Konfiguration** aus, und geben Sie ein Kennwort für Ihre Auswahl ein.

   Das Kennwort kann maximal 20 alphanumerische Zeichen enthalten und darf keine Leerzeichen enthalten.

   Wenn Sie dieses Kennwort angeben möchten, stellen Sie sicher, dass Sie es den Benutzern separat von der Konfigurations-URL zur Verfügung stellen.
6. Optional: Wählen Sie das Kontrollkästchen **SSL/TLS-Zertifikat-Pinning** aus und fügen Sie den SHA-1-Fingerabdruck des SSL-oder TLS-Zertifikats ein, mit dem der Eingangspunkt auf Ihrem Cognos Analytics -Server gesichert wird. Ein Beispiel für den Cognos Analytics -Servereingangspunkt ist ein Web-Server, ein Proxy-Server oder eine Lastausgleichsfunktion.

Aktivieren Sie diese Einstellung, um sicherzustellen, dass der Client nur mit den Servern kommuniziert, die mit dem X.509v3-Zertifikat konfiguriert sind, und die denselben SHA-1-Fingerabdruck haben.

Der Wert für diese Einstellung ist eine Folge von 40 Hexadezimalzeichen (a-f und 0-9) ohne Interpunktionszeichen. Entfernen Sie die Punktuationsmarkierungen aus dem Wert, bevor Sie sie in diesem Feld einfügen. Sie können mehrere SHA-1-Fingerabdruckwerte angeben, die sie mit einem Doppelpunkt (:) trennen.

Tipp: In Firefox können Sie den SHA-1-Fingerabdruck abrufen, indem Sie in der URL-Leiste des Browsers auf das Symbol für das Vorhängeschloss klicken und dann auf **Weitere Informationen** > **Zertifikat anzeigen**klicken.

7. Klicken Sie auf **Mobile-Konfigurationscode generieren**.

   Es wird eine base64-codierte URL generiert, die die angegebenen Konfigurationseinstellungen enthält.

   Im Folgenden sehen Sie ein Beispiel für die generierte URL:

   ```
   cmug://aHR0cDovL3ZvdHRtb2IxL2NzcDI-dmVyc2lvbj0xLjAmcGFzcz1vZmYmYXV0b
   2R3bj1vZmYmZGlzcHNhbXA9b24mcHdkPW9uJnNhbHQ9UWlzQVJoTTNPaFVfJmhhc2g9Q
   VFnQUFBQkliV0ZqVTBoQk1iV2U3SEJiUjhkczJBV2wrKzI0Y2d6cWxLMi8.
   ```

8. Kopieren Sie die Konfigurations-URL, und stellen Sie sie den Cognos Analytics Mobile Reports -Anwendungsbenutzern per E-Mail, Chat oder mit anderen Methoden zur Verfügung.

   Stellen Sie sicher, dass die folgenden Bedingungen beim Kopieren und Übertragen der URL erfüllt sind:

   - Alle Zeichen in der URL, einschließlich Unterstreichungszeichen (_), werden beim Kopieren der URL ausgewählt.
   - Die Anwendung, die Sie zum Übertragen der Konfigurations-URL verwenden, verwaltet den Fall der URL. Bei der URL muss die Groß-/Kleinschreibung beachtet werden.

Ergebnisse

Wenn Benutzer auf die Konfigurations-URL vom Administrator tippen, wird die Cognos Analytics Mobile Reports -Anwendung auf ihrem iOS-oder Android-Gerät geöffnet. Die Benutzer müssen bestätigen, ob sie mit der automatischen Konfiguration fortfahren möchten. Wenn das Kennwort für die mobile Konfiguration in Schritt 5 angegeben wurde, müssen die Benutzer das Kennwort eingeben, wenn sie dazu aufgefordert werden. Die Anwendung wird dann mit den Einstellungen konfiguriert, die in der URL angegeben sind.

Wenn die Benutzer ein falsches Kennwort eingeben oder auf die Schaltfläche **Abbrechen** tippen, wird die Anwendung geöffnet, ohne dass Konfigurationseinstellungen angewendet werden.

Tipp: Einige E-Mail-Anwendungen liefern die Konfigurations-URL für Benutzer als Klartext. In dieser Situation können die Administratoren die URL auf einer Webseite platzieren, auf die die Benutzer zugreifen können. Unter iOS können Nutzer die URL auch kopieren und in den Browser einfügen und von dort aus öffnen.

Erweiterte Einstellungen für Cognos Analytics Mobile Reports angeben

Sie können erweiterte IBM Cognos Analytics Mobile Reports -Einstellungen global für alle Services, für einen bestimmten Dispatcher oder für einen bestimmten Cognos Analytics Mobile Reports -Service konfigurieren.

Wenn die Einstellungen global konfiguriert sind, werden die Werte, die Sie angeben, von allen Instanzen des Cognos Analytics Mobile Reports -Service erfasst. Sie können die globalen Werte überschreiben, indem Sie angepasste Werte auf dem Dispatcher-oder Cognos Analytics Mobile Reports -Service-Level angeben.

Wenn der Konfigurationseintrag untergeordnete Einträge mit Einstellungen enthält, die die globalen Einstellungen überschreiben, können die angepassten Einstellungen für die untergeordneten Einträge

zurückgesetzt werden, um die Standardwerte zu verwenden. Um den Wert einer beliebigen Einstellung auf den Standardwert zurückzusetzen, löschen Sie die Einstellung.

Vorgehensweise

1. Klicken Sie in der IBM Cognos Administration auf der Registerkarte **Konfiguration** auf **Dispatcher und Services** und führen Sie eine der folgenden Aktionen aus:
   - Um erweiterte Einstellungen global zu konfigurieren, klicken Sie in der Symbolleiste auf der **Konfiguration** -Seite auf das Symbol **Eigenschaften festlegen-Konfiguration**  und fahren Sie mit Schritt 3 fort.
   - Um erweiterte Einstellungen für einen bestimmten Dispatcher zu konfigurieren, suchen Sie den Dispatcher, und klicken Sie in der Spalte **Aktionen** auf das Symbol **Eigenschaften festlegen**  . Fahren Sie dann mit Schritt 3 fort.
   - Wenn Sie erweiterte Einstellungen für einen bestimmten Mobile-Service konfigurieren möchten, klicken Sie auf den Dispatcher, der diesen Service enthält. Suchen Sie in der Liste der Dispatcherservices **MobileService**. Klicken Sie in der Spalte **Aktionen** auf das **Eigenschaften festlegen** -Symbol  , das dem Service zugeordnet ist, und fahren Sie mit Schritt 3 fort.
2. Klicken Sie auf die Registerkarte **Einstellungen** .
3. Klicken Sie für **Erweiterte Einstellungen**auf **Bearbeiten**.

   Wenn der Parameter nicht aufgelistet ist, geben Sie den Namen des Parameters ein.
4. Geben Sie den entsprechenden Wert für die Einstellung an und klicken Sie auf **OK**.

   Tipp: Wenn Sie eine erweiterte Einstellung löschen möchten, wählen Sie das entsprechende Kontrollkästchen aus und klicken Sie auf **Löschen**.

Cognos Analytics Mobile Reports -Thema konfigurieren

Das Thema IBM Cognos Analytics Mobile Reports definiert die Darstellung der Begrüßungsseite für die Cognos Analytics Mobile Reports -Anwendung. Standardmäßig verwenden die Clientanwendungen das Standardmotiv, das in das Produkt integriert ist. Sie können Ihr eigenes Cognos Analytics Mobile Reports -Motiv erstellen, um das Aussehen der Anwendung anzupassen und das Motiv so zu konfigurieren, dass es den von Ihnen ausgewählten Benutzergruppen und Rollen zur Verfügung steht. Administratoren können jederzeit auf das Standardmotiv zurückgreifen.

Informationen zu diesem Vorgang

Zu den Konfigurationstasks gehören die Aktivierung der Unterstützung für Cognos Analytics Mobile Reports -Themen, das Hinzufügen, Bearbeiten oder Löschen der Themen sowie das Definieren, welche Gruppen und Rollen die Themen verwenden können.

Der gleiche Benutzer kann zu verschiedenen Gruppen und Rollen gehören und kann daher Zugriff auf verschiedene Themen haben. Um sicherzustellen, dass korrekte Themen für die Benutzer angewendet werden, müssen die Administratoren sorgfältig überlegen, welche Gruppen und Rollen sie bei der Konfiguration des Themas auswählen können.

Das Cognos Analytics Mobile Reports -Standardschema wird in der `defaultTheme.zip` -Vorlage definiert, die mit dem Produkt installiert wird. Administratoren können diese Vorlage als Ausgangspunkt verwenden, wenn Sie ein angepasstes Motiv erstellen. Diese Vorlage ist nicht erforderlich, damit das Produkt ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter „Angepasstes Cognos Analytics Mobile Reports -Motiv erstellen” auf Seite 409.

Vorgehensweise

1. Melden Sie sich über einen Desktop-Browser bei IBM Cognos Analytics mit mobilen Administratorberechtigungen an.

2. Rufen Sie die IBM Cognos Administration auf, und klicken Sie auf die Registerkarte **Mobil** .
3. Führen Sie die folgenden Schritte aus, um sicherzustellen, dass die Themenunterstützung für den Mobile-Service aktiviert ist:
   a) Klicken Sie auf **Serverkonfiguration**.
   b) Suchen Sie in der Gruppe **Richtlinie** der Einstellungen die Einstellung **Unterstützung für mobile Themen** und stellen Sie sicher, dass der Wert von **ThemenIn** für diese Einstellung angegeben ist.
   c) Klicken Sie auf die Schaltfläche **Mobile Konfiguration anwenden** , um die Konfiguration zu speichern.
4. Öffnen Sie die Seite **Konfiguration der mobilen Benutzerschnittstelle** .
5. Um ein neues Thema hinzuzufügen, klicken Sie auf das Symbol **Neues Thema**  .
6. Führen Sie auf der **Mobile Themenkonfiguration** -Seite die folgenden Schritte aus:
   a) Geben Sie in das Feld **Geben Sie einen Namen für das Thema an.** den Themennamen ein. Sie können einen beliebigen Namen angeben, der für Ihre Umgebung aussagekräftig ist.
   b) Suchen Sie im Feld **Geben Sie eine zu ladende Themendatei an** nach einer komprimierten Datei, die die Motivressourcen enthält.
   c) Klicken Sie im Feld **Gruppe oder Rolle angeben** auf die Schaltfläche **Gruppe auswählen** , und wählen Sie die Gruppen oder Rollen aus, die das Motiv verwenden müssen. Sie können Gruppen und Rollen aus dem Cognos -Namespace oder aus anderen aktiven Namespaces auswählen.
   d) Klicken Sie auf **OK** , wenn alle Parameter korrekt angegeben sind.

   Der Themenname wird auf der **Konfiguration der mobilen Benutzerschnittstelle** -Seite angezeigt.
7. Wenn Sie das Thema bearbeiten möchten, klicken Sie auf das Symbol **Eigenschaften festlegen** in der Spalte **Aktionen** . Sie können jeden der Motivparameter bearbeiten.
8. Wenn Sie das Thema löschen möchten, wählen Sie das entsprechende Kontrollkästchen aus und klicken Sie in der Symbolleiste auf das Symbol **Löschen**  .

   Wenn Sie zum Standardthema Cognos Analytics Mobile Reports zurückkehren möchten, löschen Sie das aktuell konfigurierte Thema. Die Benutzer, die dieses Thema verwenden, kehren automatisch zur Verwendung des Standardthemas zurück, wenn sie das nächste Mal eine Verbindung zum Cognos Analytics -Server herstellen.
9. Stellen Sie mithilfe von iOS-und Android-Geräten eine Verbindung zum Server her, für den das Motiv so konfiguriert wurde, dass Sie testen können, ob Ihre Änderungen ordnungsgemäß angewendet wurden.

Ergebnisse

Die Benutzer können die Anwendung weiterhin verwenden, während die Motivressourcen auf ihre Einheiten heruntergeladen werden. Das Motiv wird angewendet, wenn die Benutzer das nächste Mal eine Verbindung zum Cognos Analytics -Server herstellen oder ihre Anwendung aktualisieren.

Wenn ein Benutzer eine Verbindung zu mehreren Servern herstellen möchte, die möglicherweise unterschiedliche Themen konfiguriert haben, ist das Thema, das für den Benutzer angewendet wird, das Motiv, das für den Server konfiguriert ist, an den der Client zuerst erfolgreich angeschlossen wurde. Das Herstellen einer Verbindung zu anderen Servern ändert das Thema des Benutzers nicht, auch wenn die Server unterschiedliche Themen verwenden. Wenn Sie das Thema in dem für einen anderen Server konfigurierten Thema ändern möchten, entfernen Sie die Verbindung zum Server mit dem aktuellen Motiv. Anschließend kann der Benutzer eine Verbindung zu dem Server herstellen, der das erforderliche Motiv verwendet.

Angepasstes Cognos Analytics Mobile Reports -Motiv erstellen

Sie können ein angepasstes IBM Cognos Analytics Mobile Reports -Motiv erstellen, um das Standardthema zu ersetzen, das mit Cognos Analytics Mobile Reportsbereitgestellt wird.

Vorbereitende Schritte

Planen Sie das Design Ihres benutzerdefinierten Motivs und bereiten Sie die erforderlichen Ressourcen, wie z. B. Bilddateien, vor.

Informationen zu diesem Vorgang

Wenn Cognos Analytics Mobile Reports installiert ist, enthält das Installationsverzeichnis *Installationsposition*/templates/mobile die Datei defaultTheme.zip . Dies ist die Standardmotivvorlage. Sie können diese Vorlage als Ausgangspunkt verwenden, wenn Sie Ihr eigenes benutzerdefiniertes Motiv erstellen.

Die Datei defaultTheme.zip enthält verschiedene Verzeichnisse und Dateien. Die Datei main_panel\index.html ist die einzige Datei, die für Ihr benutzerdefiniertes Thema erforderlich ist. In dieser Datei definieren Sie alle Ressourcen, wie z. B. Bilder, die Sie in Ihrem benutzerdefinierten Motiv verwenden möchten, und ändern das Farbschema und die Schriftartstile.

Das Verzeichnis **Nls** in der Standardthemenvorlage enthält eine Verzeichnisstruktur für sprachspezifische Themen. Sie können diese Struktur emulieren oder Ihren eigenen Mechanismus für die Erstellung sprachspezifischer Themen implementieren.

Sie können die folgende Prozedur als Anleitung verwenden, wenn Sie ein angepasstes Mobile-Motiv auf der Basis des Standardthemas erstellen.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis *Installationsposition*/templates/mobile , erstellen Sie eine Kopie der defaultTheme.zip -Datei und speichern Sie sie unter einem anderen Namen.
2. Extrahieren Sie die Dateien aus der ZIP-Datei, die Sie im vorherigen Schritt erstellt haben.
3. Bearbeiten Sie die main_panel\index.html -Datei nach Bedarf. Diese Datei muss Verweise auf alle Ressourcen enthalten, die mit dem Thema enthalten sind.
4. Komprimieren Sie alle Motivressourcen in einer komprimierten Datei. Die ZIP-Datei muss mindestens die geänderte main_panel\index.html -Datei enthalten.
5. Speichern Sie die ZIP-Datei für Ihr Motiv in ein Verzeichnis Ihrer Wahl.

   Jetzt können Sie Cognos Analytics Mobile Reports für die Verwendung des angepassten Motivs konfigurieren. Weitere Informationen finden Sie unter „Cognos Analytics Mobile Reports -Thema konfigurieren“ auf Seite 408.

Cognos Analytics Mobile Reports -Services konfigurieren

Sie können global alle Instanzen des IBM Cognos Analytics Mobile Reports -Service konfigurieren.

Informationen zu diesem Vorgang

Durch die globale Anwendung der Cognos Analytics Mobile Reports -Konfigurationseinstellungen wird sichergestellt, dass alle Instanzen des Cognos Analytics Mobile Reports -Service synchronisiert werden, was dazu beiträgt, Fehler zu vermeiden.

Wichtig: Die Einstellungen können nicht für unterschiedliche Tenants in einer Multi-Tenant-Umgebung angepasst werden.

Vorgehensweise

1. Melden Sie sich über einen Desktop-Browser bei IBM Cognos Analytics mit mobilen Administratorberechtigungen an.
2. Rufen Sie die IBM Cognos Administration auf, und klicken Sie auf die Registerkarte **Mobil** .
3. Klicken Sie auf die Seite **Serverkonfiguration** .

4. Suchen Sie die Einstellung, die Sie konfigurieren möchten, und geben Sie ihren Wert nach Bedarf an.

   Sie können mehrere Einstellungen konfigurieren. Eine Liste der Einstellungen finden Sie unter „Einstellungen für Cognos Analytics Mobile Reports -Service-Konfigurationen" auf Seite 411.
5. Klicken Sie auf die Schaltfläche **Mobile Konfiguration anwenden** .

Einstellungen für Cognos Analytics Mobile Reports -Service-Konfigurationen

Diese Einstellungen werden verwendet, um die Bereitstellung von IBM Cognos Analytics -Inhalten in IBM Cognos Analytics Mobile Reports -Anwendungen zu verwalten.

Richtlinieneinstellungen

Diese Einstellungen definieren, wie Cognos Analytics -Inhalte an Cognos Analytics Mobile Reportsübergeben werden.

Maximale Anzahl von Seiten, die für jeden Bericht gespeichert werden sollen
Seiten über den angegebenen Grenzwert werden automatisch von der Einheit gelöscht.

Diese Einstellung gilt für Drillthrough-Zielberichte, die aus dem Arbeitsbereich von IBM Cognos gestartet werden.

Standardwert: 5

Tipp: Wenn Ihre Cognos Analytics Mobile Reports -Umgebung nur native Clients enthält, richten Sie die Standardeinstellung auf 50 Seiten ein. Verwenden Sie andernfalls den vorgeschlagenen Standardwert von 5.

Maximale Anzahl Tage zum Speichern eines Berichts
Gibt die maximale Zeit (in Tagen) an, die ein Bericht in der Datenbank gespeichert wird. Berichte, die diesen Grenzwert überschreiten, werden automatisch aus der Einheit entfernt.

Wert: 1 bis 999

Standardwert: 30

Maximale Anzahl Stunden zwischen den Ausführungen der Quellen-und Zielberichte
Gibt in Stunden die maximal zulässige Zeit zwischen den Ausführungen der Quellen-und Zielberichte an, wenn die Anwendung Drillthrough-Funktion mit aktiven Berichten in der nativen iOS-App verwendet wird. Wenn die Differenz zwischen den beiden Ausführungen diesen Betrag überschreitet, wird das Anwendungsdrillthrough-Ziel nicht verwendet.

Der Standardwert 1 bedeutet, dass der Zielbericht erfolgreich geöffnet werden kann, solange der Zielbericht innerhalb von 1 Stunde nach der Ausführung des Quellenberichts ausgeführt wurde.

Der Wert 0 inaktiviert die Anwendungsdrillthrough-Funktionalität. Wenn Sie den Quellenbericht nach dem Zielbericht mit diesem Wert ausführen, wird der Zielbericht nicht geöffnet und es wird eine Fehlernachricht angezeigt. In der Fehlernachricht wird angegeben, dass der Zielbericht nicht vorhanden ist und zuerst ausgeführt werden muss.

Diese Einstellung ist für die native Android-App Android nicht anwendbar.

Berechtigung zum Freigeben von Berichtsanzeigenerfassungen
Ermöglicht oder ermöglicht es den Benutzern eines nativen Clients, Screenshots der Berichte, die sie anzeigen, gemeinsam zu nutzen. Benutzer können Berichtsanzeigenerfassungen per E-Mail oder mit anderen Methoden gemeinsam nutzen.

Wert: Wahr oder Falsch

Standardwert: True

Cognos Analytics Mobile Reports -Stammordner
Gibt den Namen des Stammordners an, den Cognos Analytics Mobile Reports -Benutzer beim Durchsuchen oder Durchsuchen von Inhalten von einem mobilen Gerät aus starten müssen.

Standardwert: leer

Der Wert für diese Einstellung muss der Content Manager-Suchpfad im folgenden Format sein: /content/package [@name= '<*root_folder_name*>'].

Wenn die Einstellung leer ist, verwendet Cognos Analytics Mobile Reports den Stamminhaltsordner oder den Stammordner, der in der Datei "system.xml" des Portals angegeben ist, die im Verzeichnis *Installationsposition*/templates/ps gespeichert ist. Wenn Sie einen Stammordner hinzufügen, verwenden Sie die Syntax der Einstellung Consumer-Root in der Datei system.xml .

Tipp: Um den Suchpfad in IBM Cognos Analytics zu finden, zeigen Sie die Eigenschaften des Pakets oder Ordners an, das Sie als Cognos Analytics Mobile Reports -Stammordner verwenden möchten. Klicken Sie anschließend auf **Suchpfad, ID und URL anzeigen**.

Unterstützung für mobile Themen
Gibt an, ob angepasste mobile Motive für die Cognos Analytics Mobile Reports -Webanwendung unterstützt werden.

Werte: **ThemenIn** und **ThemenAus**

Standardwert: **ThemenAus**

Maximale Anzahl Stunden für den Zugriff auf mobile lokale Daten, die auf einer Einheit gespeichert sind
Gibt die maximale Anzahl Stunden an, in denen Benutzer von mobilen Geräten auf die lokalen Cognos Analytics Mobile Reports -Daten zugreifen können, die auf einer Einheit gespeichert sind.

Wert: 0 bis 8760

Standardwert: 36

Der Wert 0 inaktiviert den Leasingschlüsselmechanismus.

Maximale Anzahl Stunden zum Speichern zwischengespeicherter Berechtigungsnachweise
Wenn Sie Berechtigungsnachweise auf einer Einheit nicht speichern möchten, geben Sie 0 ein. Wenn Sie Berechtigungsnachweise auf einer Einheit speichern möchten, geben Sie einen Wert ein, der größer ist als die aktuelle Zeitlimiteinstellung für IBM Cognos Analytics. Solange Benutzer angemeldet sind, haben sie Zugriff auf ihre zwischengespeicherten Berechtigungsnachweise.

Wert: 0 bis 8760

Standardwert: 0

Maximale Anzahl an Stunden, die der Client mit geplanten Berichten aus dem aktuellen Stand bleiben kann
Diese Einstellung gilt für die Fälle, in denen ein Administrator Berichte für einen Benutzer auf dem Server plant und der Benutzer nicht anderweitig mit dem Server kommuniziert, bevor die Zeit abläuft, z. B. zum Abrufen anderer Berichte oder zum Durchsuchen des IBM Cognos Analytics -Portals. In der Mehrzahl der Fälle, z. B. wenn Berichte aus vorhandenen Zeitplänen oder aus vom Benutzer eingeleitete Aktionen stammen, ist diese Einstellung kein Faktor, da die Einheit normalerweise nur in Sekunden hinter dem Server lags bleibt.

Wert: 0 bis 999

Standardwert: 24

Der Wert 0 pusht Berichte, die sofort auf Einheiten heruntergeladen werden sollen.

Sicherheitseinstellungen

Diese Einstellungen werden verwendet, um die Cognos Analytics Mobile Reports -Anwendung zu sichern.

Lokale Speicherverschlüsselungsebene für IBM Cognos Analytics Mobile Reports -Anwendungen
Gibt die Methode an, mit der Daten, die auf iOS-oder Android-Geräten gespeichert werden, verschlüsselt werden.

Werte: NONE, AES128, AES256

Standardwert: AES128

Tipp: Die Webanwendung speichert Daten nicht lokal und ist von dieser Einstellung nicht betroffen.

Zeitlimit für Sicherheitscode-Sitzung in Sekunden
Gibt an, dass beim Zugriff auf die Cognos Analytics Mobile Reports -Anwendung und die maximale Anzahl an Sekunden, die die Anwendung inaktiv bleiben kann, ein Sicherheitscode erforderlich ist. Der Sicherheitscode darf keine aufeinanderfolgenden oder wiederholten Zahlen enthalten.

Wert: 1 bis 8760

Standardwert: -1

Ein Wert von -1 bedeutet, dass kein Sicherheitscode erforderlich ist. Der Wert 0 bedeutet, dass der Benutzer einen Sicherheitscode erstellen und ihn jedes Mal eingeben muss, um auf die App zuzugreifen.

Ein Wert größer als 0 gibt an, dass der Benutzer einen Sicherheitscode erstellen muss und die App für die in der Einstellung angegebene Anzahl Sekunden inaktiv lassen kann, bevor der Code erneut eingegeben werden muss, damit die App verwendet werden kann. Wenn der Wert beispielsweise auf 60 gesetzt ist, muss der Benutzer einen Sicherheitscode eingeben und die Mobile-App für 60 Sekunden inaktiv lassen.

Maximale Anzahl der Versuche, beim Zugriff auf die Cognos Analytics Mobile Reports -Anwendung einen Sicherheitscode einzugeben
Gibt die maximale Häufigkeit an, mit der Benutzer beim Zugriff auf die Cognos Analytics Mobile Reports -Anwendung versuchen können, ihren Sicherheitscode einzugeben.

Wert: 1 bis 99

Standardwert: 10

Benachrichtigungseinstellungen

Unterstützung für Apple-Push-Benachrichtigungen
Ermöglicht Apple-Push-Benachrichtigungen für die native iOS-App und gibt den Wortlaut der Nachricht an, die den Benutzern des iOS-Geräts angezeigt wird. Die Werte lauten wie folgt:

- Keine-Apple-Push-Benachrichtigungen sind inaktiviert, und Nachrichten werden vom Server nicht an den Apple Push-Benachrichtigungsservice gesendet.
- Name-Apple-Push-Benachrichtigungen sind aktiviert. Zu den Nachrichten, die vom Server an den Apple Push Notification Service gesendet werden, gehören der Berichtsname.
- Generisches-Apple-Push-Benachrichtigungen sind aktiviert. Die Nachrichten, die vom Server an den Apple Push Notification Service gesendet werden, enthalten nicht den Berichtsnamen. Stattdessen wird eine generische Nachricht angezeigt.

Standardwert: Name

Die folgenden Einstellungen sind veraltet:

- **Benachrichtigungs-E-Mail für Apple-Push-Benachrichtigungen**
- **Häufigkeitsprüfung für das Ablaufdatum des Apple-Push-Benachrichtigungszertifikats in Stunden**
- **Feedback-Intervall für Apple-Push-Benachrichtigungen in Stunden**
- **Ablauf-Schwellenwert für Apple-Push-Benachrichtigungen in Tagen**

Anmerkung: Diese Einstellungen wurden aus Cognos Analytics 11.1.7 IF 1034 und neueren Versionen entfernt. Diese Einstellungen sind in Versionen vor 11.1.7 IF 1034 vorhanden, aber die Einstellungen haben keine Funktionalität.

Konfiguration von Apple-Push-Benachrichtigungen für die native iOS-App

Apple-Push-Benachrichtigungen benachrichtigen die nativen iOS-App-Benutzer über die Verfügbarkeit neuer IBM Cognos Analytics -Berichte.

Um Push-Benachrichtigungen zu senden, benötigt der IBM Cognos Analytics Mobile Reports -Server ein SSL-Zertifikat von Apple. Das SSL-Zertifikat ist in jeder freigegebenen Version von Cognos Analytics Mobile Reportsenthalten und gilt für 12 Monate ab dem Datum, zu dem es von Apple ausgegeben wurde. Der Administrator muss das Verfallsdatum des Zertifikats überwachen und das Zertifikat aktualisieren, bevor es abläuft. Andernfalls werden die Push-Benachrichtigungen von den Benutzern gestoppt. Weitere Informationen finden Sie unter „Verwalten des SSL-Zertifikats für Apple-Push-Benachrichtigungen" auf Seite 414.

Die folgenden TCP-Ports werden für die Kommunikation zwischen dem Cognos Analytics Mobile Reports -Server, dem Apple iOS-Gerät und dem Apple Push Notification Service (APNS) verwendet:

- Port 2195 wird vom Cognos Analytics Mobile Reports -Server zum Senden von Benachrichtigungen an APNS verwendet.
- Port 2196 wird vom Cognos Analytics Mobile Reports -Server verwendet, um den APNS-Feedback-Service zu erreichen.
- Port 5223 wird von dem iOS-Gerät verwendet, das über WLAN mit APNS verbunden ist.

Halten Sie diese Ports in der Internet-Verbindungs-Firewall offen.

Verwalten des SSL-Zertifikats für Apple-Push-Benachrichtigungen

Der Administrator überwacht die Protokolldateien und E-Mails für Nachrichten über das Ablaufdatum des bevorstehenden Zertifikats und aktualisiert das Zertifikat bei Bedarf.

Informationen zu diesem Vorgang

Das SSL-Zertifikat für Apple-Push-Benachrichtigungen gilt für 12 Monate ab dem Datum, an dem es von Apple ausgegeben wurde. Vierzehn Tage vor dem Ablaufdatum des Zertifikats startet der IBM Cognos Analytics Mobile Reports -Server die Protokollierung von Warnungen in der Datei *Installationsposition*\logs\mob.log über das Ablaufdatum des bevorstehenden Zertifikats. Um sicherzustellen, dass die Warnungen zum Ablaufdatum des Zertifikats protokolliert werden, muss die Serverprotokollierung mindestens auf das Warnung -Niveau gesetzt werden. Wenn die Protokollierungsstufe auf Fehlergesetzt ist, werden die Ablaufnachrichten für das Zertifikat nicht protokolliert.

Zusätzlich zu den Warnungen für die Protokolldatei kann der Cognos Analytics Mobile Reports -Server auch so konfiguriert werden, dass E-Mails an Administratoren über das Ablaufdatum des bevorstehenden Zertifikats gesendet werden.

Der Text der Warnung in der Protokolldatei oder im E-Mail-Hauptteil, nur in Englisch, gibt das Ablaufdatum des Zertifikats und die URL des IBM Support-Website (http://www.ibm.com/support/) an, auf dem das neueste Cognos Analytics Mobile Reports -Fixpack mit dem aktualisierten Apple-SSL-Zertifikat verfügbar ist.

Vorgehensweise

1. Stellen Sie sicher, dass die folgenden Konfigurationseinstellungen in IBM Cognos Administration angegeben sind. Diese Einstellungen werden verwendet, um den Cognos Analytics Mobile Reports -Server so zu konfigurieren, dass E-Mail-Nachrichten an Administratoren über das Ablaufdatum des Zertifikats gesendet werden.
   - **Benachrichtigungs-E-Mail für Apple-Push-Benachrichtigungen**
   - **Häufigkeitsprüfung für das Ablaufdatum des Apple-Push-Benachrichtigungszertifikats in Stunden**
   - **Ablauf-Schwellenwert für Apple-Push-Benachrichtigungen in Tagen**

   Weitere Informationen finden Sie unter „Apple-Push-Benachrichtigungen aktivieren" auf Seite 415.
2. Überwachen Sie die Protokollnachrichten und E-Mails, um Informationen zum Ablaufdatum des Zertifikats zu erhalten.

3. Um das Zertifikat zu aktualisieren, rufen Sie die Website IBM Support (http://www.ibm.com/support) auf, und laden Sie das neueste Cognos Analytics Mobile Reports -Fixpack herunter, das ein gültiges Zertifikat für Apple-Push-Benachrichtigungen enthält.
4. Installieren Sie das neue Zertifikat auf allen betroffenen Servern.

Apple-Push-Benachrichtigungen aktivieren

Der Administrator muss die IBM Cognos Analytics Mobile Reports -Serviceeinstellungen konfigurieren, die Apple-Push-Benachrichtigungen zugeordnet sind, bevor Benutzer Push-Benachrichtigungen empfangen können.

Informationen zu diesem Vorgang

Beim ersten Mal, dass ein Push-fähiges Anwendungsregister für Push-Benachrichtigungen registriert wird, erhalten die Benutzer einen Alert, in dem sie gefragt werden, ob sie Benachrichtigungen empfangen möchten. Nachdem Sie auf diesen Alert geantwortet haben, sehen die Benutzer den Alert nicht erneut, es sei denn, ihre Einheit wird wiederhergestellt oder die Anwendung wurde mindestens für einen Tag deinstalliert. Später benachrichtigt ein Textalert den iOS-Gerätebenutzer jedes Mal, wenn ein neuer Bericht verfügbar ist, und das Anwendungssymbol wird mit der Anzahl der neuen Berichte aktualisiert. Der Benutzer kann die Anwendung von der Benachrichtigung aus öffnen.

Die native iOS-App von Cognos Analytics Mobile Reports kann Push-Benachrichtigungen von mehreren Cognos Analytics -Servern empfangen. Wenn die Benutzer keine Benachrichtigungen mehr anzeigen möchten, müssen sie die Benachrichtigungseinstellungen für die Anwendung in iOS-Einstellungen inaktivieren.

Vorgehensweise

1. Klicken Sie in IBM Cognos Administration auf die Registerkarte **Mobil** .
2. Klicken Sie auf **Serverkonfiguration**.
3. Geben Sie die folgende **Benachrichtigung** -Einstellung an:

   Unterstützung für Apple-Push-Benachrichtigungen
   Ermöglicht Apple-Push-Benachrichtigungen für die native iOS-App und gibt den Wortlaut der Nachricht an, die den Benutzern des iOS-Geräts angezeigt wird. Die Werte lauten wie folgt:

   - Keine-Apple-Push-Benachrichtigungen sind inaktiviert, und Nachrichten werden vom Server nicht an den Apple Push-Benachrichtigungsservice gesendet.
   - Name-Apple-Push-Benachrichtigungen sind aktiviert. Zu den Nachrichten, die vom Server an den Apple Push Notification Service gesendet werden, gehören der Berichtsname.
   - Generisches-Apple-Push-Benachrichtigungen sind aktiviert. Die Nachrichten, die vom Server an den Apple Push Notification Service gesendet werden, enthalten nicht den Berichtsnamen. Stattdessen wird eine generische Nachricht angezeigt.

   Standardwert: Name
4. Klicken Sie auf die Schaltfläche **Mobile Konfiguration anwenden** .
5. Geben Sie die erweiterte **`Database.DeviceExpiryIntervalDays`** -Einstellung für den Mobile-Service an. Weitere Informationen finden Sie unter „Erweiterte Einstellungen für Cognos Analytics Mobile Reports angeben“ auf Seite 407.

Berichtsverwaltung unter Cognos Analytics Mobile Reports

IBM Cognos Analytics Mobile Reports -Benutzer können gespeicherte aktive Berichtsausgaben öffnen oder aktive Berichte auf ihren mobilen Geräten abliefern. Die Benutzer können die Arbeitsbereiche von IBM Cognos ausführen.

Aktive Berichte können den Benutzern mithilfe der folgenden Methoden zugestellt werden:

- Planen von Berichten, die an die Geräte der Benutzer in bestimmten Intervallen zugestellt werden sollen.
- Verbursterte Berichte an die Geräte der Benutzer senden.
- Es wird eine Anzahl verschiedener Berichte als Job ausgeführt und an die Geräte der Benutzer gesendet.
- Ereignisse definieren, die einen Bericht auslösen, der ausgeführt und dann an die Geräte der Benutzer übergeben werden soll.

Benutzer können Berichte von ihren Einheiten löschen. Wenn sie dies tun, löschen sie nur die Kopie auf dem Gerät, nicht den eigentlichen Bericht.

Cognos Analytics Mobile Reports -Direktaufrufe auf einem mobilen Gerät

Während Sie mit IBM Cognos Analytics Mobile Reports auf Ihrem Gerät arbeiten, können Sie eine Reihe von Direktaufrufen für die Navigation verwenden und andere Aktionen ausführen.

Tabelle 80. Cognos Analytics Mobile Reports -Direktaufrufe auf einem mobilen Gerät

Aktion	**Verknüpfung**
Startseite	1
Ende	9
Nach oben	2
Nach unten	8
Links	4
Rechts	6
Eingabetaste	Öffnen
Vergrößern	F
Verkleinern	A
Zoomen	Z
Seite	P
Mark-Zelle	5

Cognos Analytics Mobile Reports -Protokollierungsfunktionen

Die Protokollierung für IBM Cognos Analytics Mobile Reports wird durch die eigenen Protokollierungsfunktionen und die Protokollierungsfunktionen in IBM Cognos Analyticsbereitgestellt.

Beide Protokollierungsmethoden erzeugen Protokolldateien, die zur Überwachung von Aktivitäten und zur Behebung von Fehlern verwendet werden. Diese Dateien befinden sich im Verzeichnis *Installationsposition*/logs . Die Konfigurationsdateien, die sich im Verzeichnis *Installationsposition*/configuration mit den Komponenten der Anwendungsschicht befinden, werden verwendet, um die Protokollierungsfunktionen von Cognos Analytics Mobile Reports zu ändern.

Beide Protokollierungsmethoden können gleichzeitig koexistieren. Beispielsweise kann der Cognos Analytics Mobile Reports -Standardprotokollierungsmechanismus verwendet werden, um die Cognos Analytics Mobile Reports -Serviceaktivität zu verfolgen, und der Protokollierungsmechanismus von Cognos Analytics kann verwendet werden, um die Tracefunktion für Debug zu aktivieren. Die Prüfprotokollierung ist nur über die Protokollierungsfunktionen von Cognos Analytics verfügbar.

Ereignisse, die dem Starten und Stoppen des Cognos Analytics Mobile Reports -Service zugeordnet sind, werden in der Cognos Analytics *Installationsposition*/logs/cogaudit.log -Datei protokolliert.

Zusätzlich zu den Protokollierungsfunktionen von Cognos Analytics Mobile Reports und Cognos Analytics können Sie die iOS-und Android-Diagnosefunktionen für die Protokollierung von Ereignissen verwenden, die mit den nativen Cognos Analytics Mobile Reports -Apps verknüpft sind.

Cognos Analytics Mobile Reports -Protokollierung

IBM Cognos Analytics Mobile Reports zeichnet Aktivitäten auf, die sich auf den Service-Start, die Konfigurationskonfiguration und die Ausführung von Berichten in der `mob.log` -Datei im Verzeichnis *`Installationsposition`*`/logs` beziehen. Dies ist der Standardtyp der Protokollierung in Cognos Analytics Mobile Reports.

Die Protokollinformationen, die in der `mob.log` -Datei angezeigt werden, werden von der *`Installationsposition`*`/configuration/mob.log4j.xml` -Datei bestimmt.

Wenn Sie die `mob.log4j.xml` -Standarddatei verwenden, kann ein Administrator den Mobile-Service für Ereignisse wie Datenbankschemaupgrades, Cognos Analytics Mobile Reports -Servicekonfigurationseinstellungen und erweiterte Einstellungsänderungen sowie Warnungen und Fehler überwachen. Die `mob.log4j.xml` -Standarddatei enthält jedoch nicht die Protokollierungsstufe `Debug` . Wenn Sie diese Stufe der Protokollierung in Ihrer `mob.log` -Datei benötigen, müssen Sie das Debugging aktivieren. Weitere Informationen finden Sie unter „Standard- Cognos Analytics Mobile Reports -Protokollierungsfunktionen für Debugstufen erhöhen" auf Seite 417.

In der folgenden Tabelle sind die Protokollierungsstufen in der Datei mob.log von der höchsten bis zur niedrigsten Ebene angegeben:

Tabelle 81. Protokollierungsstufen in mob.log

Protokollierungsstufe	**Beschreibung**
`Debug`	Stellt Debuginformationen bereit. Diese Ebene wird in der Regel für das Debugging bestimmter Probleme verwendet. Diese Version ist standardmäßig nicht verfügbar und muss aktiviert sein. Weitere Informationen finden Sie unter „Standard- Cognos Analytics Mobile Reports -Protokollierungsfunktionen für Debugstufen erhöhen" auf Seite 417.
`Info`	Stellt Informationen zu Cognos Analytics Mobile Reportsbereit.
`Warnung`	Zeigt ein verdächtiges Vorkommen an, das eine weitere Untersuchung rechtfertigen könnte.
`Fehler`	Zeigt eine schwerwiegende Fehlerbedingung an, die eine Intervention erfordert.

Die Protokollierungsstufe, die der Benutzer auswählt, enthält alle Ebenen, die darunter liegen. Wenn der Benutzer beispielsweise `Info`auswählt, werden auch Warnungen und Fehlernachrichten in die Protokolldatei geschrieben.

Standard- Cognos Analytics Mobile Reports -Protokollierungsfunktionen für Debugstufen erhöhen

Sie können die `Debug` -Protokollierungsstufe für die `mob.log` -Datei aktivieren.

Informationen zu diesem Vorgang

Die `mob.log4j.xml` -Standarddatei enthält nicht die Protokollierungsstufe `Debug` . Verwenden Sie zum Aktivieren des Debuggings die Datei *`Installationsposition`*`/configuration/mob.log4j.xml.DEBUG.sample` .

Vorgehensweise

1. Stoppen Sie den Mobile-Service in IBM Cognos Konfiguration.
2. Führen Sie im Verzeichnis *Installationsposition*/configuration die folgenden Änderungen aus:
   a) Benennen Sie mob.log4j.xml in mob.log4j.xml.originalum.
   b) Benennen Sie mob.log4j.xml.DEBUG.sample in mob.log4j.xmlum.
3. Starten Sie den IBM Cognos Analytics Mobile Reports -Service.

Ergebnisse

Die vollständige Debugprotokollierung ist jetzt für Cognos Analytics Mobile Reportsaktiviert.

Cognos Analytics -Protokollierung für Cognos Analytics Mobile Reports -Server aktivieren

IBM Cognos Analytics Mobile Reports zeichnet Aktivitäten und Debugging-Informationen sowie Informationen zu Benutzer-und Berichtsaktivitäten auf.

Informationen zu diesem Vorgang

Der Typ der Informationen, die in den Cognos Analytics Mobile Reports -Protokolldateien protokolliert werden, wird durch die Protokollierungsstufe bestimmt, die in der Datei ipfclientconfig.xml im Verzeichnis *Installationsposition*/configuration definiert ist. Das gleiche Verzeichnis enthält die Datei ipfMOBclientconfig.xml.sample . Um die Protokollierung zu aktivieren, müssen Sie ipfMOBclientconfig.xml.sample nur in ipfclientconfig.xmlumbenennen.

Die folgenden Protokollebenen können für Cognos Analytics Mobile Reportsdefiniert werden:

Tabelle 82. Cognos Analytics Mobile Reports -Protokollierungsstufen

Protokollierungsstufe	**Beschreibung**
Debug	Stellt Debuginformationen bereit. Diese Protokollebene wird normalerweise für das Debugging bestimmter Probleme verwendet.
Info	Stellt Informationen zu IBM Cognos -Services bereit.
Warnung	Zeigt ein verdächtiges Vorkommen an, das eine weitere Untersuchung rechtfertigen könnte.
Fehler	Zeigt eine schwerwiegende Fehlerbedingung an, die eine Intervention erfordert.

Die Protokollierungsstufe, die der Benutzer auswählt, enthält alle Ebenen, die darunter liegen. Wenn der Benutzer beispielsweise Infoauswählt, werden auch Warnungen und Fehlernachrichten in die Protokolldatei geschrieben.

Sie können die Protokollierung auch in der IBM Cognos Administration aktivieren. Weitere Informationen finden Sie unter „Prüfprotokollierung in IBM Cognos Administration einrichten” auf Seite 419.

Vorgehensweise

1. Stoppen Sie den Mobile-Service in IBM Cognos Konfiguration.
2. Benennen Sie ipfMOBclientconfig.xml.sample im Verzeichnis *Installationsposition*/configuration in ipfclientconfig.xmlum.

3. Öffnen Sie die Datei `ipfclientconfig.xml` , geben Sie die gewünschten Protokollstufen an, und speichern Sie die Datei.
4. Starten Sie den IBM Cognos -Service.

Ergebnisse

Abhängig von den Protokollierungsstufen, die in der `ipfclientconfig.xml` -Datei angegeben sind, werden die folgenden Protokolldateien im Verzeichnis *Installationsposition*`/logs` generiert.

- `ipf-MOB_`*xxxx*`.log`

  Diese Datei zeichnet Informationen zu Cognos Analytics Mobile Reports -Prüfereignissen auf. Wenn eine Protokollierungsdatenbank in IBM Cognos Configuration unter **Umwelt**, **Protokollierung**, definiert ist, werden die Prüfereignisse auch in dieser Datenbank protokolliert. Diese Art der Protokollierung ist in der `ipfMOBclientconfig.xml.sample` -Datei standardmäßig aktiviert.

  Informationen zum Einrichten einer Protokolldatenbank finden Sie im *IBM Cognos Analytics Installations-und Konfigurationshandbuch.* .

- `ipfMOBtrace_`*xxxx*`.log`

  Diese Datei zeichnet Cognos Analytics Mobile Reports -Trace-und Debugprotokolldaten auf. Der Typ der Daten, die in dieser Datei erfasst werden, ist mit den Daten in der Datei mob.log identisch. Diese Datei kann jedoch für eine andere Protokollierungsstufe konfiguriert werden, um mehr oder weniger Informationen aufzuzeichnen. Diese Art der Protokollierung ist in der `ipfMOBclientconfig.xml.sample` -Datei standardmäßig aktiviert.

- `ipfMOBperf_`*xxxx*`.log`

  Diese Datei zeichnet Cognos Analytics Mobile Reports -Leistungsdaten auf. Diese Art der Protokollierung ist in der `ipfMOBclientconfig.xml.sample` -Datei standardmäßig inaktiviert.

Prüfprotokollierung in IBM Cognos Administration einrichten

Verwenden Sie Prüfprotokolle, um Informationen zu IBM Cognos Analytics Mobile Reports -Benutzer-und -Berichtsaktivitäten anzuzeigen.

Informationen zu diesem Vorgang

Beispiele für Aktionen, die in Prüfprotokollen aufgezeichnet werden, umfassen Benutzeranmelde-und Abmeldezeiten, abgelaufene Benutzersitzungen, terminierte Berichtszustellung, gespeicherte Ausgabe usw.

Sie können die Prüfprotokollierung auch in der *Installationsposition*`/configuration/ipfclientconfig.xml` -Datei aktivieren. Weitere Informationen finden Sie unter „Cognos Analytics -Protokollierung für Cognos Analytics Mobile Reports -Server aktivieren" auf Seite 418.

Weitere Informationen zu Prüfberichten finden Sie im *IBM Cognos Analytics Administration and Security Guide*. Dieses Dokument enthält auch Informationen zu den Beispielprüfberichten von Cognos Analytics Mobile Reports .

Vorgehensweise

1. Öffnen Sie Cognos Administration.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Dispatcher und Services**.
3. Klicken Sie auf den Namen des Dispatchers.
4. Suchen Sie in der Liste der Dispatcher-Services den **MobileService**, und klicken Sie in der Spalte **Aktionen** auf das Symbol **Eigenschaften festlegen** .
5. Klicken Sie auf die Registerkarte **Einstellungen** und wählen Sie unter **Kategorie**den Eintrag **Protokollierung**aus.

6. Wählen Sie für **Prüfprotokollebene für mobilen Service**einen beliebigen Wert mit Ausnahme von **Minimal**aus.

   Die folgenden Protokollebenen können angegeben werden, um die Prüfprotokollierung zu aktivieren: **Basis**, **Anforderung**, **Trace**und **Voll**. Die Protokollierungsstufe **Minimal** inaktiviert die Prüfprotokollierung.
7. Klicken Sie auf **OK**.
8. Um den Wert anzuwenden, stoppen Sie den IBM Cognos -Service und starten Sie ihn erneut.

Benutzerdiagnose

Benutzer können die Anmeldung in ihren nativen iOS-und Android-Apps aktivieren und inaktivieren und die Menge der erfassten Protokollierungsdetails auswählen.

Die folgende Liste zeigt die unterstützten Protokollstufen, von der höchsten bis zur niedrigsten Ebene:

· Netz

· Debug

· Info

· Warnung

· Fehler

Die Protokollierungsstufe, die der Benutzer auswählt, enthält alle Ebenen, die darunter liegen. Wenn der Benutzer z. B. "Info" auswählt, werden auch Warnungen und Fehlernachrichten in die Protokolldatei geschrieben.

Die maximale Größe einer protokollierten Nachricht beträgt 2 KB. Wenn eine Nachricht diese Größe überschreitet, wird sie abgeschnitten.

iOS-Anwendungen

Wenn die Protokollierung aktiviert ist, wird ein Verzeichnis mit dem Namen `SupportArtifacts` im Verzeichnis der Anwendungsdokumente erstellt. Eine Datei mit dem Namen `mobile_ios.log` wird im Verzeichnis `SupportArtifacts` erstellt. Alle protokollierten Ereignisse werden in diese Datei geschrieben.

Die maximale Größe einer aktiven Protokolldatei beträgt 1 MB. Wenn diese Größe erreicht ist, wird der Inhalt der aktiven Protokolldatei in eine Datei mit dem Namen `mobile_ios.log.alt`verschoben. Wenn eine `mobile_ios.log.alt` -Datei vorhanden ist, wird sie zuerst entfernt. Eine neue `mobile_ios.log` -Datei wird erstellt und wird zur aktiven Protokolldatei.

Wenn die Protokollierung inaktiviert ist, werden das Verzeichnis und der gesamte Inhalt aus dem Verzeichnis der Anwendungsdokumente entfernt.

Android-Anwendungen

Wenn die Protokollierung aktiviert ist, wird ein Verzeichnis mit dem Namen `SupportArtifacts` im Verzeichnis `/Android/data/com.ibm.cogmob.artoo/files` erstellt. Eine Datei mit dem Namen `cogmob.log` wird im Verzeichnis `SupportArtifacts` erstellt. Alle protokollierten Ereignisse werden in diese Datei geschrieben.

Die maximale Größe einer aktiven Protokolldatei beträgt 1 MB. Wenn diese Größe erreicht ist, wird der Inhalt der aktiven Protokolldatei in eine Datei mit dem Namen `cogmob.log.old`verschoben. Wenn die Datei `cogmob.log.old` bereits vorhanden ist, wird sie zuerst entfernt. Eine neue `cogmob.log` -Datei wird erstellt und wird zur aktiven Protokolldatei.

Wenn die Protokollierung inaktiviert ist, werden das Verzeichnis und der gesamte Inhalt aus dem Verzeichnis der Anwendungsdokumente entfernt.

Cognos Analytics Mobile Reports -Beispiele

Die IBM Cognos Analytics -Beispiele enthalten aktive Berichte, die für die Verwendung mit IBM Cognos Analytics Mobile Reports auf einem mobilen Gerät optimiert wurden.

Cognos Analytics Mobile Reports -Benutzer können die interaktive Funktionalität aktiver Berichte testen. Diese Berichte ermöglichen es den Benutzern, verschiedene Bereiche ihres Geschäfts miteinander zu vergleichen, um Trends zu ermitteln, z. B. im Laufe der Zeit, nach Regionen, nach Abteilungen oder in Kombination, oder um Geschäftsmethoden und Statistiken zu vergleichen.

Cognos Analytics Mobile Reports -Beispielaktive Berichte veranschaulichen die folgenden Produktmerkmale.

- Interaktives Verhalten zwischen Steuerelementen.
- Zugriff auf Details on Demand durch Nutzung der Drill-down-Funktionalität.
- Bedingte Palette und Drilldown zu Details aus einem Diagramm.
- Spezifische Gesten für das Design von Tablet-PCs, wie zum Beispiel das Schwicken und Scrollen.
- Besondere Benutzeroberflächengestaltung, wie z. B. Deckblatt und Farbpalette.
- Verschiedene Arten von aktiven Berichtselementen, wie z. B. Deck, Registerkartensteuerung, Diagramm, Schaltflächen, Dropdown-Liste, Iterator und Slider

Paket 'GO Data Warehouse (Analyse)'

Das Package "AUF Data Warehouse (Analyse)" enthält die folgenden aktiven Berichte.

Ergebnisse der Kernprodukte
Dieser aktive Bericht zeigt Umsatzdaten für die Kernprodukte Camping Equipment und Golf Equipment an.

Finanzbericht
Dieser aktive Bericht zeigt die aktuelle Leistung und die Veränderungen in der Finanzlage eines Unternehmens. Diese Art von Informationen ist für alle Benutzer nützlich, die an der Entscheidungsfindung von Geschäftsentscheidungen beteiligt sind. Die Finanzabteilung wird jedoch höchstwahrscheinlich von diesen Informationen profitieren, wenn sie die Kontrollen und Kontrollen im System durchführen, um die Rechts-, Steuer-und Rechnungslegungsvorschriften und -anforderungen zu erfüllen, und wenn sie Ratschläge für zukünftige Richtungen, Leistung und Chancen für das Unternehmen geben. Dieser Bericht ist für Tablets optimiert.

Bericht über Bestandsumsatz
Dieser aktive Bericht zeigt Informationen zum Umsatz des regionalen Produktbestands auf der Grundlage von zwei Jahren vergleichbarer Daten an. Der Bericht stellt wichtige Bestandsmetriken bereit, die ein Unternehmen zur Verwaltung seines Bestands verwenden kann. Sie können für jede Produktkategorie einen Drilldown durchführen, um die detaillierten Bestandsinformationen und die Anzahl der fehlgeschlagenen Bestellungen im Zusammenhang mit dem Bestand anzuzeigen. Dieser Bericht ist für Tablets optimiert.

Verkaufsziel nach Region
Dieser aktive Bericht zeigt das Verkaufsziel nach Region an, einschließlich der prozentualen Unterschiede zwischen geplanten und tatsächlichen Einnahmen.

Paket 'AUF Data Warehouse (Abfrage)'

Das Paket "AUF Data Warehouse (Abfrage)" enthält die folgenden aktiven Berichte.

Werbung-Kosten vs. Einnahmen
Dieser aktive Bericht zeigt die Werbekosten gegenüber dem Umsatz im Jahr. Registerkartensteuerelemente werden für die Gruppierung ähnlicher Berichtselemente verwendet.

Kundenzufriedenheit
In diesem aktiven Bericht wird die Anzahl der Rückgaben nach Bestellmethode und Region durch Kunden verglichen. Der Bericht enthält zusätzliche Informationen über die Bestellmethode mit der

höchsten Anzahl an Rückgaben. Darüber hinaus werden die Ergebnisse der Kundenbefragung für verschiedene Regionen angezeigt. Dieser Bericht ist für Tablets optimiert.

Mitarbeiterrekrutierung
Dieser aktive Bericht vergleicht die Effektivität verschiedener Personalbeschaffung-Methoden für jede Abteilung und jedes Land oder jede Region. Er zeigt die Namen der Organisation, die Positionen, die besetzt sind, die geplanten Positionen und eine bulletendiagramm der Positionen, die mit den geplanten Positionen gefüllt sind. Dieser Bericht ist für Tablets optimiert.

Einnahmen nach Produkt
Dieser aktive Bericht zeigt die Einnahmen des ausgewählten Produkts an. Dieser Bericht ist für Mobiltelefongeräte optimiert.

Sicherheit für Cognos Analytics Mobile Reports

IBM Cognos Analytics Mobile Reports kombiniert die Sicherheitskennzahlen von IBM Cognos Analytics mit den zusätzlichen Maßnahmen, die für mobile Geräte erforderlich sind.

Die Sicherheitsvorkehrungen bieten Schutz vor Verlust und Diebstahl und gegen unberechtigten Zugriff auf das drahtlose Netzwerk. Die Sicherheit gilt, ob die Einheit im Modus 'Verbunden' oder 'Nicht verbunden' verwendet wird.

Die Cognos Analytics Mobile Reports -Lösung umfasst die folgenden Sicherheitsmaßnahmen, die in den IBM Cognos und einheitenspezifischen Umgebungen implementiert sind:

- Standarddatenverschlüsselung für IBM Cognos
- Standard- IBM Cognos -Authentifizierung, einschließlich Unterstützung für angepasste IBM Cognos -Authentifizierungsprovider
- PKCS12-Zertifikate
- Leasing-Schlüsseltechnologie
- Authentifizierungsrichtlinien für Einheitenbenutzer
- Einheitenbasierte mobile verschlüsselte Datenbank
- Standardgerätespezifische sichere Datenübertragung und Verschlüsselung
- Einheitenbasierter Kennwortschutz
- Abwischen der fernen Einheit

Cognos Analytics Mobile Reports unterstützt Web-Server, die für die Verwendung der Basisauthentifizierung konfiguriert sind, wie z. B. Microsoft Fenster NTLM, Microsoft Active Directory und einige Konfigurationen von CA SiteMinder. Mit diesen Authentifizierungstypen kann eine Anwendung Benutzerberechtigungsnachweise zwischenspeichern, wenn der Administrator die Cacheoption für den Benutzerberechtigungsnachweis aktiviert. Für alle anderen Authentifizierungstypen, wie z. B. die HTML-Serverantwortseite, zeigt die Anwendung eine Seite an, die es dem Benutzer ermöglicht, mit der Seite zu interagieren, wie vom Authentifizierungsprovider beabsichtigt.

Anmerkung: Für Single-Sign-on-Sicherheitskonfigurationen ist die Cacheoption für den Benutzerberechtigungsnachweis nicht verfügbar.

Cognos Analytics Mobile Reports unterstützt die Single Sign-on-Sicherheitskonfiguration. In der Regel werden Benutzer von mobilen Geräten jedoch nicht vor Sicherheitsdomänen so vorauthentifiziert, wie es für Desktopbenutzer erforderlich ist. Daher müssen Benutzer von mobilen Geräten in der Regel bei jedem Zugriff auf den Cognos Analytics -Server ihre Single Sign-on-Berechtigungsnachweise angeben.

Wichtig: Die iPad-Anwendung von Cognos Analytics Mobile Reports unterstützt auch Single-Sign-on-Sicherheitskonfigurationen. Benutzer können die einmalige Anmeldung von ihrem iPad **Einstellungen** aktivieren, indem sie die Einstellung **Durchgriffsauthentifizierung** für die Anwendung IBM Cognos aktivieren. Wenn diese Einstellung aktiviert ist, werden die iPad-Benutzer bei jedem Zugriff auf den Cognos Analytics -Server aufgefordert, Berechtigungsnachweise für die Anmeldung zu verwenden.

In einigen Fällen können Anmeldeberechtigungsnachweise auf dem mobilen Gerät zwischengespeichert werden, so dass sich der Benutzer nur einmal anmelden muss, um auf die Einheit und auf Cognos Analytics Mobile Reportszuzugreifen.

Anmerkung: Berechtigungsnachweise können nur zwischengespeichert werden, wenn die Einstellung **Durchgriffsauthentifizierung** inaktiviert ist. Für Single-Sign-on-Sicherheitskonfigurationen ist daher die Option für den Cache der Benutzerberechtigungsnachweise nicht verfügbar.

Cognos Analytics Mobile Reports bietet eine verschlüsselte Datenbanktechnologie als Content-Store auf dem Gerät. Der Zugriff auf den lokalen Einheitenspeicher wird durch einen zentral erteilten Leasingschlüssel gesteuert, der regelmäßig erneuert werden muss. Sie können die Länge des Leasingverhältnisses konfigurieren, sodass die Daten nicht zugänglich sind, wenn das Gerät verloren geht oder gestohlen wird.

Abhängig von den Anforderungen Ihrer Organisation können Sie unterschiedliche Sicherheitsstufen haben. Zusätzlich zum Speichern von Anmeldeberechtigungsnachweisen auf dem Gerät können Sie eine anonyme Anmeldung zulassen oder sich auf die Netzsicherheitsfunktionen des mobilen Geräts verlassen.

Für eine höhere Sicherheitsstufe können Sie die Sicherheit von Cognos für alle Kommunikation verwenden oder die Leasingschlüsseltechnologie verwenden, um den Zugriff auf Daten zu steuern.

Informationen zur Cognos Analytics -Sicherheit finden Sie im Artikel Kapitel 10, „Sicherheitsmodell”, auf Seite 181. Informationen zur Einheitensicherheit finden Sie in der Dokumentation zu dieser Einheit.

Funktionen von Cognos Analytics Mobile Reports

Die Funktionen von IBM Cognos Analytics Mobile Reports in IBM Cognos Administration werden verwendet, um den Zugriff auf Cognos Analytics Mobile Reports für Benutzer und Administratoren zu beschränken.

Tipp: Die Funktionen von IBM Cognos Analytics werden auch als gesicherte Funktionen und Features bezeichnet.

Zu den Cognos Analytics Mobile Reports -Funktionen gehören:

- **Mobil**

  Diese geschützte Funktion wird verwendet, um den Zugriff auf Cognos Analytics Mobile Reports für Benutzer zu beschränken. Nur Benutzer, Gruppen oder Rollen, die über Ausführungsberechtigungen für diese geschützte Funktion verfügen, können sich bei Cognos Mobile anmelden. Wenn Benutzer, die nicht über die erforderlichen Berechtigungen verfügen, versuchen, sich anzumelden, wird eine Fehlernachricht angezeigt, in der sie aufgefordert werden, sich an einen Cognos Analytics -Administrator zu wenden.

- **Mobile Administration**

  Diese geschützte Funktion der gesicherten Funktion **Verwaltung** wird verwendet, um den Zugriff auf die Verwaltungsseiten auf der Registerkarte **Mobil** in der Verwaltung von Cognos zu beschränken. Nur Benutzer, Gruppen oder Rollen, die über Ausführungsberechtigungen für diese geschützte Komponente verfügen, können auf diese Registerkarte zugreifen, um Verwaltungstasks, wie z. B. die Konfiguration des Mobile-Service, für Cognos Analytics Mobile Reportsauszuführen.

Um den Prozess zum Festlegen von Zugriffsberechtigungen für die Funktionen von **Mobil** und **Mobile Administration** zu vereinfachen, können Sie die vordefinierten Rollen **Mobile Benutzer** und **Mobile Adminsitrator** verwenden, die im **Cognos** -Namespace in der Cognos -Verwaltung vorhanden sind. Die Rolle **Mobile Benutzer** enthält Berechtigungen, die für den Zugriff auf Cognos Analytics Mobile Reports für reguläre Benutzer erforderlich sind. Die Rolle **Mobile Adminsitrator** enthält Berechtigungen, die für den Zugriff auf Verwaltungsfunktionen von Cognos Analytics Mobile Reports auf der Registerkarte **Mobil** in der Cognos -Verwaltung erforderlich sind. Sie können Benutzer, Gruppen oder Rollen aus Ihrem Organisationsverzeichnis zu diesen Rollen hinzufügen und diese Rollen in Ihre Cognos Analytics -Sicherheitsrichtlinien aufnehmen. Sie können diese Rollen auch ignorieren oder löschen und Ihre eigenen Sicherheitsgruppen oder Rollen erstellen, die für das Festlegen von Zugriffsberechtigungen für Cognos Analytics Mobile Reportsverwendet werden sollen.

Das Festlegen von Zugriffsberechtigungen für die Funktionen von **Mobil** und **Mobile Administration** ist eine der ersten Tasks, die ein Administrator ausführen muss, wenn Cognos Analytics Mobile Reportskonfiguriert wird. Weitere Informationen finden Sie unter Kapitel 13, „Funktionen”, auf Seite 207.

Kennwortschutz

In der Regel möchten Unternehmen den Kennwortschutz auf mobilen Geräten.

Nach einer bestimmten Inaktivitätszeit werden Benutzer aufgefordert, ihr Einheitenkennwort erneut einzugeben, und es kann eine Begrenzung geben, wie oft sie versuchen können, ein Kennwort einzugeben. Wenn der Grenzwert erreicht ist, wird das mobile Gerät zurückgesetzt, und es werden alle Daten aus der Einheit entfernt. Der Benutzer muss dann die entsprechenden Aktionen ausführen, um die Daten auf dem Gerät wiederherzustellen.

Sie können IBM Cognos -Berechtigungsnachweise für Benutzer auf ihren mobilen Geräten speichern, damit sie ihre Berechtigungsnachweise nur zum ersten Mal eingeben müssen, wenn sie auf IBM Cognos Analytics Mobile Reportszugreifen. Danach werden sie immer noch für ihre Berechtigungsnachweise gefragt, wenn sie sich anmelden, Cognos Analytics Mobile Reports aber automatisch ihre Kennwörter für sie eingibt. Nur wenn der Zeitgrenzwert für die gespeicherten Berechtigungsnachweise erreicht ist, müssen die Benutzer ihre Berechtigungsnachweise erneut eingeben.

Wenn eine Geräte-PIN auf einem iOS-Gerät konfiguriert ist, verschlüsselt Cognos Analytics Mobile Reports die manuell importierten aktiven Cognos -Berichte, die auf dem Gerät gespeichert sind. Diese Funktion gilt für aktive Berichte, die manuell über E-Mail, iTunes oder einen Dateiserver importiert werden.

Informationen zum Aktivieren oder Festlegen von Kennwortrichtlinien für ein mobiles Gerät finden Sie in der Dokumentation für das Gerät.

HTML-und HTTP-Unterstützung während der Anmeldung

Das IBM Cognos Analytics Mobile Reports -Produkt, das auf mobilen Geräten verwendet wird, ist eine native Anwendung, im Gegensatz zu einer Webanwendung. Es verwendet keinen Webbrowser und verwendet keine HTML, um Berichte auf mobilen Geräten anzuzeigen.

Cognos Analytics Mobile Reports verwendet jedoch HTTP für die Kommunikation mit dem IBM Cognos Analytics -Server. Daher muss es mit allen webbasierten Sicherheitsmechanismen, die den Zugriff auf den Cognos Analytics -Server steuern, zusammenarbeiten. Um Benutzern die Authentifizierung und Navigation durch diese Sicherheitsmechanismen zu ermöglichen, zeigt Cognos Analytics Mobile Reports grundlegende HTML-Formularelemente an und ermöglicht dem Benutzer die Ausführung der zugehörigen Aktionen.

In der folgenden Tabelle sind die HTTP-und HTML-Funktionen aufgeführt, die von Cognos Analytics Mobile Reportsunterstützt werden.

Tabelle 83. Von Cognos Analytics Mobile Reports unterstützte HTTP-und HTML-Funktionen

Funktion	**Beschreibung**
HTTP-Umleitungen	Unterstützt HTTP 301, das permanent verschoben wurde, und HTTP 302 wurde vorübergehend verschoben. Er folgt sowohl relativen als auch absoluten URLs, die im Header "Location" angegeben sind.
HTML-Umleitungen	Unterstützt das HTML-Äquivalent einer HTTP-Umleitung, zum Beispiel < meta http-equiv="Refresh " content="3; URL=http:// ... ">.
HTTP-Authentifizierung	Unterstützt HTTP 401 Unberechtigt sowohl mit dem Basisschema als auch mit NTLM. Bei NTLM handelt es sich überwiegend um ein Microsoft -Authentifizierungsschema, das auch als Fenster Integrated Authentication bezeichnet wird.

Tabelle 83. Von Cognos Analytics Mobile Reports unterstützte HTTP-und HTML-Funktionen (Forts.)	
Funktion	**Beschreibung**
HTML-Formulare	Zeigt den Text einer HTML-Seite (einschließlich Text mit Ankertags), Schaltflächen und dem Eingabefeldtyp Text, Kennwort und Verborgenes an. Außerdem wird der ausgewählte Eingabetyp angezeigt, der verwendet wird, um eine Liste der Elemente anzuzeigen, aus denen Sie auswählen können, z. B. eine Liste mit Sicherheitsnamensbereichen.

Zertifikatsauthentifizierung

Wenn Ihr Web-Server so konfiguriert ist, dass eine Clientzertifikatsauthentifizierung erforderlich ist, können Sie ein Client-SSL-Zertifikat (Client-X509v3-Zertifikat) verwenden, um eine nahtlose Anmeldung und sichere Kommunikation zwischen dem IBM Cognos Analytics -Server und den nativen Apps zu ermöglichen.

Tipp: Diese Art der Authentifizierung wird auch als bidirektionale SSL-Authentifizierung oder gegenseitige Authentifizierung bezeichnet.

Die Zertifikatsdatei muss im PKCS12-Format (Erweiterung .pkcs12) enthalten sein und muss die Identität des Clients in Form eines Zertifikats und eines privaten Schlüssels enthalten. Ein Administrator muss einen sicheren Mechanismus zum Importieren der Zertifikatsdatei in die nativen Apps einrichten und den Benutzern das Zertifikatskennwort angeben, damit sie beim Importieren des Zertifikats in das Zertifikat eingegeben werden können.

Ein Administrator kann die folgenden Mechanismen bereitstellen, um das Client-SSL-Zertifikat für iOS- und Android-Apps von IBM Cognos Analytics Mobile Reports zu importieren:

- Ein Link zu der Zertifikatsdatei von einer Website.

  Ein Administrator muss die Benutzer auf eine Website richten, die einen Link zur .pkcs12-Datei enthält. Benutzer tippen auf den Link, um die Datei in die App zu importieren. Auf Android-Geräten werden die Benutzer aufgefordert, die Datei zu speichern.

- Eine E-Mail mit der angehängten Zertifikatsdatei.

  Benutzer müssen die angehängte .pkcs12-Datei herunterladen. Auf Android-Geräten werden die Benutzer aufgefordert, die Datei zu speichern.

- Kopieren der Zertifikatsdatei auf die Einheit.

  In diesem Szenario wird das mobile Gerät an einen Personal Computer angeschlossen. Für Android kann die .pkcs12-Datei manuell vom Personal Computer kopiert werden, zu dem ein Administrator die Datei sicher versorgt, an das mobile Gerät. Für iOS kann der Administrator oder Benutzer die .pkcs12-Datei über iTunes bereitstellen, indem er die Datei in den Ordner **IBM Cognos-Dokumente** stellt.

  Diese Methode ist nicht skalierbar und nützlich, um nur einmalige Probleme zu lösen oder einmalige Setups durchzuführen.

Wenn Sie die .pkcs12-Datei auf ihren mobilen Geräten auswählen, müssen Benutzer **IBM Cognos Analytics Mobile Reports** im Dialogfeld **Öffnen mit** auswählen. Die Benutzer werden dann zur Eingabe des Kennworts aufgefordert, das der Datei '.pkcs12' im Dialogfeld **Clientzertifikat** zugeordnet ist. Nachdem die App geöffnet wurde, wird das Zertifikat im Kennwortspeichersystem, wie z. B. Keychain auf iOS-Geräten, auf dem mobilen Gerät des Benutzers gespeichert.

Tipp: Wenn die Gmail-App nicht in der Lage ist, ein PKCS12-Zertifikat zu öffnen, besteht bei Android eine mögliche Ausweichlösung darin, einen anderen Mail-Client zu verwenden, wie z. B. die Standard-E-Mail-App. Wenn dies nicht möglich ist, kann mit der Erweiterung .p12 die App die App ordnungsgemäß importieren. Wenn Sie ein Zertifikat über einen Hyperlink importieren, sollte die Erweiterung .pkcs12 verwendet werden.

Cognos Analytics Mobile Reports -Anwendungssicherheit

Ein Sicherheitscode kann verwendet werden, um den Zugriff auf die IBM Cognos Analytics Mobile Reports -App für Benutzer von iOS-und Android-Geräten zu beschränken.

Der Cognos -Administrator kann angeben, dass ein Benutzer eines mobilen Geräts einen Sicherheitscode eingeben muss, um auf die App Cognos Analytics Mobile Reports zuzugreifen, und die Zeit, die die Cognos Analytics Mobile Reports -App inaktiv sein kann, bevor der Benutzer den Code erneut eingeben muss, um die App zu verwenden. Diese Funktionalität wird durch die Konfigurationseinstellung von **Zeitlimit für Sicherheitscode-Sitzung** gesteuert.

Wenn der Wert dieser Einstellung angibt, dass der Benutzer einen Sicherheitscode benötigt, stellt dieser Wert auch die Anzahl der Sekunden dar, die die Cognos Analytics Mobile Reports -App inaktiv bleiben kann, bevor der Benutzer zum erneuten Eingeben des Sicherheitscodes aufgefordert wird, um auf die App Cognos Analytics Mobile Reports zuzugreifen.

Zusätzlich zu dieser Einstellung gibt es auch einen Standardzeitlimitwert, der in den nativen Cognos Analytics Mobile Reports -Apps enthalten ist. Der Wert, den Sie für die Servereinstellung angeben, überschreibt den Standardwert in der App.

Die Benutzer können die Servereinstellung auf ihren mobilen Geräten ausschalten, aber sie können ihren Wert nicht ändern. Wenn die Einstellung inaktiviert ist, die Servereinstellung jedoch erfordert, dass der Benutzer einen Sicherheitscode verwendet, muss er das nächste Mal, wenn der Benutzer versucht, die App auszuführen, mit dem Server eine erneute Authentifizierung durchführen und wird aufgefordert, einen Sicherheitscode zu erstellen. Ohne diesen Code können die Benutzer keine lokalen Inhalte sehen.

Der Cognos -Administrator kann auch einen Grenzwert für die Anzahl der fehlgeschlagenen Versuche festlegen, den Sicherheitscode einzugeben, wenn Sie sich an den Cognos Analytics Mobile Reports -Apps anmelden. Dies wird durch die Konfigurationseinstellung **Maximale Anzahl der Versuche, beim Zugriff auf die Cognos Analytics Mobile Reports -Anwendung einen Sicherheitscode einzugeben** gesteuert. Wenn der Benutzer die maximale Anzahl an Versuchen überschreitet, werden alle Cognos -Inhalte auf ihren mobilen Einheiten gelöscht. Wenn der Benutzer eine PIN für den Zugriff auf den Server benötigt, überschreibt die Anzahl der vom Server angegebenen Wiederholungsversuche den Wiederholungswert auf dem mobilen Gerät.

Weitere Informationen finden Sie in den Sicherheitseinstellungen in „Einstellungen für Cognos Analytics Mobile Reports -Service-Konfigurationen” auf Seite 411.

Berichtsdatensicherheit in IBM Cognos Analytics Mobile Reports

Alle kompilierten und komprimierten Versionen von IBM Cognos Analytics -Berichten werden verschlüsselt und lokal in der mobilen verschlüsselten Datenbank des mobilen Geräts gespeichert. Diese Berichte können nur von der IBM Cognos Analytics Mobile Reports -Clientanwendung gelesen oder anderweitig interpretiert werden.

Sie können die Leasingschlüsseltechnologie verwenden, um eine Ablaufzeit für Berichtsdaten festzulegen, die auf dem mobilen Gerät gespeichert werden. Nach Ablauf der Ablaufzeit können die Berichtsdaten auf dem Gerät erst dann abgerufen werden, wenn die Einheit die Kommunikation mit dem Server wieder herstellen kann und der Benutzer sich mit dem Server erneut authentifizieren kann.

Wenn eine Geräte-PIN auf einem iOS-Gerät konfiguriert ist, verschlüsselt Cognos Analytics Mobile Reports die manuell importierten aktiven Cognos -Berichte, die auf dem Gerät gespeichert sind. Diese Funktion gilt für aktive Berichte, die manuell über E-Mail, iTunes oder einen Dateiserver importiert werden.

Inhalt von einer Einheit löschen

Möglicherweise müssen Sie alle Inhalte von einem mobilen Gerät löschen. Dies kann notwendig sein, wenn ein Gerät verloren geht oder gestohlen wird oder ein Mitarbeiter Rollen wechselt oder das Unternehmen verlässt.

Durch Gerätekennwörter und Leasingschlüsseltechnologie wird sichergestellt, dass Inhalte nur berechtigten Benutzern zur Verfügung stehen. Für alle Geräte werden Sicherheit und Management durch mobile Endgeräte-Management-Lösungen von Drittanbietern abgewickelt.

Wenn IBM Cognos Analytics Mobile Reports für einen bestimmten Zeitraum nicht mit dem Server verbunden ist, werden die Daten von IBM Cognos auf der Basis der in der **Maximale Anzahl Stunden für den Zugriff auf mobile lokale Daten, die auf einer Einheit gespeichert sind** -Konfigurationseinstellung angegebenen Stunden von der Einheit nicht zugänglich. Weitere Informationen zu den Konfigurationseinstellungen finden Sie unter „Einstellungen für Cognos Analytics Mobile Reports -Service-Konfigurationen" auf Seite 411.

Leasingschlüssel festlegen

Cognos Analytics Mobile Reports verwendet das Konzept eines Leasingvertrags, um den Zugriff auf Daten zu steuern, die auf mobilen Geräten gespeichert sind.

Data is leased from the server for a length of time controlled by the IBM Cognos administrator through the server setting named **Maximale Anzahl Stunden für den Zugriff auf mobile lokale Daten, die auf einer Einheit gespeichert sind**. Diese Einstellung gibt die maximale Zeit an, die ein Benutzer auf Daten auf einer mobilen Einheit zugreifen kann, die nicht mit dem Server in Kontakt steht. Das Gerät ist beispielsweise offline oder außerhalb des Funkbereichs. Wenn die Einheit innerhalb des angegebenen Zeitraums nicht mehr in der Lage ist, ihren Mietvertrag zu verlängern, werden die Daten auf dem Gerät nicht mehr zugänglich. Der gültige Wertebereich für diese Einstellung ist in Stunden 0 bis 8760. Der Standardwert ist 36 Stunden. Der Wert 0 inaktiviert den Leasingschlüsselmechanismus. Informationen zur Angabe dieser Einstellung finden Sie im Artikel „Cognos Analytics Mobile Reports -Services konfigurieren" auf Seite 410.

Benutzerauthentifizierungsrichtlinien für ein mobiles Gerät festlegen

Cognos Analytics Mobile Reports device user authentication policies define whether IBM Cognos Analytics authentication credentials are cached on the mobile device and how often users must reenter these credentials. Benutzer müssen ihre Berechtigungsnachweise mindestens einmal eingeben.

Alle IBM Cognos Analytics -Zeitlimitüberschreitungen gelten für den Benutzer des mobilen Geräts. Die Richtlinien für die Benutzerauthentifizierung des Geräts befinden sich auf der Oberseite von Zeitlimitüberschreitungen, die IBM Cognos Analyticszugeordnet sind.

Um den Authentifizierungsprozess für den Benutzer zu vereinfachen, kann der Administrator von IBM Cognos zulassen, dass Berechtigungsnachweise auf dem mobilen Gerät mithilfe der Einstellung **Maximale Anzahl Stunden zum Speichern zwischengespeicherter Berechtigungsnachweise**zwischengespeichert werden. Der Wertebereich für diese Einstellung ist in Stunden 0 bis 8760. Der Standardwert 0 bedeutet, dass Berechtigungsnachweise nicht auf einer Einheit gespeichert werden sollen. Informationen zur Angabe dieser Einstellung finden Sie im Artikel „Cognos Analytics Mobile Reports -Services konfigurieren" auf Seite 410.

Die Einstellung für den CAM (IBM Cognos -Sicherheitssteuerungsmechanismus) in IBM Cognos Analytics gilt für alle Einheiten. Wenn der Grenzwert für die Passeinstellung abgelaufen ist, wird die Benutzersitzung beendet. Wenn jedoch das Zeitlimit für die Einheitenberechtigung das Zeitlimit überschreitet, das die Sitzung beendet hat, bleibt das Zeitlimit für die Einheitenberechtigung bestehen, nachdem die Benutzersitzung beendet wurde. Nur wenn das Zeitlimit für die Einheitenauthentifizierung erreicht ist, müssen die Benutzer ihre Berechtigungsnachweise erneut eingeben.

Vorgehensweise

Verwenden Sie die folgende Prozedur, um das Zeitlimit für den CAM-Pass festzulegen.

1. Öffnen Sie **IBM Cognos-Konfiguration** auf dem Computer, auf dem IBM Cognos Content Manager installiert ist.
2. Klicken Sie im Teilfenster **Explorer** auf **Explorer** > **Authentifizierung**.
3. Geben Sie im Teilfenster ' **Eigenschaften** ' für **Inaktivitätszeitlimit in Sekunden**den erforderlichen Wert ein.

Weitere Informationen zur Konfiguration von IBM Cognos finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Anhang A. Funktionen zur behinderten

IBM Cognos Administration verfügt über Funktionen zur behindertengerechten Bedienung, die Benutzern mit einer körperlichen Behinderung, wie z. B. eingeschränkter Mobilität oder eingeschränktem Sehvermögen, bei der Verwendung von Informationstechnologieprodukten helfen.

Die Verfügbarkeit von Funktionen zur behindertengerechten Bedienung kann jedoch unterschiedlich sein, wenn andere Seiten und Komponenten, die die behindertengerechte Bedienung nicht unterstützen, der Benutzerschnittstelle von Cognos Administration hinzugefügt werden.

Weitere Informationen zu der Zusage, die IBM für die behindertengerechte Bedienung hat, finden Sie in der Veröffentlichung IBM Accessibility Center (http://www.ibm.com/able).

Die folgenden Funktionen unterstützen die behindertengerechte Bedienung in Cognos Administration:

- Um zu hören, was auf dem Bildschirm angezeigt wird, können Personen mit eingeschränktem Sehvermögen Sprachausgabeprogramme verwenden, zusammen mit einem digitalen Sprachsynthesizer. Cognos Administration verwendet Web Accessibility Initiative-Accessible Rich Internet Applications (WAI-ARIA).
- Um in der Software zu navigieren und Befehle mit nur einer Tastatur auszugeben, können Sie die StandardTastaturkurzbefehle von Microsoft Fenster verwenden. Es gibt keine eindeutigen Direktaufrufe für die Tastatur.
- Um Links in Kopfzeilen und Menüs zu umgehen und direkt zum Hauptinhalt der Seite zu gelangen, können JAWS-Benutzer den Link **Zu Haupt springen** in der Liste der Links auswählen. Tastaturbenutzer sehen die Option **Zu Haupt springen** , wenn sie zu ihr navigieren.
- Administratoren können systemweite Einstellungen für die zugängliche Berichtsausgabe angeben, die für alle Einträge gelten.
- Die zugängliche Ausgabe kann auch für einzelne Berichte, Jobs, Schritte innerhalb von Jobs und geplante Einträge in den Softwareformaten PDF, HTML und Microsoft Excel 2007 festgelegt werden.

Systemweite zugängliche Berichtsausgabe aktivieren

Sie können systemweite Einstellungen für die zugängliche Berichtsausgabe angeben, die für alle Einträge gelten, einschließlich Berichte, Jobs und geplante Einträge.

Zugängliche Berichte enthalten Features, wie z. B. Alternativtext, die Benutzern mit Behinderungen den Zugriff auf Berichtsinhalte mit Hilfe von unterstützenden Technologien ermöglichen, wie z. B. Sprachausgabeprogrammen.

Die Einstellungen für die behindertengerechte Bedienung in den Benutzervorgaben und Berichtseigenschaften können die systemweiten Einstellungen in der IBM Cognos Administration überschreiben.

Für barrierefreie Berichte ist mehr Berichtsverarbeitung erforderlich und eine größere Dateigröße als nicht zugängliche Berichte. Infolgedessen wirken sich zugängliche Berichte auf die Leistung aus. Standardmäßig ist die Unterstützung für die zugängliche Berichtsausgabe inaktiviert.

Die verfügbare Berichtsausgabe ist für die folgenden Formate verfügbar: PDF, HTML und Microsoft Excel.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Dispatcher und Services**.
2. Klicken Sie in der Symbolleiste der Seite ' **Konfiguration** ' auf die Schaltfläche 'Eigenschaften festlegen'  .
3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Klicken Sie in der Dropdown-Liste **Kategorie** auf **Administratorüberschreibung**.

5. Klicken Sie für die Kategorie **Administratorüberschreibung** neben **Unterstützung der behindertengerechten Bedienung für**in der Spalte **Wert** auf **Bearbeiten**.
6. Wählen Sie auf der Seite **Unterstützung der behindertengerechten Bedienung für** eine der folgenden Optionen aus:

Option	Beschreibung
Inaktivieren	Die zugängliche Berichtsausgabe ist für Benutzer nicht verfügbar.
Obligatorisch machen	Die zugängliche Berichtsausgabe wird immer erstellt.
Dem Benutzer die Möglichkeit geben,	Die zugängliche Berichtsausgabe wird vom Benutzer angegeben. Wenn Sie diese Option auf **Nicht ausgewählt**setzen, wird die zugängliche Berichtsausgabe nicht automatisch erstellt. Dies ist der Standardwert. Wenn Sie diese Option auf **Ausgewählt**setzen, wird die zugängliche Berichtsausgabe standardmäßig erstellt.

Cognos Analytics Mobile Reports zur behindertengerechten Bedienung

IBM Cognos Analytics Mobile Reports ist auf iOS 7 und größeren Einheiten vollständig zugänglich. Wenn die Funktion **VoiceOver** aktiviert ist, handelt es sich bei diesen Einheiten um einen Sprachausgabeprogramm. Benutzer können dann mit einer Bluetooth-Tastatur oder mit Anzeigengesten navigieren, indem sie Standardbefehle für die Tastatur von Apple-Tastatur verwenden. Weitere Informationen finden Sie in Ihrer Einheitendokumentation.

Cognos Analytics Mobile Reports enthält zusätzliche Direktaufrufe über die Tastatur, mit denen Sie in verschiedenen Ansichten navigieren können.

Tastaturkurzbefehle in Cognos Analytics Mobile Reports

Tastaturkurzbefehle sind für unterschiedliche Ansichten in IBM Cognos Analytics Mobile Reportsdefiniert.

Tastaturkurzbefehle sind für die folgenden Anzeigen, Leerzeichen und Ansichten definiert:

- Cognos Analytics Mobile Reports -Hauptanzeige.
- Meine Berichte, Importierte Inhalte und Beispielbereiche.
- Ansichten durchsuchen und durchsuchen.
- Berichtsanzeige.
- **Sicherheitscode eingeben** -Fenster.

Cognos Analytics Mobile Reports -Hauptanzeige

Wenn die **VoiceOver** -Funktion auf Ihrem mobilen iOS-Gerät aktiviert ist, können Sie IBM Cognos Analytics Mobile Reports -Direktaufrufe über die Tastatur verwenden, um IBM Cognos Analytics im Cognos Analytics Mobile Reports -Hauptanzeige zu navigieren.

Führen Sie in der Cognos Analytics Mobile Reports -Hauptanzeige die folgende Tastenkombination aus, um die folgende Aktion auszuführen:

Tabelle 84. Direktaufrufe über die Tastatur in Cognos Analytics Mobile Reports	
Aktion	**Tastaturkurzbefehl**
Wenn eine Speicherbereichsverbindung den Fokus hat, öffnen Sie das Fenster "Löschen".	Strg + D

Meine Berichte, importierte Inhalte und Beispielbereiche

Wenn die **VoiceOver** -Funktion auf Ihrem mobilen iOS-Gerät aktiviert ist, können Sie mithilfe von Cognos Mobile-Tastaturkurzbefehlen IBM Cognos Analytics in den Bereichen "Eigene Berichte", "Importierte Inhalte" und "Beispiele" navigieren.

Tastaturkurzbefehle lösen verschiedene Aktionen aus, die von dem Modus abhängen, in dem Sie sich befinden. Die Modi sind Standard und bearbeiten.

Standardmodus

Verwenden Sie im Standardmodus die folgenden Direktaufrufe über die Tastatur, um die folgenden Aktionen auszuführen:

Tabelle 85. Eigene Berichte, importierte Inhalte und Beispielbereiche, Tastaturkurzbefehle für den Standardmodus	
Aktion	**Tastaturkurzbefehl**
Verlassen Sie einen Speicherbereich oder minimieren Sie ihn.	Strg + X
Öffnen Sie die Anzeige-und Suchansichten (nur My Reports-Bereich).	Strg + B
Aktualisieren Sie die Liste der Berichte.	Strg + R
Bearbeiten Sie den Speicherplatztitel.	Strg + T
Öffnen oder schließen Sie die Benutzerauthentifizierungseinstellungen (nur My Reports-Bereich).	Strg + A
Öffnen oder schließen Sie die Hintergrundeinstellungen des Hintergrundpapiers.	Strg + W
Geben Sie den Berichtsvorschaumodus ein oder beenden Sie ihn	Strg + P
Bearbeiten Sie den Bearbeitungsmodus.	Strg + D

Bearbeitungsmodus

Verwenden Sie im Bearbeitungsmodus die folgenden Direktaufrufe über die Tastatur, um die folgenden Aktionen auszuführen:

Tabelle 86. Eigene Berichte, importierte Inhalte und Beispielbereiche, Tastaturkurzbefehle im Bearbeitungsmodus	
Aktion	**Tastaturkurzbefehl**
Kehren Sie zum Standardmodus zurück, wenn Sie die Bearbeitung beendet haben.	Strg + D
Wählen Sie alle aus, wenn keine ausgewählt sind, oder wählen Sie keine aus, wenn alle ausgewählt sind.	Strg + A
Tauschen Sie einen Bericht mit dem Fokus mit dem nächsten Bericht aus (behält den Fokus auf dem bewegten Bericht).	Strg + S

Tabelle 86. Eigene Berichte, importierte Inhalte und Beispielbereiche, Tastaturkurzbefehle im Bearbeitungsmodus (Forts.)	
Aktion	**Tastaturkurzbefehl**
Löschen Sie die ausgewählten Berichte und kehren Sie zum Standardmodus zurück.	Löschen

Ansichten durchsuchen und suchen

Wenn die **VoiceOver** -Funktion auf Ihrem mobilen iOS-Gerät aktiviert ist, können Sie mithilfe von Cognos Mobile-Tastaturkurzbefehlen IBM Cognos Analytics in der Ansicht "Durchsuchen" und "Suchen" navigieren.

Im Bereich "Eigene Berichte" können Sie suchen und suchen. Verwenden Sie in der Anzeige "Durchsuchen" und "Suchen" die folgenden Direktaufrufe über die Tastatur, um die folgenden Aktionen auszuführen:

Tabelle 87. Direktaufrufe über die Tastatur durchsuchen und anzeigen	
Aktion	**Tastaturkurzbefehl**
Schließen Sie das Durchsuchen oder die Suchansicht.	Strg + X
Aktualisieren Sie die aktuelle Anzeige-oder Suchseite.	Strg + R
Wechseln Sie zur nächsten Seite.	Opt + Links-oder Rechtspfeil
Wenn das Fenster **Gespeicherte Ausgabe** geöffnet ist, schließen Sie es.	Zurück oder Eingabetaste

Berichtsanzeige

Wenn die **VoiceOver** -Funktion auf Ihrem mobilen iOS-Gerät aktiviert ist, können Sie Cognos Mobile-Direktaufrufe über die Tastatur verwenden, um IBM Cognos Analytics in der Berichtsanzeige zu navigieren.

Im Bereich "Eigene Berichte" können Sie Berichte in der Berichtsanzeige anzeigen. Tastaturkurzbefehle lösen verschiedene Aktionen aus, die von dem Modus abhängen, in dem Sie sich befinden. Die Modi sind Standard und zeichnen sich aus.

Standardmodus

Verwenden Sie im Standardmodus die folgenden Direktaufrufe über die Tastatur, um die folgenden Aktionen auszuführen:

Tabelle 88. Berichtsanzeigefunktion, Tastaturkurzbefehle für Standardmodus	
Aktion	**Tastaturkurzbefehl**
Schließen oder minimieren Sie den Berichtsviewer. Gehen Sie beim Durchbohren zur Quelle zurück.	Strg + X
Öffnen oder schließen Sie die Seitenauswahlfunktion.	Strg + P
Öffnen oder schließen Sie das Aktionsmenü.	Strg + A
Zeichemodus eingeben.	Strg + D
Rufen Sie die nächste Seite auf.	Strg +. (>)
Rufen Sie die vorherige Seite auf.	Strg +, (<)

Zugmodus

Verwenden Sie im Ziehmodus die folgenden Direktaufrufe über die Tastatur, um die folgenden Aktionen auszuführen:

Tabelle 89. Berichtsanzeigefunktion, Direktaufrufe für den Ziehmodus	
Aktion	**Tastaturkurzbefehl**
Änderungen verwerfen und Auszugmodus verlassen.	Strg + D
Teilen Sie einen Bericht mit Annotationen.	Strg + M
Wenn das Menü "Draw Box" geöffnet ist, erhöhen Sie die Breite der Draw-Box um 10 Pixel.	Strg + W
Wenn das Menü "Draw Box" geöffnet ist, verringern Sie die Breite des Draw-Box um 10 Pixel.	Strg + Umschalttaste + W
Wenn das Menü "Draw Box" geöffnet ist, erhöhen Sie die Höhe der Draw-Box um 10 Pixel.	Strg + H
Wenn das Menü "Draw Box" geöffnet ist, verringern Sie die Höhe der Draw-Box um 10 Pixel.	Strg + Umschalttaste + H
Wenn das Menü "Draw Box" geöffnet ist, verlassen Sie das Menü "Draw Box".	Strg + X

Fenster 'Sicherheitscode eingeben'

Wenn das Feature **VoiceOver** auf Ihrem mobilen iOS-Gerät aktiviert ist, können Sie im **Sicherheitscode eingeben** -Fenster Cognos Mobile-Tastaturkurzbefehle verwenden, um im IBM Cognos Analytics -Fenster zu navigieren.

Verwenden Sie die folgenden Direktaufrufe über die Tastatur, um die folgenden Aktionen auszuführen:

Tabelle 90. Tastaturkurzbefehle für den Sicherheitscode eingeben	
Aktion	**Tastaturkurzbefehl**
Geben Sie Ihre PIN ein.	Zahlen auf der Tastatur
Löschen Sie die letzte Eingabe, die Sie zuletzt eingegeben haben.	Löschen

Bekannte Probleme

IBM Cognos Analytics Mobile Reports enthält Direktaufrufe über die Tastatur, die Ihnen beim Navigieren und Ausführen von Tasks in IBM Cognos Analytics helfen, indem Sie nur eine Tastatur verwenden. Möglicherweise stoßen Sie jedoch auf bekannte Probleme mit dem Feature "iOS **VoiceOver** ".

Bei der Anzeige von Berichtsinhalten funktionieren Cognos -Tastaturkurzbefehle nicht

Wenn die **VoiceOver** -Funktion aktiviert ist und Sie Berichtsinhalte wie den Berichtsinhalt in der Berichtsanzeige oder in der IBM Cognos Analytics Mobile Reports -Hauptanzeige anzeigen, funktionieren die Tastaturbefehle von Cognos Analytics Mobile Reports nicht. Um dieses Problem zu beheben, bewegen Sie den Fokuscursor zurück in den Symbolleistenbereich.

Tastaturlistener stoppt die Arbeit, wenn ein Element abgegriffen wird

Wenn Sie den Berichtsinhalt in der Anwendung " IBM Cognos Analytics Mobile Reports " anzeigen, wird die Funktion " **VoiceOver** " gestoppt, wenn Sie auf ein Element tippen. Die Problemumgehung besteht darin, die **VoiceOver** -Funktion aus-und wieder auszuschalten oder zu einer anderen Ansicht zu

navigieren und dann zur ursprünglichen Ansicht zurückzukehren, um die **VoiceOver** -Funktion zurückzusetzen.

Der Löschschlüssel funktioniert nicht in Texteingabefeldern

Wenn Sie sich im **VoiceOver** -Modus befinden, funktioniert der Löschschlüssel nicht in Texteingabefeldern in der IBM Cognos Analytics Mobile Reports -Anwendung. Wenn Sie einen Fehler machen und zum Löschen eines Zeichens möchten, verwenden Sie den Direktaufruf über die Tastatur, Strg + Löschen.

Anhang B. Round Trip Safety Configuration of Shift-JIS Charaktere

Shift-JIS ist ein Zeichencodierungssystem für japanische Zeichen. Es ist äquivalent zu ASCII, einem Zeichencodierungssystem für englische Zeichen.

Native Codierung und Unicode

Da Shift-JIS und ASCII beide Zeichen für eine Sprache definieren, handelt es sich um native Codierungssysteme. Unicode ist ein Zeichencodierungssystem, das Zeichen für alle Sprachen definiert. Da Software in einer globalen, mehrsprachigen Umgebung verwendet wird, müssen die Zeichen für die Verarbeitung durch Computer häufig zwischen systemeigenen Codierungssystemen und Unicode konvertiert werden.

Round-Trip-Sicherheit

Probleme, die mit Konvertierungen zwischen nativen Codierungssystemen und Unicode verbunden sind, werden als Round Trip Safety-Probleme bezeichnet.

Mit Unicode werden Anwendungen entwickelt, die die Eingabe aus verschiedenen Sprachen gleichzeitig bearbeiten können. Eingabedaten, die von Benutzern eingegeben oder aus Datenbanken abgerufen werden, können Zeichen enthalten, die in einem nativen Codierungssystem codiert sind. Beispiel: In Microsoft Fenster werden die von einem Benutzer eingegebenen englischen Zeichen unter Windows-1252 codiert.

Wenn eine Anwendung Zeichen in einem nativen Codierungssystem empfängt, konvertiert sie die Zeichen in Unicode für die Verarbeitung. Nachdem die Verarbeitung beendet ist, können die Zeichen wieder in das native Codierungssystem konvertiert werden.

In den meisten Fällen werden die Zeichen ohne Mehrdeutigkeit konvertiert, da jedes native Zeichen einem einzigen Unicode-Zeichen zugeordnet ist. Wenn die Konvertierung eines nativen Sprachcharakters in und aus Unicode-Ergebnissen den ursprünglichen Charakter hat, wird der Charakter als "Round Trip Safe" betrachtet.

Zum Beispiel ist das Zeichen "A" bei Windows-1252 rund um die Reise sicher, wie folgt:

- Das Windows-1252 Zeichen für "A" ist 0x41.
- Es wandelt sich in Unicode U + 0041 um.
- Kein anderes Windows-1252-Zeichen wandelt auf das gleiche Unicode-Zeichen um, so dass es immer wieder in 0x41 konvertiert wird.

Spezifische Fragen zu Shift-JIS

Obwohl die Zeichen aus den meisten nativen Zeichencodierungssystemen eine runde Reise sicher sind, ist das Umschalt-JIS-Codierungssystem eine Ausnahme. Ungefähr 400 Zeichen in Shift-JIS sind nicht rundum sicher, da mehrere Zeichen in dieser Gruppe dem gleichen Unicode-Zeichen zugeordnet werden können. Zum Beispiel konvertieren die Shift-JIS-Zeichen 0x8790 und 0x81e0 in das Unicode-Zeichen U + 2252.

IBM Cognos Analytics und Shift-JIS

IBM Cognos Analytics verwendet Unicode. Die Rundumsicherheit von Zeichen ist wichtig, um die Genauigkeit der Daten in generierten Berichten zu gewährleisten.

Das Round Trip Safety Configuration-Dienstprogramm sorgt für die Umlaufsicherheit von Shift-JIS-Zeichen nur, wenn es sowohl zum Konvertieren von Zeichen als auch zum Konvertieren von Zeichen verwendet wird:

- von Shift-JIS zu Unicode
- von Unicode zu Shift-JIS

Wenn Daten aus einer Datenbank angefordert werden, die über einen eigenen automatischen Mechanismus für die Konvertierung von Shift-JIS in Unicode verfügt, ruft IBM Cognos Analytics das Dienstprogramm "Round Trip Safety Configuration" nicht auf, um die Zeichen von Unicode in Shift-JIS zu konvertieren. Die Rundumsicherheit von Zeichen in den Daten kann nicht gewährleistet werden.

Weitere Informationen zum Dienstprogramm 'Round Trip Safety Configuration' finden Sie im Artikel „Das Round Trip Safety Configuration Utility" auf Seite 436.

Beispiel: Safe Conversion of Shift-JIS

Das folgende Beispiel veranschaulicht das Problem mit Shift-JIS-Konvertierung in Unicode:

- Eine Datenbank enthält Zeichen, die in Shift-JIS codiert sind.
- Ein Datensatz in der Datenbank enthält das Shift-JIS-Zeichen 0x8790.
- Ein Benutzer gibt das Shift-JIS-Zeichen 0x8790 in ein Dateneingabeformular in einem Browser ein.
- Die Anwendung empfängt das Eingabeformular und konvertiert das Shift-JIS-Zeichen 0x8790 in das Unicode-Zeichen U + 2252.
- Da die Datenbank Shift-JIS-codierte Zeichen enthält, kann das Unicode-Zeichen U + 2252 nicht als Teil der Abfrage angegeben werden.
- Die Anwendung muss U + 2252 zurück in ein Shift-JIS-Zeichen konvertieren. Sowohl 0x8790 als auch 0x81e0 konvertieren auf U + 2252. Wenn der Konvertierungsprozess 0x81e0 auswählt, gibt die Abfrage keine Datensätze zurück.

Um dieses Problem zu beheben, können Sie mit dem Dienstprogramm für die Sicherheitskonfiguration der runden Trip sicherstellen, dass die Konvertierung auf 0x8790 erfolgt und der Datensatz gefunden wird.

Das Round Trip Safety Configuration Utility

Sie können das Dienstprogramm für die Sicherheitskonfiguration "Round Trip Safety Configuration" verwenden, um den Konvertierungsprozess von Shift-JIS-Zeichen so zu konfigurieren, dass IBM Cognos Analytics immer die richtigen Datensätze zurückgibt.

Dieses Dienstprogramm gibt Ihnen die Kontrolle über die beiden folgenden Situationen:

- Mehr als ein Shift-JIS-Zeichen wandelt auf das gleiche Unicode-Zeichen.

  Wenn Ihre Daten solche Shift-JIS-Zeichen enthalten, können Sie mit dem Dienstprogramm angeben, dass das Unicode-Zeichen immer in den erforderlichen Shift-JIS-Zeichensatz konvertiert werden soll. Weitere Informationen finden Sie unter „Konvertierungen angeben" auf Seite 436.
- Mehr als ein Unicode-Zeichen steht nach der Konvertierung für das gleiche oder ähnliche Zeichen.

  Solche Unicode-Zeichen können als identisch betrachtet werden, wenn sie von Computern verarbeitet werden und für einander ersetzt werden können. Sie können das Dienstprogramm verwenden, um sicherzustellen, dass die korrekte Ersetzung vorgenommen wird. Weitere Informationen finden Sie unter „Ersetzen angeben" auf Seite 437.

Konvertierungen angeben

Wenn Ihre Daten mehr als ein Shift-JIS-Zeichen enthalten, das dasselbe Unicode-Zeichen konvertiert, verwenden Sie das Dienstprogramm für die Sicherheitskonfiguration "Round Trip Safety Configuration", um anzugeben, dass das Unicode-Zeichen immer in den erforderlichen Shift-JIS-Zeichensatz konvertiert werden soll.

Bevor Sie das Shift-JIS-Zeichen auswählen, das in einer Konvertierung verwendet werden soll, bestimmen Sie, welches Shift-JIS-Zeichen derzeit in der Umgebung verwendet wird. Nur einer der möglichen Shift-JIS-Äquivalente eines Unicode-Zeichens kann in einer bestimmten Umgebung verwendet werden.

Auf der Registerkarte "Konvertierung" werden native Codierungszeichen im Format 0xJJJJ angezeigt, und Unicode-Zeichen werden im Format U + JJJJ angezeigt, wobei JJJJ den Hexadezimalwert des Unicode-Zeichens darstellt.

Das Zeichen "A" wird z. B. wie folgt angezeigt:

- für native Codierung, 0x41
- für Unicode, U + 0041

Jede Zeile stellt eine Zuordnungsregel dar, die zwei oder drei Shift-JIS-Zeichen mit dem Unicode-Zeichen in der ersten Spalte verknüpft.

Standardmäßig werden alle Shift-JIS-Zeichen in einer Zeile in das zugehörige Unicode-Zeichen konvertiert. Zum Beispiel konvertieren die Shift-JIS-Zeichen 0x8782 und 0xFA59 in das Unicode-Zeichen U + 2116.

Sie können mehr als ein Zeichen zu einem bestimmten Zeitpunkt konfigurieren.

Vorgehensweise

1. Starten Sie das Dienstprogramm 'Round Trip Safety Configuration' im Verzeichnis '*Installationsposition*/bin':
   - für Microsoft Fenster -Betriebssystem, rtsconfig.exe
   - für UNIX -Betriebssystem, rtsconfig
2. Klicken Sie auf die Registerkarte **Konvertierung** .

   Tipp: Klicken Sie im Menü **Anzeigen** auf **Glyphen**, um die Glyph neben dem Unicode-Zeichen anzuzeigen. Abhängig von der Art und der Größe der von Ihnen verwendeten Schriftarten sind einige Glyphen möglicherweise nicht sichtbar.
3. Klicken Sie im Menü **Bearbeiten** auf **Finde einen Charakter,** , und geben Sie dann den Hexadezimalwert des Shift-JIS-Zeichens ein.
4. Klicken Sie auf **OK**.
5. Wählen Sie in der Spalte **Erste Shift-JIS-Zeichen**, **Zweite Shift-JIS-Zeichen**oder **Dritte Umschalttaste-JIS-Zeichen** das Shift-JIS-Zeichen aus, in das das Unicode-Zeichen konvertiert werden soll.
6. Wiederholen Sie die Schritte 3 bis 5 für jedes Shift-JIS-Zeichen, das Sie konfigurieren möchten.
7. Speichern Sie Ihre Spezifikationen mit einer der folgenden Methoden:
   - Wenn Sie nur Ihre Spezifikationen speichern möchten, klicken Sie im Menü **Datei** auf **Speichern**.
   - Um Ihre Spezifikationen zu speichern und anzuwenden, klicken Sie im Menü **Werkzeuge** auf **Konfigurieren**.

   Wenn Sie nur speichern, können Sie Ihre Spezifikation später anwenden. Weitere Informationen finden Sie unter „Conversions und Substitutionen anwenden” auf Seite 438. Sie können auch Standardeinstellungen wiederherstellen. Weitere Informationen finden Sie unter „Standardeinstellungen für Konvertierungseinstellungen wiederherstellen” auf Seite 439.

   Die Spezifikationen werden in der Datei 'shift-jis.xml' im Verzeichnis 'bin' von *Installationsposition/* gespeichert.

Ersetzen angeben

Nach der Konvertierung können die Unicode-Daten Zeichen enthalten, die im Sinn identisch, aber in der Darstellung unterschiedlich sind. Beispiel: Eine Tilde (~) mit voller Breite und eine Tilde mit halber Breite haben unterschiedliche Werte in Unicode, können aber während der Verarbeitung als identisch betrachtet werden.

Sie können das Dienstprogramm für die Sicherheitskonfiguration "Round Trip Safety Configuration" verwenden, um anzugeben, dass bestimmte Paare ähnlicher Zeichen durch ein einzelnes Zeichen ersetzt

werden sollen. Zum Beispiel können Sie angeben, dass beide Tilde-Breiten durch eine Tilde mit voller Breite ersetzt werden.

Auf der Registerkarte 'Substitution' (Substitution) enthält die erste Spalte Paare von Zeichen, die im Allgemeinen das gleiche bedeuten, aber durch unterschiedliche Werte in Unicode dargestellt werden. Jede Zeile stellt eine Substitutionsregel dar. In der ersten Spalte werden die Daten vor der Konvertierung aufgelistet. In der zweiten Spalte werden die möglichen Ersatzzeichen aufgelistet.

Vorgehensweise

1. Starten Sie das Dienstprogramm 'Round Trip Safety Configuration' im Verzeichnis '*Installationsposition*/bin':
   - für Microsoft Fenster -Betriebssystem, rtsconfig.exe
   - für UNIX -Betriebssystem, rtsconfig
2. Klicken Sie auf die Registerkarte **Substitution** .

   Tipp: Klicken Sie im Menü **Anzeigen** auf **Glyphen**, um die Glyph neben dem Unicode-Zeichen anzuzeigen. Abhängig von der Art und der Größe der von Ihnen verwendeten Schriftarten sind einige Glyphen möglicherweise nicht sichtbar.
3. Klicken Sie in der Spalte **Ursprünglicher Code** auf das Zeichen, das Sie ersetzen möchten.
4. Klicken Sie in der Spalte **Ersatzcode** auf das entsprechende Zeichen.

   Eine Liste möglicher Substitutionsoptionen wird angezeigt.
5. Klicken Sie in der Liste auf das Unicode-Zeichen, das Sie verwenden möchten, oder klicken Sie auf **Nicht ersetzen**.
6. Wiederholen Sie die Schritte 3 bis 5 für jedes Unicode-Zeichen, das ersetzt werden soll.
7. Speichern Sie Ihre Spezifikationen mit einer der folgenden Methoden:
   - Wenn Sie nur Ihre Spezifikationen speichern möchten, klicken Sie im Menü **Datei** auf **Speichern**.
   - Um Ihre Spezifikationen zu speichern und anzuwenden, klicken Sie im Menü **Werkzeuge** auf **Konfigurieren**.

   Wenn Sie nur speichern, können Sie Ihre Spezifikation später anwenden. Weitere Informationen finden Sie unter „Konvertierungen angeben” auf Seite 436. Sie können auch Standardeinstellungen wiederherstellen. Weitere Informationen finden Sie unter „Standardeinstellungen für Konvertierungseinstellungen wiederherstellen” auf Seite 439.

   Die Spezifikationen werden in der Datei 'shift-jis.xml' im Verzeichnis 'bin' von *Installationsposition/* gespeichert.

Conversions und Substitutionen anwenden

Wenn Sie Änderungen nicht anwenden, wenn Sie speichern, können Sie die Daten später anwenden. Basierend auf Informationen, die in der Datei install_location/bin/shift-jis.xml gespeichert wurden, werden zwei Dateien generiert:

- für Substitutionsdaten, i18n_res.xml
- für Konvertierungsdaten, ibm-943_P14A-2000.cnv

Informationen zu diesem Vorgang

Wenn Sie die Daten anwenden, werden die Zeichen standardmäßig nicht auf die Sicherheit für Rundreisen überprüft. Wenn Sie den Konfigurationsmodus festlegen, können Sie auswählen, ob die Sicherheit für Rundreisen überprüft werden soll, indem Sie die Option auswählen, die während der Laufzeit einen Konvertierungsfehler für Zeichen zurückgibt, die nicht rund um die Reise sicher sind. Dies kann nützlich sein, um zunächst zu erkennen, welche Shift-JIS-Zeichen konfiguriert werden müssen.

Vorgehensweise

1. Stoppen Sie IBM Cognos Analytics.
2. Klicken Sie im Dienstprogramm für die Sicherheitskonfiguration "Round Trip Safety Configuration" im Menü **Werkzeuge** auf **Konfigurieren Sie den Konfigurationsmodus.**.
3. Geben Sie an, ob Zeichen für die Sicherheit von Rundreisen überprüft werden sollen.
4. Klicken Sie im Menü **Werkzeuge** auf **Konfigurieren**.
5. Starten Sie IBM Cognos Analytics.

Standardeinstellungen für Konvertierungseinstellungen wiederherstellen

Sie können die Standardeinstellungen in Ihren Konfigurations-und Substitutionsdaten jederzeit schnell wiederherstellen. Sie können die Konfiguration beispielsweise in den folgenden Situationen wiederherstellen:

· Nachdem Ihre Anwendung für die Verwendung einer anderen Datenquelle festgelegt wurde, für die eine andere Konfiguration erforderlich ist

· nach dem Prototyping

Vorgehensweise

1. Stoppen Sie IBM Cognos Analytics.
2. Klicken Sie im Dienstprogramm für die Sicherheitskonfiguration "Round Trip Safety Configuration" im Menü **Werkzeuge** auf **Standardwerte wiederherstellen**.

   Der Konvertierungsprozess wird so festgelegt, dass die Standardwerte verwendet werden.
3. Starten Sie IBM Cognos Analytics.

Geben Sie Konvertierungen für Web Reports der Series 7 PowerPlay an.

IBM Cognos Series 7 liefert eine begrenzte Lösung für die japanischen Vendor Defined Characters (VDC) in Shift-JIS-Codierung. Um die Datenintegrität und -konsistenz bei der Verwendung von PowerPlay -Webberichten mit IBM Cognos Analyticssicherzustellen, müssen Sie die Zeichenzuordnung auf die Standardwerte setzen.

Vorgehensweise

1. Stoppen Sie IBM Cognos Analytics.
2. Starten Sie das Dienstprogramm "Round Trip Safety Configuration" (siehe „Das Round Trip Safety Configuration Utility” auf Seite 436).
3. Klicken Sie im Menü **Werkzeuge** auf **Standardwerte wiederherstellen**.
4. Klicken Sie im Menü **Werkzeuge** auf **Konfigurieren**.

   Die Konvertierungstabellen werden so eingestellt, dass die Standardwerte im Hintergrund verwendet werden.
5. Schließen Sie das Sicherheitskonfigurationsdienstprogramm "Round Trip".
6. Starten Sie IBM Cognos Analytics.

Anhang C. Anfangszugriffsberechtigungen

Wenn Content Manager in IBM Cognos Analyticseinen Content-Store initialisiert, erstellt er Basisstrukturen und Sicherheitsinformationen. Zu diesen Strukturen gehört eine Hierarchie von Ordnern.

Content Manager enthält die folgenden Ordner und Ordnerinhalte:

/Root
Alle Ordner unten /Root in der Hierarchie.

/Root/Verzeichnis
Informationen zu Authentifizierungsprovidern und anderen Informationen, die normalerweise in einem Verzeichnisservice zu finden sind.

/Root/Verzeichnis/Cognos
Der Cognos -Verzeichnisnamensbereich, der Cognos -Gruppen, Datenquellen, Verteilerlisten und Kontakte enthält.

/Root/Directory/*other_providers*
Andere Sicherheitsbereiche, z. B. LDAP und Active Directory.

/Root/Öffentlicher Inhalt
Alle Anwendungsdaten in Content Manager.

/Root/Directory/*Anwendungspakete*
Ein separater Ordner für jede Anwendung, die Informationen zu der Anwendung enthält.

/Root/Konfiguration
Konfigurationsdaten für alle Cognos -Komponenten und -Schablonen.

/Root/Capabilities
Objekte, die durch Richtlinien gesichert werden können, die den Zugriff auf Funktionen beschränken, wie z. B. Verwaltung, Reportingund Query Studio, und Funktionen, wie z. B. benutzerdefiniertes SQL, und Bersten.

Es wird empfohlen, die Anfangseinstellungen so zu ändern, dass die IBM Cognos -Software gesichert wird. Weitere Informationen finden Sie unter Kapitel 15, „Anfangssicherheit”, auf Seite 223 und Kapitel 12, „Zugriffsberechtigungen und Berechtigungsnachweise”, auf Seite 193.

Anfangszugriffsberechtigungen für Content Manager-Objekte mit Root-und höchster Ebene

Wenn Content Manager in IBM Cognos Analyticseinen Content-Store initialisiert, erstellt er Basisstrukturen und Sicherheitsinformationen. Zu diesen Strukturen gehören die Anfangszugriffsberechtigungen für das Stammelement und die Content Manager-Objekte der höchsten Ebene.

Das Stammobjekt

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 91. Das Stammobjekt und die Berechtigungen für zugehörige Gruppen oder Rollen

Objekt	Gruppe oder Rolle	Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Stammelement	Jeder	X		X		X

Content Manager-Objekte der höchsten Ebene

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 92. Content Manager-Objekte der höchsten Ebene und Berechtigungen für zugehörige Gruppen und Rollen

Objekt	Gruppe oder Rolle	Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Funktionen	Verzeichnisadministratoren				X	X
	Jeder					X
Verwaltung	Verzeichnisadministratoren			X	X	X
	Bibliotheksadministratoren			X		X
	Mobile Administratoren			X		X
	Modellierungsprogramme			X		X
	Portaladministratoren			X		X
	PowerPlay-Administratoren			X		X
	Berichtsadministratoren			X		X
	Serveradministratoren			X		X
Konfiguration	Verzeichnisadministratoren	X	X	X	X	X
	Jeder	X		X		X
Bibliothek	Bibliotheksadministratoren	X	X	X	X	X
	Jeder	X		X		X

Tabelle 92. Content Manager-Objekte der höchsten Ebene und Berechtigungen für zugehörige Gruppen und Rollen (Forts.)

Objekt	Gruppe oder Rolle	Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Öffentlicher Inhalt	Analysebenutzer	X		X		X
	Verfasser	X	X	X		X
	Verbraucher	X		X		X
	Informationsverteilung	X				X
	Modellierungsprogramme	X	X	X		X
	PowerPlay-Administratoren	X	X	X	X	X
	PowerPlay-Benutzer	X		X		X
	Benutzer abfragen	X		X		X
	Leser	X				X
	Berichtsadministratoren	X	X	X	X	X
Verzeichnis	Jeder					X
Cognos	Verzeichnisadministratoren	X	X	X	X	X
	Jeder	X		X		X

Anfängliche Zugriffsberechtigungen für Funktionen

Wenn Content Manager in IBM Cognos Analyticseinen Content-Store initialisiert, erstellt er Basisstrukturen und Sicherheitsinformationen. Zu diesen Strukturen gehören die ersten Zugriffsberechtigungen für die Funktionen.

Die Funktionen werden auch als gesicherte Funktionen und geschützte Features bezeichnet.

Anmerkung: Wenn Sie Änderungen an den Anfangszugriffsberechtigungen vornehmen möchten, siehe "Zugriff auf Funktionen festlegen" in der *IBM Cognos Analytics -Leitfaden*.

Berechtigungsstufen

Es gibt fünf Arten von Zugriffsberechtigungen, die einer Gruppe oder einer Rolle zugeordnet werden können: **Lesen**, **Schreiben**, **Ausführen**, **Richtlinie festlegen**und **Traverse**. Eine Beschreibung der zulässigen Aktionen, die für jeden Berechtigungstyp verfügbar sind, finden Sie unter Kapitel 12, „Zugriffsberechtigungen und Berechtigungsnachweise", auf Seite 193.

Darüber hinaus werden für jede Funktion Kombinationen von Zugriffsberechtigungen erteilt. Diese Kombinationen sind als Berechtigungsstufen definiert, wie in der folgenden Tabelle dargestellt:

Berechtigungsstufe	Zugriffsberechtigungen erteilt
Zugriff	**Ausführen** und **Traverse**
Zuordnen	**Traverse** und **Richtlinie festlegen**
Verwalten	**Ausführen**, **Traverse**und **Richtlinie festlegen**
Angepasst	Jede andere Kombination, die nicht oben aufgeführt ist.

Funktionsnamen

In diesem Abschnitt werden alle Cognos Analytics-Funktionen aufgelistet. Für jede Funktion können Sie sehen, welche Gruppen oder Rollen anfänglich auf die Funktionalität zugreifen können, sowie die Zugriffsberechtigungen, die ihnen erteilt wurden.

Adaptive Analytics-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 93. Adaptive Analytics-Funktion und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Verzeichnisadministratoren	Zuordnen				✓	✓

Verwaltungsfunktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 94. Verwaltungsfunktion und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Verzeichnisadministratoren	Verwalten			✓	✓	✓
Bibliotheksadministratoren	Zugriff			✓		✓
Mobile Administratoren	Zugriff			✓		✓

Tabelle 94. Verwaltungsfunktion und Berechtigungen für zugehörige Gruppen und Rollen (Forts.)						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Modellierungsprogramme	Zugriff			✓		✓
Portaladministratoren	Zugriff			✓		✓
PowerPlay -Administratoren	Zugriff			✓		✓
Berichtsadministratoren	Zugriff			✓		✓
Serveradministratoren	Zugriff			✓		✓

Die gesicherten Features in der folgenden Tabelle sind untergeordnete Elemente der Verwaltungsfunktion.

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 95. Gesicherte Funktionen der Verwaltungsfunktion und Berechtigungen für zugehörige Gruppen und Rollen								
Gesicherte Funktion	**Gruppe oder Rolle**	**Berechtigungsstufe**	**Berechtigungstyp**					
			Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Adaptive Analytics-Administration	Adaptive Analytics-Administratoren				✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓

Tabelle 95. Gesicherte Funktionen der Verwaltungsfunktion und Berechtigungen für zugehörige Gruppen und Rollen (Forts.)

Gesicherte Funktion	Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
			Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Verwaltungstasks	Serveradministratoren	Zugriff			✓		✓
	Berichtsadministratoren	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓
	PowerPlay-Administratoren	Zugriff			✓		✓
Collaboration-Verwaltung	Verzeichnisadministratoren	Verwalten			✓	✓	✓
System konfigurieren und verwalten	Serveradministratoren	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓
Controllerverwaltung	Verzeichnisadministratoren	Zuordnen				✓	✓
Datenquellen-Verbindungen	Verzeichnisadministratoren	Verwalten			✓	✓	✓
	Modellierungsprogramme	Zugriff			✓		✓
Verteilerlisten und Kontakte	Verzeichnisadministratoren	Verwalten			✓	✓	✓
Visualisierungen verwalten	Verzeichnisadministratoren	Zuordnen				✓	✓
	Bibliotheksadministratoren	Zugriff			✓		✓
Metrische Studio-Verwaltung	Verzeichnisadministratoren	Zuordnen				✓	✓

Tabelle 95. Gesicherte Funktionen der Verwaltungsfunktion und Berechtigungen für zugehörige Gruppen und Rollen (Forts.)

Gesicherte Funktion	**Gruppe oder Rolle**	**Berechtigungsstufe**	**Berechtigungstyp**				
			Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Mobile Administration	Verzeichnisadministratoren	Zuordnen				✓	✓
	Mobile Administratoren	Zugriff			✓		✓
Planungsverwaltung	Verzeichnisadministratoren	Zuordnen				✓	✓
PowerPlay-Server	Verzeichnisadministratoren	Zuordnen				✓	✓
	PowerPlay-Administratoren	Zugriff			✓		✓
Drucker	Verzeichnisadministratoren	Verwalten			✓	✓	✓
Service 'Query Service'	Verzeichnisadministratoren	Zuordnen				✓	✓
	Serveradministratoren	Zugriff			✓		✓
Aktivitäten und Zeitpläne ausführen	Berichtsadministratoren	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓
	PowerPlay-Administratoren	Zugriff			✓		✓
Funktionalität festlegen und UI-Profile verwalten	Verzeichnisadministratoren	Verwalten			✓	✓	✓

Tabelle 95. Gesicherte Funktionen der Verwaltungsfunktion und Berechtigungen für zugehörige Gruppen und Rollen (Forts.)							
Gesicherte Funktion	**Gruppe oder Rolle**	**Berechtigungsstufe**	**Berechtigungstyp**				
			Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Stile und Portlets	Portaladministratoren	Zugriff			✓		✓
	Verzeichnisadministratoren	Verwalten			✓	✓	✓
	Bibliotheksadministratoren	Zugriff			✓		✓
Benutzer, Gruppen und Rollen	Verzeichnisadministratoren	Verwalten			✓	✓	✓

AI-Funktionalität

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 96. AI-Funktionalität und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Analyse-Explorers	Zugriff			✓		✓
Analysebenutzer	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓

Die gesicherten Features in der folgenden Tabelle sind untergeordnete Elemente der AI-Funktionalität.

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 97. Gesicherte Funktionen der KI-Funktion und Berechtigungen für zugehörige Gruppen und Rollen							
Gesicherte Funktion	**Gruppe oder Rolle**	**Berechtigungsstufe**	**Berechtigungstyp**				
			Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Lernen	Analyse-Explorers	Zugriff			✓		✓
	Analysebenutzer	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓
Assistent verwenden	Analyse-Explorers	Zugriff			✓		✓
	Analysebenutzer	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓

Analyse Studio-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 98. Analyse Studio-Funktion und Berechtigungen für zugehörige Gruppen und Rollen							
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**					
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**	
Analysebenutzer	Zugriff			✓		✓	
Verfasser	Zugriff			✓		✓	
Verzeichnisadministratoren	Zuordnen				✓	✓	
Modellierungsprogramme	Zugriff			✓		✓	
Berichtsadministratoren	Zugriff			✓		✓	

Funktion 'Ausgaben anhängen'

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 99. Funktion 'Ausgaben anhängen' und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Analyse-Explorers	Zugriff			✓		✓
Analysebenutzer	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓

Cognos Analytics for Mobile-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 100. Cognos Analytics for Mobile-Funktion und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Analyse-Explorers	Zugriff			✓		✓
Analysebenutzer	Zugriff			✓		✓
Analyseanzeigefunktionen	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓
Berichtsadministratoren	Zugriff			✓		✓

Cognos Insight-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 101. Cognos Insight-Funktion und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen 	**Schreiben** 	**Ausführen** 	**Richtlinie festlegen** 	**Traverse** 
Verzeichnisadministratoren	Zuordnen				✓	✓

Funktion 'Cognos Viewer'

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 102. Funktion und Berechtigungen für Cognos Viewer für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen 	**Schreiben** 	**Ausführen** 	**Richtlinie festlegen** 	**Traverse** 
Analysebenutzer	Zugriff			✓		✓
Verfasser	Zugriff			✓		✓
Verbraucher	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓
Analyseanzeigefunktionen	Zugriff			✓		✓
Modellierungsprogramme	Zugriff			✓		✓
PowerPlay-Administratoren	Zugriff			✓		✓
PowerPlay-Benutzer	Zugriff			✓		✓
Benutzer abfragen	Zugriff			✓		✓
Leser	Zugriff			✓		✓
Berichtsadministratoren	Zugriff			✓		✓

Die gesicherten Funktionen in der folgenden Tabelle sind untergeordnete Elemente der Funktion 'Cognos Viewer'.

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 103. Gesicherte Funktionen der Cognos Viewer-Funktion und Berechtigungen für zugehörige Gruppen und Rollen

Gesicherte Funktion	**Gruppe oder Rolle**	**Berechtigungsstufe**	**Berechtigungstyp**				
			Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Kontextmenü Auswahl Symbolleiste	Berichtsadministratoren	Zugriff			✓		✓
	Verfasser	Zugriff			✓		✓
	Verbraucher	Zugriff			✓		✓
	Benutzer abfragen	Zugriff			✓		✓
	Analysebenutzer	Zugriff			✓		✓
	Leser	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓
	Analyseanzeigefunktionen	Zugriff			✓		✓
	Modellierungsprogramme	Zugriff			✓		✓
	PowerPlay-Administratoren	Zugriff			✓		✓
	PowerPlay-Benutzer	Zugriff			✓		✓

Tabelle 103. Gesicherte Funktionen der Cognos Viewer-Funktion und Berechtigungen für zugehörige Gruppen und Rollen (Forts.)							
Gesicherte Funktion	**Gruppe oder Rolle**	**Berechtigungsstufe**	**Berechtigungstyp**				
			Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Mit Optionen ausführen	Berichtsadministratoren	Zugriff			✓		✓
	Verfasser	Zugriff			✓		✓
	Verbraucher	Zugriff			✓		✓
	Benutzer abfragen	Zugriff			✓		✓
	Analysebenutzer	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓
	Modellierungsprogramme	Zugriff			✓		✓
	PowerPlay-Administratoren	Zugriff			✓		✓
	PowerPlay-Benutzer	Zugriff			✓		✓

Funktionalität für Zusammenarbeit

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 104. Funktionalität und Berechtigungen für zusammengehörige Gruppen und Rollen							
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**					
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**	
Analysebenutzer	Zugriff			✓		✓	
Verfasser	Zugriff			✓		✓	
Verbraucher	Zugriff			✓		✓	

Tabelle 104. Funktionalität und Berechtigungen für zusammengehörige Gruppen und Rollen (Forts.)						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓
Modellierungsprogramme	Zugriff			✓		✓
PowerPlay-Administratoren	Zugriff			✓		✓
PowerPlay-Benutzer	Zugriff			✓		✓
Benutzer abfragen	Zugriff			✓		✓
Berichtsadministratoren	Zugriff			✓		✓

Die gesicherten Features in der folgenden Tabelle sind untergeordnete Elemente der Funktion "Collaborate".

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 105. Gesicherte Funktionen der Funktion 'Collaborate' und Berechtigungen für zugehörige Gruppen und Rollen

Gesicherte Funktion	Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
			Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Collaboration-Funktionen zulassen Collaboration-Tools starten	Analysebenutzer	Zugriff			✓		✓
	Verfasser	Zugriff			✓		✓
	Verbraucher	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓
	Modellierungsprogramme	Zugriff			✓		✓
	PowerPlay-Administratoren	Zugriff			✓		✓
	PowerPlay-Benutzer	Zugriff			✓		✓
	Benutzer abfragen	Zugriff			✓		✓
	Berichtsadministratoren	Zugriff			✓		✓

Controller-Studio-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 106. Controller-Studio-Funktion und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Verzeichnisadministratoren	Zuordnen				✓	✓

Dashboardfunktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 107. Dashboardfunktionalität und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Analyse-Explorers	Zugriff			✓		✓
Analysebenutzer	Zugriff			✓		✓
Analyseanzeigefunktionen	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓

Die gesicherten Features in der folgenden Tabelle sind untergeordnete Elemente der Dashboard-Funktion.

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 108. Gesicherte Funktionen der Dashboard-Funktion und der Berechtigungen für zugehörige Gruppen und Rollen

Gesicherte Funktion	Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
			Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Erstellen/ Bearbeiten	Analyse-Explorers	Zugriff			✓		✓
	Analysebenutzer	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓

Data Manager-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 109. Data Manager-Funktion und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓

Datenerfassungsfunktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 110. Datensätze können Funktionen und Berechtigungen für zugehörige Gruppen und Rollen festlegen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓
Jeder	Zugriff			✓		✓

Desktop-Tools-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 111. Desktop-Tools-Funktion und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Analyse-Explorers	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓

Funktionalität für detaillierte Fehler

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 112. Detaillierte Fehlerfunktionalität und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓

Visualisierungsfunktionalität entwickeln

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 113. Entwickeln von Visualisierungsfunktionen und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Analyse-Explorers	Zugriff			✓		✓
Analysebenutzer	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓

Drillthrough-Assistent-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 114. Drillthrough-Assistent-Funktion und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓

11.1.7-E-Mail-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 115. E-Mail-Funktionalität und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Analyse-Explorers	Zugriff			✓		✓
Analysebenutzer	Zugriff			✓		✓
Analyseviewer	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓

Die gesicherten Features in der folgenden Tabelle sind untergeordnete Elemente der E-Mail-Funktionalität.

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 116. Gesicherte Funktionen der E-Mail-Funktionalität und Berechtigungen für zugehörige Gruppen und Rollen								
Gesicherte Funktion	**Gruppe oder Rolle**	**Berechtigungsstufe**	**Berechtigungstyp**					
			Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Optionen für E-Mail	Analyse-Explorers	Zugriff			✓		✓
	Analysebenutzer	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓
Link in E-Mail einschließen	Analyse-Explorers	Zugriff			✓		✓
	Analysebenutzer	Zugriff			✓		✓
	Analyseviewer	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓
Mit E-Mail teilen	Analyse-Explorers	Zugriff			✓		✓

Tabelle 116. Gesicherte Funktionen der E-Mail-Funktionalität und Berechtigungen für zugehörige Gruppen und Rollen (Forts.)								
Gesicherte Funktion	**Gruppe oder Rolle**	**Berechtigungsstufe**	**Berechtigungstyp**					
			Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**	
	Analysebenutzer	Zugriff			✓		✓	
	Analyseviewer	Zugriff			✓		✓	
	Verzeichnisadministratoren	Zuordnen				✓	✓	
Typ in externer E-Mail	Analyse-Explorers	Zugriff			✓		✓	
	Analysebenutzer	Zugriff			✓		✓	
	Analyseviewer	Zugriff			✓		✓	
	Verzeichnisadministratoren	Zuordnen				✓	✓	

Event Studio-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 117. Event Studio-Funktion und Berechtigungen für zugehörige Gruppen und Rollen							
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**					
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**	
Verfasser	Zugriff			✓		✓	
Verzeichnisadministratoren	Zuordnen				✓	✓	
Modellierungsprogramme	Zugriff			✓		✓	
Berichtsadministratoren	Zugriff			✓		✓	

Indexierte Suchfunktionalität ausführen

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 118. Indexierte Suchfunktionalität und Berechtigungen für zugehörige Gruppen und Rollen ausführen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Analysebenutzer Verfasser Verbraucher Analyseanzeigefunktionen Modellierungsprogramme PowerPlay-Administratoren PowerPlay-Benutzer Benutzer abfragen Leser Berichtsadministratoren	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓

Funktion "Executive Dashboard"

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 119. Funktionen und Berechtigungen für das Executive Dashboard für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Analysebenutzer	Zugriff			✓		✓
Verfasser	Zugriff			✓		✓
Verbraucher	Zugriff			✓		✓

Tabelle 119. Funktionen und Berechtigungen für das Executive Dashboard für zugehörige Gruppen und Rollen (Forts.)

Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen 	**Schreiben** 	**Ausführen** 	**Richtlinie festlegen** 	**Traverse** 
Verzeichnisadministratoren	Zuordnen				✓	✓
Analyseanzeigefunktionen	Angepasst			Berechtigung verweigert		Berechtigung verweigert
Modellierungsprogramme	Zugriff			✓		✓
PowerPlay -Administratoren	Zugriff			✓		✓
PowerPlay -Benutzer	Zugriff			✓		✓
Benutzer abfragen	Zugriff			✓		✓
Leser	Zugriff			✓		✓
Berichtsadministratoren	Zugriff			✓		✓

Die gesicherten Features in der folgenden Tabelle sind untergeordnete Elemente der Funktion "Executive Dashboard".

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 120. Gesicherte Funktionen der Funktion "Executive Dashboard" und Berechtigungen für zugehörige Gruppen und Rollen

Gesicherte Funktion	Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
			Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Erweiterte Dashboard-Funktionen verwenden Interaktive Dashboard-Features verwenden	Verfasser	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓
	Analyseanzeigefunktionen	Angepasst					
	Modellierungsprogramme	Zugriff					
	Benutzer abfragen	Zugriff			✓		✓
	Berichtsadministratoren	Zugriff			✓		✓

Explorationsfähigkeit

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 121. Explorationsfähigkeit und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Analyse-Explorers	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓
Analyseanzeigefunktionen	Angepasst			Berechtigung verweigert		Berechtigung verweigert

Funktion 'Externe Repositorys'

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 122. Funktionalität und Berechtigungen für externe Repositorys für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓
Jeder	Zugriff			✓		✓

Die gesicherten Features in der folgenden Tabelle sind untergeordnete Elemente der Funktion 'Externe Repositorys'.

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 123. Gesicherte Funktionen der Funktion für externe Repositorys und Berechtigungen für zugehörige Gruppen und Rollen							
Gesicherte Funktion	**Gruppe oder Rolle**	**Berechtigungsstufe**	**Berechtigungstyp**				
			Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Repository-Verbindungen verwalten	Verzeichnisadministratoren	Zuordnen				✓	✓
Externe Dokumente anzeigen	Verzeichnisadministratoren	Zuordnen				✓	✓
	Jeder	Zugriff			✓		✓

CSV-Ausgabe generieren

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 124. Generieren von CSV-Ausgabefunktionen und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓
Jeder	Zugriff			✓		✓

PDF-Ausgabefunktion generieren

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 125. PDF-Ausgabefunktionalität und Berechtigungen für zugehörige Gruppen und Rollen generieren						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓
Jeder	Zugriff			✓		✓

XLS-Ausgabefunktion generieren

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 126. XLS-Ausgabefunktion und Berechtigungen für zugehörige Gruppen und Rollen generieren						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓
Jeder	Zugriff			✓		✓

XML-Ausgabefunktion generieren

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 127. Generieren von XML-Ausgabefunktionen und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Verzeichnisadministratoren	Zuordnen				✓	✓
Jeder	Zugriff			✓		✓

Glossar-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 128. Glossarfunktion und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Jeder	Zuordnen			✓		✓
Verzeichnisadministratoren	Zugriff				✓	✓

Funktion 'Einträge ausblenden'

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 129. Funktionen für Einträge ausblenden und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Jeder	Zuordnen			✓		✓
Verzeichnisadministratoren	Zugriff				✓	✓

Funktionalität für relationale Metadaten importieren

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 130. Funktionalität und Berechtigungen für relationale Metadaten für zugehörige Gruppen und Rollen importieren

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Verzeichnisadministratoren	Zuordnen				✓	✓
Berichtsadministratoren	Zugriff			✓		✓

Jobfunktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 131. Jobfunktion und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Analyse-Explorers	Zugriff			✓		✓
Analysebenutzer	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓
11.1.7 -Berichtsadministratoren	Zugriff			✓		✓

Abstammungsfunktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 132. Lineage-Funktionalität und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Jeder	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓

Content-Funktionalität verwalten

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 133. Verwalten von Inhaltsfunktionen und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Bibliotheksadministratoren Mobile Administratoren Portaladministratoren PowerPlay-Administratoren Berichtsadministratoren Serveradministratoren	Zugriff			✓		✓
Verzeichnisadministratoren	Verwalten			✓	✓	✓

Eigene Datenquellensignonenfunktion verwalten

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 134. Eigene Datenquellensignonenfunktionen und Berechtigungen für zugehörige Gruppen und Rollen verwalten						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen 	**Schreiben** 	**Ausführen** 	**Richtlinie festlegen** 	**Traverse** 
Verzeichnisadministratoren	Zuordnen				✓	✓

Metrik Studio-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 135. Metrik-Studio-Funktion und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen 	**Schreiben** 	**Ausführen** 	**Richtlinie festlegen** 	**Traverse** 
Analyse-Explorers	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓

Die gesicherten Features in der folgenden Tabelle sind untergeordnete Elemente der Metric Studio-Funktion.

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 136. Gesicherte Funktionen der Metric Studio-Funktion und der Berechtigungen für zugehörige Gruppen und Rollen								
Gesicherte Funktion	**Gruppe oder Rolle**	**Berechtigungsstufe**	**Berechtigungstyp**					
			Lesen 	**Schreiben** 	**Ausführen** 	**Richtlinie festlegen** 	**Traverse** 	
Ansicht bearbeiten	Analyse-Explorers	Zugriff			✓		✓	
	Verzeichnisadministratoren	Zuordnen				✓	✓	

Mobile Funktionalität

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 137. Funktion und Berechtigungen von Cognos Analytics Mobile Reports für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Verzeichnisadministratoren	Zuordnen				✓	✓
Analyseanzeigefunktionen	Zugriff			✓		✓
Mobile Administratoren	Zugriff			✓		✓
Mobile Benutzer	Zugriff			✓		✓

Notizbuchfunktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 138. Notizbuchfunktion und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Verzeichnisadministratoren	Zuordnen				✓	✓

Planungsmitarbeiterfunktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 139. Planungsfunktion und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓

PowerPlay Studio-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 140. PowerPlay Studio-Funktion und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verfasser	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓
Modellierungsprogramme	Zugriff			✓		✓
PowerPlay -Administratoren	Zugriff			✓		✓
PowerPlay -Benutzer	Zugriff			✓		✓

Query Studio-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 141. Query Studio-Funktion und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verfasser	Zugriff			✓		✓

Tabelle 141. Query Studio-Funktion und Berechtigungen für zugehörige Gruppen und Rollen (Forts.)						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓
Modellierungsprogramme	Zugriff			✓		✓
Benutzer abfragen	Zugriff			✓		✓
Berichtsadministratoren	Zugriff			✓		✓

Die gesicherten Features in der folgenden Tabelle sind untergeordnete Elemente der Query Studio-Funktion.

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 142. Gesicherte Funktionen der Query Studio-Funktion und der Berechtigungen für zugehörige Gruppen und Rollen								
Gesicherte Funktion	**Gruppe oder Rolle**	**Berechtigungsstufe**	**Berechtigungstyp**					
			Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Erstellen Erweitert	Verfasser	Zugriff			✓		✓
	Modellierungsprogramme	Zugriff			✓		✓
	Benutzer abfragen	Zugriff			✓		✓
	Berichtsadministratoren	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓

Report Studio-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 143. Funktion und Berechtigungen von Reporting für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verfasser	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓
Bibliotheksadministratoren	Zugriff			✓		✓
Modellierungsprogramme	Zugriff			✓		✓
Berichtsadministratoren	Zugriff			✓		✓

Die gesicherten Features in der folgenden Tabelle sind untergeordnete Elemente der Funktion Reporting .

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 144. Gesicherte Funktionen der Reporting -Funktionalität und -Berechtigungen für zugehörige Gruppen und Rollen								
Gesicherte Funktion	**Gruppe oder Rolle**	**Berechtigungsstufe**	**Berechtigungstyp**					
			Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Platzen HTML-Elemente im Bericht Benutzerdefiniertes SQL Erstellen/Löschen	Verfasser	Zugriff			✓		✓
	Bibliotheksadministratoren	Zugriff			✓		✓
	Modellierungsprogramme	Zugriff			✓		✓
	Berichtsadministratoren	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓
Externe Daten zulassen	Verzeichnisadministratoren	Zuordnen				✓	✓
	Bibliotheksadministratoren	Zugriff					

In Cloud-Funktion speichern

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 145. Funktionalität und Berechtigungen für zugehörige Gruppen und Rollen in Cloud speichern

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Analyse-Explorers	Zugriff			✓		✓
Analysebenutzer	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓
Berichtsadministratoren	Zugriff			✓		✓

Das gesicherte Feature in der folgenden Tabelle ist ein untergeordnetes Element der Funktion "In Cloud speichern".

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 146. Gesicherte Funktionen der Funktion "In Cloud speichern" und Berechtigungen für zugehörige Gruppen und Rollen

Gesicherte Funktion	Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
			Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Verbindungen verwalten	Verzeichnisadministratoren	Zuordnen				✓	✓
	Berichtsadministratoren	Zugriff			✓		✓

Planungsfunktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 147. Planungsfunktion und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Analysebenutzer	Zugriff			✓		✓
Verfasser	Zugriff			✓		✓
Verbraucher	Angepasst					✓
Verzeichnisadministratoren	Zuordnen				✓	✓
Modellierungsprogramme	Zugriff			✓		✓
PowerPlay -Administratoren	Zugriff			✓		✓
PowerPlay -Benutzer	Zugriff			✓		✓
Benutzer abfragen	Zugriff			✓		✓
Berichtsadministratoren	Zugriff			✓		✓

Die gesicherten Features in der folgenden Tabelle sind untergeordnete Elemente der Planungsfunktion.

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 148. Gesicherte Funktionen der Planungsfunktion und der Berechtigungen für zugehörige Gruppen und Rollen

Gesicherte Funktion	**Gruppe oder Rolle**	**Berechtigungsstufe**	**Berechtigungstyp**				
			Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Terminieren nach Tag Zeitplan nach Stunde Zeitplan für Minute Zeitplan nach Monat Zeitplan nach Auslöser Zeitplan für Woche Zeitplan für Jahr	Analysebenutzer	Zugriff			✓		✓
	Verfasser	Zugriff			✓		✓
	Verbraucher	Angepasst (Ausnahme: Zeitplan für Tag, wobei Berechtigungsstufe = Zugriff)					✓
	Verzeichnisadministratoren	Zuordnen				✓	✓
	Modellierungsprogramme	Zugriff			✓		✓
	Benutzer abfragen	Zugriff			✓		✓
	Berichtsadministratoren	Zugriff			✓		✓
	PowerPlay-Administratoren	Zugriff			✓		✓
	PowerPlay-Benutzer	Zugriff			✓		✓
Terminierungspriorität	Berichtsadministratoren	Zugriff			✓		✓
	Verzeichnisadministratoren	Zuordnen				✓	✓
	PowerPlay-Administratoren	Zugriff			✓		✓

Funktion des Self-Service-Paketassistenten

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 149. Funktion des Self-Service-Paketassistenten und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Verzeichnisadministratoren	Verwalten			✓	✓	✓

Funktionalität für eintragsspezifische Funktionen festlegen

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 150. Funktion für eintragsspezifische Funktionen und Berechtigungen für zugehörige Gruppen und Rollen festlegen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Verzeichnisadministratoren	Zuordnen				✓	✓

Share Pin Board

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 151. Funktion und Berechtigungen für verwandte Gruppen und Rollen mit dem Pin-Board teilen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Analyse-Explorers	Zugriff			✓		✓
Analysebenutzer	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓

Tabelle 151. Funktion und Berechtigungen für verwandte Gruppen und Rollen mit dem Pin-Board teilen (Forts.)						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Berichtsadministratoren	Zugriff			✓		✓

Funktionalität für Momentaufnahmen

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 152. Funktionen für Momentaufnahmen und Anfangsberechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓
Jeder	Zugriff			✓		✓
Modellierungsprogramme	Zugriff			✓		✓

Spezifikationsausführungsfunktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 153. Funktionalität für Spezifikationsausführung und Anfangsberechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓

Dateien hochladen, Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 154. Hochladen von Dateifunktionen und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Jeder	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓
Analyseanzeigefunktionen	Angepasst			Berechtigung verweigert		Berechtigung verweigert
Modellierungsprogramme	Zugriff			✓		✓

Visualisierungsalerts-Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 155. Funktionen zur Visualisierung von Alerts und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Analyse-Explorers	Zugriff			✓		✓
Analysebenutzer	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓
Berichtsadministratoren	Zugriff			✓		✓

Überwachungsregeln, Funktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 156. Überwachungsregeln und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Analysebenutzer	Zugriff			✓		✓
Verfasser	Zugriff			✓		✓
Verbraucher	Zugriff			✓		✓
Verzeichnisadministratoren	Zuordnen				✓	✓
Modellierungsprogramme	Zugriff			✓		✓
PowerPlay-Administratoren	Zugriff			✓		✓
PowerPlay-Benutzer	Zugriff			✓		✓
Benutzer abfragen	Zugriff			✓		✓
Berichtsadministratoren	Zugriff			✓		✓

Webbasierte Modellierungsfunktion

In der folgenden Tabelle gibt ein Häkchen (✓) an, dass eine Berechtigung für eine Gruppe oder eine Rolle für ein Objekt erteilt wird.

Tabelle 157. Webbasierte Modellierungsfunktionalität und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓
Analyseanzeigefunktionen	Angepasst			Berechtigung verweigert		Berechtigung verweigert
Jeder	Zugriff			✓		✓
Modellierungsprogramme	Zugriff			✓		✓

Anhang D. Lokalisierung von Beispieldatenbanken

Die Beispieldatenbanken, die mit IBM Cognos -Software bereitgestellt werden, veranschaulichen eine mehrsprachige Berichtsumgebung.

Die Beispiele speichern eine Auswahl von Textfeldern, wie Namen und Beschreibungen, in 23 Sprachen.

Dieser Anhang enthält Informationen dazu, wie Daten in den Beispieldatenbanken gespeichert werden und wie die Beispieldatenbanken für die Verwendung mehrsprachiger Daten eingerichtet werden.

Weitere Informationen zu den Beispielen finden Sie unter *Handbuch für IBM Cognos Analytics Beispiele*.

Eine Spalte pro Sprache

In dieser Struktur enthalten Tabellen Gruppen von 23 Spalten, eine für jede Sprache.

Es wird eine logische Namenskonvention verwendet, um anzugeben, welche Sprache eine Spalte enthält. Der Name der einzelnen Spalten endet mit einem Sprachencode-Suffix, wie z. B. _EN für Englisch und _FR für Französisch. Die Spalte, die Informationen zu Ländern und Regionen enthält, wird beispielsweise COUNTRY_FR für französische Daten und COUNTRY_DE für deutsche Daten genannt. Alle Tabellen verwenden diese Struktur, mit Ausnahme von PRODUCT_LOOKUP.

Festlegen der Sprache (Spalten) im Modell

In Framework Manager können Sie ein Makro in das SQL der Datenquellenabfrage einfügen, um eine bestimmte Datenspalte zurückzugeben. Das Abfragesubjekt verwendet das Makro, um die Ländereinstellung anzuwenden und einen Sprachencode zurückzugeben. Die Ländereinstellung gibt linguistische Informationen und kulturelle Konventionen für den Zeichentyp, die Sortierfolge, das Format von Datum und Uhrzeit, die Währungseinheit und die Nachrichten an.

Das Makro 'runLocale' verwendet eine Parameterzuordnung, um die gewünschte Inhaltssprache des Benutzers in einen vollständigen oder partiellen Spaltennamen zu konvertieren. Dieser Spaltenname wird dann in der SQL ersetzt, bevor die Abfrage ausgeführt wird.

Da die Beispieldatenbanken einen Sprachencode als Suffix für den Spaltennamen verwenden, verwendet das Makro eine Parameterzuordnung, um gültige Ausführungsorte in einen Sprachencode zu konvertieren, und verknüpft dann den Sprachencode mit dem Namen der Basisspalte.

Beispielabfrage

Das Makro in dieser Beispielabfrage verwendet die Sitzungsvariable 'runLocale' als Parameterzuordnungsschlüssel 'Language_lookup'.

Sie gibt den Sprachencode zurück, der als Suffix des Spaltennamens verwendet werden soll. In der folgenden Anweisung SELECT, bei der Französisch die Sprache ist, generiert das Makro den Spaltennamen COUNTRY_FR.

```
Select
COUNTRY.COUNTRY_CODE,
#'COUNTRY.COUNTRY_' + $Language_lookup{$runLocale}# as
Product_Line
from
[great_outdoors].COUNTRY
```

Da Framework Manager flexibel ist, müssen Ihre mehrsprachigen Spalten nicht das in den Beispielen verwendete Namenssystem verwenden. In der Tat können Ihre mehrsprachigen Spalten ein beliebiges Benennungssystem verwenden. Sie können Ihr Benennungsschema nach Bedarf in die Parameterzuordnung codieren. Sie können jede Sitzungsvariable als Parameterzuordnungsschlüssel verwenden und eine beliebige SQL-Syntax zurückgeben, die Sie zur Laufzeit ersetzen müssen. Weitere Informationen finden Sie im Framework Manager *Benutzerhandbuch*.

Eine Zeile pro Sprache

In dieser Struktur verfügt jeder Zeichenfolgewert über eine separate Zeile mit einer Codespalte, die die Sprache identifiziert.

Die Daten werden gefiltert, um nur die Zeile zurückzugeben, die die erforderlichen Sprachdaten enthält. In der Regel werden mehrsprachige Daten in einer separaten Tabelle gespeichert, um Duplikate nicht beschreibender oder einsprachiger Daten zu vermeiden.

In den Beispieldatenbanken enthält die Datentabelle die Primärschlüsseldaten und die einsprachigen Daten, wie z. B. die Datumsinformationen. Die mehrsprachige Tabelle enthält Daten und einen zusammengesetzten Schlüssel, der sich aus dem Fremdschlüssel und dem Sprachencode zusammensetzt. Die Tabelle PRODUCT_NAME_LOOKUP enthält beispielsweise die Spalten PRODUCT_NUMBER, PRODUCT_LANGUAGE und PRODUCT_NAME, wobei PRODUCT_NUMBER und PRODUCT LANGUAGE den Primärschlüssel bilden. Jeder der lokalisierten Artikel wird in 23 Zeilen ausgedrückt, einer für jede Sprache.

Die folgende Fremdschlüsseltabelle enthält ein oder mehrere lokalisierte Elemente.

Tabelle 158. Beispiel für eine Fremdschlüsseltabelle, die lokalisierte Elemente enthält

Primärschlüsseltabelle	**Fremdschlüsseltabelle**	**Datenbank**
PRODUKT	PRODUKTNAME _LOOKUP	GOSALES
SLS PRODUCT DIM	SLS_PRODUCT _LOOKUP	GOSALESDW

Die Beispieldatenbanken verwenden die ISO-Sprachencodes, um jede Datenzeile zu identifizieren.

Festlegen der Sprache (Zeilen) im Modell

In Framework Manager können Sie ein Makro in das SQL der Datenquellenabfrage einfügen, um eine bestimmte Datenzeile zurückzugeben.

Das Abfragesubjekt verwendet das Makro, um die Ländereinstellung anzuwenden und einen Sprachencode zurückzugeben.

Beispielabfrage

Das Makro in der folgenden Beispielabfrage verwendet die Sitzungsvariable 'runLocale' als Parameterzuordnungsschlüssel 'Language_lookup' und gibt den entsprechenden Sprachencode zurück. Die Funktion sq () gibt an, dass der Rückgabewert des Makros in einfache Anführungszeichen eingeschlossen werden soll, um ein gültiges SQL-Filterprädikat zu erzeugen. In der folgenden Select-Anweisung, wo Deutsch die Sprache ist, identifiziert das Makro die Sprache als DE (Deutsch) und Produkt den Filter (PRODUCT_MULTILINGUAL. "LANGUAGE" = 'DE ').

```
Select
P.INTRODUCTION_DATE,
P.PRODUCT_TYPE_CODE,
P.PRODUCTION_COST,
P.MARGIN,
PRODUCT_LOOKUP.PRODUCT_NUMBER as PRODUCT_NUMBER1,
PRODUCT_LOOKUP."PRODUCT_LANGUAGE",
PRODUCT_LOOKUP.PRODUCT_NAME,
PRODUCT_LOOKUP.PRODUCT_DESCRIPTION
From
gosales].PRODUCT as P,
[gosales].PRODUCT_LOOKUP
Where
P.PRODUCT_NUMBER = PRODUCT_LOOKUP.PRODUCT_NUMBER
and
(PRODUCT_LOOKUP."PRODUCT_LANGUAGE" = #sq($Language_lookup{$runLocale})#)
```

Transliterationen und Multiscript-Erweiterungen

Für die Transliteration asiatischer Sprachen enthält eine Tabelle zwei Spalten mit gleichwertigen Informationen.

In einer Spalte werden Zeichenfolgewerte mit nur lateinischen Zeichen angezeigt. Die andere Spalte enthält Zeichenfolgewerte, die sowohl asiatische als auch lateinische Zeichen verwenden. Die Namenskonvention besteht darin, das Suffix _MB hinzuzufügen.

In den Spalten 'Nur lateinisch' definiert die Transliteration das phonetische Äquivalent des Werts, der in der Spalte '_MB' definiert ist.

Die folgenden Tabellen enthalten Spalten, die transliterierte Werte enthalten.

Tabelle 159. Spalten mit äquivalenten, übersetzten Werten, Beispiel

Tabelle	**Datenbank**
ORDER_HEADER	GOSALES
EINZELHÄNDLER	GOSALES
HÄNDLER-SITE _MB	GOSALES
VERZWEIGUNG	GOSALES
MITARBEITER	GOSALES

Transliterationen im Modell

Im folgenden Beispiel wird eine einzelne Datenquelle erstellt, die auf einem Abfragesubjekt von zwei Tabellen basiert. Die Tabellen sind identisch mit Ausnahme der Verwendung asiatischer Zeichen in einer Tabelle.

Spalte mit Namen, die mit dem Suffix _MB enden, speichern asiatische Daten, die asiatische Zeichen verwenden, wie z. B. chinesische Ideogramme. Dadurch wird eine gewisse Duplizierung entfernt und die Definition von Beziehungen zu anderen Abfragesubjekten im Modell vereinfacht.

```
Select
RS.RTL_RETAILER_SITE_CODE,
RS.RTL_RETAILER_CODE,
RS.RTL_ADDRESS1,
RS.RTL_ADDRESS2,
RS.RTL_CITY,
RS.RTL_REGION,
RS.RTL_POSTAL_ZONE,
RS.RTL_COUNTRY_CODE,
RS.RTL_ACTIVITY_STATUS_CODE,
RS_MB.RTL_ADDRESS1 as Address1_MB,
RS_MB.RTL_ADDRESS2 as Address2_MB,
RS_MB.RTL_CITY as City_MB,
RS_MB.RTL_REGION as Region_MB
from
[goretailers].RETAILER_SITE as RS,
[goretailers].RETAILER_SITE_MB
as RS_MB
where
RETAILER_SITE.RETAILER_SITE_CODE = RETAILER_SITE_MB.RETAILER_SITE_CODE
```

Multiscripterweiterungen

Nachdem Sie die Abfragesubjekte im Modell definiert haben, werden Elemente mit der Erweiterung _MB in einer Multiscript-Erweiterung umbenannt, z. B. Adresse 1 (Multiscript), um die Verwendung und Lesbarkeit zu erleichtern.

Multi-Script-Erweiterungen für bedingte Formatierung verwenden

Ein Beispiel für die Verwendung mehrerer Scripts ist eine Mailing-Adresse, in der die Multiscript-Werte sicherstellen, dass die Mailing-Beschriftungen für die lokale Verarbeitung und Zustellung formatiert werden.

Um den Mailing-Labels mehr Wert zu verleihen, wendet das Modell GO Sales and Retailers bedingte Formatierungen an, um internationale Adressformate zu generieren.

Im folgenden Beispiel ist die Adresszeile 3 der Name einer benutzerdefinierten Berechnung, die zum Generieren von Zeile 3 eines Mailing-Labels verwendet wird. Der Ausdruck verwendet einen Country-oder Regionscodewert, um anzugeben, wie die Zeile formatiert werden soll.

```
if ([Retailers].[Retailer
site].[Country or region code] = 6) then
(' ' + [Retailers].[Retailer
site].[Address 1 (multiscript)])
else
if ([Retailers].[Retailer site].[Country or region
code] = 8) then
([Retailers].[Retailer site].[Address
2 (multiscript)])
else
if ([Retailers].[Retailer site].[Country or region
code] = 13) then
([Retailers].[Retailer site].[Region
(multiscript)] + ' ' + [Retailers].[Retailer
site].[City (multiscript)]
+ ' ' + [Retailers].[Retailer
site].[Address 1 (multiscript)] + '
' + [Retailers].[Retailer site].[Address
2 (multiscript)])
else
if ([Retailers].[Retailer site].[Country or region
code] = 14) then
([Retailers].[Retailer site].[Address
2 (multiscript)])
else
([Retailers].[Retailer site].[Address
1 (multiscript)])
```

Multiscripterweiterungen ermöglichen einem Benutzer in jeder Sprache die Verwendung derselben Modellspalten, um einen Adressblock zu erstellen, und die Adresse, die für jeden Bereitstellungsort ordnungsgemäß formatiert ist, zu sehen. Weitere Informationen finden Sie in den Abfragesubjekten für die Mailing-Adressdatenquelle im Beispielmodell 'gosales_goretailers'.

Anhang E. Schema für Datenquellenbefehle

Wenn Sie mit Datenquellenverbindungen arbeiten, können Sie auch Datenquellbefehle hinzufügen oder bearbeiten.

Datenquellenbefehle werden ausgeführt, wenn die Abfragesteuerkomponente bestimmte Aktionen für eine Datenbank ausführt, z. B. eine Verbindung zum Öffnen einer Verbindung oder zum Schließen einer Benutzersitzung. Sie können z. B. Datenquellenbefehle verwenden, um eine Oracle-Proxy-Verbindung oder eine virtuelle private Datenbank einzurichten. Weitere Informationen finden Sie unter „IBM Cognos-Kontext an eine Datenbank übergeben" auf Seite 145.

Ein Datenquellenbefehlsblock ist ein XML-Dokument, das verwendet wird, um die Befehle anzugeben, die die Datenbank ausführen soll.

Dieses Dokument enthält Referenzmaterial zu jedem Element im XML-Schema, das die Befehlsblöcke definiert.

Nach der Beschreibung der einzelnen Elemente werden die einzelnen Abschnitte beschrieben.

· die untergeordneten Elemente, die das Element haben kann oder haben muss

· Übergeordnete Elemente, die das Element enthalten können

Es gibt auch Codebeispiele, die zeigen, wie Elemente in einem Befehlsblock verwendet werden können.

Die Liste der untergeordneten Elemente für jedes Element wird als DTD-Modellgruppe dargestellt, und die Elemente werden in der Reihenfolge aufgelistet, in der sie auftreten müssen. Die folgende Standardnotation wird verwendet.

Tabelle 160. Standardschreibweise für die Bearbeitung von Datenquellenbefehlen

Symbol	**Bedeutung**
Pluszeichen (+)	Das vorhergehende Element kann mehr als einmal wiederholt werden, muss aber mindestens einmal auftreten.
Fragezeichen (?)	Das vorhergehende Element ist optional. Es darf nicht fehlen, oder es kann genau einmal vorkommen.
Stern (*)	Ein Stern (*) nach einem Element gibt an, dass das Element optional ist. Es kann null oder mehr Zeit auftreten.
Keine	Wenn für ein Element kein Pluszeichen (+), ein Fragezeichen (?) oder ein Stern (*) folgt, muss das Element nur ein einziges Mal vorkommen.
Runde Klammern	Klammergruppenelemente. Elementgruppen werden unter Verwendung der gleichen Symbole wie Elemente gesteuert.
Bar (|)	Ein Balken (|) zwischen Elementen gibt an, dass eines der aufgelisteten Elemente vorhanden sein muss.
Komma (,)	Die Elemente, die sie voneinander trennen, müssen in der angegebenen Reihenfolge vorhanden sein.

Befehlsblock

Definiert eine Gruppe von Befehlen, die von der Datenbank ausgeführt werden, wenn bestimmte Ereignisse auftreten. Dies ist das Stammelement des Schemas.

Untergeordnete Elemente des Elements 'commandBlock'

(Befehle) +

Übergeordnete Elemente des Elements 'commandBlock'

Das Element 'commandBlock' verfügt über keine übergeordneten Elemente.

Befehle

Gibt die Gruppe von Befehlen an, die von der Datenbank ausgeführt werden. Die Befehle werden in der Reihenfolge ausgeführt, in der sie innerhalb des Befehlsblocks angezeigt werden.

Hier ist ein Beispiel dafür, wie Sie dieses Element in einem Befehlsblock verwenden können.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

Untergeordnete Elemente von Befehlen Element

(sessionStartCommand|sessionEndCommand|setCommand|sqlCommand) *

Übergeordnete Elemente des Befehls 'Element'

Befehlsblock

sessionStartCommand

Definiert einen Befehl, der zum Starten einer Proxysitzung in der Datenbank verwendet wird.

Pro Befehlsblock sollte nur ein Befehl sessionStartCommand vorhanden sein. Wenn der Befehlsblock mehr als einen Befehl sessionStartCommand enthält, wird nur der letzte Befehl verwendet, um eine Proxy-Sitzung zu erstellen.

Hier ist ein Beispiel dafür, wie Sie dieses Element in einem Befehlsblock verwenden können.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
        <argument>
            <name>OCI_ATTR_PASSWORD</name>
            <value>password1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
```

Untergeordnete Elemente von sessionStartCommand-Element

(Argumente) ?

Übergeordnete Elemente des Elements "sessionStartCommand"

Befehle

sessionEndCommand

Definiert einen Befehl, der zum Beenden einer Proxysitzung in der Datenbank verwendet wird.

Wenn kein Befehl sessionEndCommand angegeben wird, wird die Proxysitzung beim Trennen der Verbindung zur Datenbank beendet.

Hier ist ein Beispiel dafür, wie Sie dieses Element in einem Befehlsblock verwenden können.

```
<commandBlock>
  <commands>
    <sessionEndCommand>
      <arguments/>
    </sessionEndCommand>
  </commands>
</commandBlock>
```

Untergeordnete Elemente des Elements "sessionEndCommand"

(Argumente) ?

Übergeordnete Elemente des Elements "sessionEndCommand"

Befehle

Argumente

Gibt die Argumentwerte an, die mit dem Befehl verwendet werden sollen.

Hier ist ein Beispiel dafür, wie Sie dieses Element in einem Befehlsblock verwenden können.

```
<commandBlock>
  <commands>
    <sessionEndCommand>
      <arguments/>
    </sessionEndCommand>
  </commands>
</commandBlock>
```

Untergeordnete Elemente von Argumenten-Element

(Argument) *

Übergeordnete Elemente des Argumenten-Elements

- sessionStart
- sessionEnd

Argument

Definiert einen Argumentwert für einen Aufruf an eine Datenbank-API.

Hier ist ein Beispiel dafür, wie Sie dieses Element in einem Befehlsblock verwenden können.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
        <argument>
            <name>OCI_ATTR_PASSWORD</name>
            <value>password1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

Untergeordnete Elemente des Argumentelements

(Name und Wert)

Übergeordnete Elemente des Argumentelements

Argumente

setCommand

Dieses Element ist für die zukünftige Verwendung reserviert.

sqlCommand

Definiert einen Befehl, der eine native SQL-Anweisung darstellt, die von der Datenbank ausgeführt werden soll.

Hier ist ein Beispiel dafür, wie Sie dieses Element in einem Befehlsblock verwenden können.

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql> BEGIN PKG1.STORED_PROC1; END; </sql>
    </sqlCommand>
  </commands>
</commandBlock>
```

Untergeordnete Elemente von sqlCommand-Element

(SQL)

Übergeordnete Elemente von sqlCommand-Element

Befehle

SQL

Gibt die SQL-Anweisung an, die für die Datenbank ausgeführt werden soll. Die SQL-Anweisung muss sich in nativem SQL befinden.

Hier ist ein Beispiel dafür, wie Sie dieses Element in einem Befehlsblock verwenden können.

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql> BEGIN PKG1.STORED_PROC1; END; </sql>
    </sqlCommand>
```

```
  </commands>
</commandBlock>
```

Untergeordnete Elemente von SQL-Element

Das SQL-Element weist keine untergeordneten Elemente auf.

Übergeordnete Elemente des SQL-Elements

sqlCommand

Name

Gibt das Argument an, das festgelegt werden soll.

Der Wert des Elements name muss einer der folgenden Werte sein:

- OCI_ATTR_USERNAME
- OCI_ATTR_PASSWORD

Hier ist ein Beispiel dafür, wie Sie dieses Element in einem Befehlsblock verwenden können.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

Untergeordnete Elemente des Namenselements

Das Namenselement weist keine untergeordneten Elemente auf.

Übergeordnete Elemente des Namenselements

- Argument
- setCommand

Wert

Gibt den Wert an, der für das Argument verwendet werden soll.

Hier ist ein Beispiel dafür, wie Sie dieses Element in einem Befehlsblock verwenden können.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
      </arguments/>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

Untergeordnete Elemente des Wertelements

Das Wertelement weist keine untergeordneten Elemente auf.

Übergeordnete Elemente des Wertelements

- Argument
- setCommand

Anhang F. Datenschema für Protokollnachrichten

Wenn Sie die IBM Cognos -Software so konfigurieren, dass Protokollnachrichten an eine Datenbank gesendet werden, werden die Tabellen und die Spalten in jeder Tabelle automatisch erstellt, wenn Sie die IBM Cognos -Services starten.

Um Namenskonflikte mit Datenbankschlüsselwörtern zu vermeiden, weisen alle Spaltennamen in der Protokolldatenbank das Präfix "COGIPF" auf. Wenn Sie Ihr eigenes Protokolldatenbankmodell erstellt haben, müssen Sie das Präfix "COGIPF" zu den Spaltennamen der Protokolldatenbanktabellen im Modell hinzufügen.

Tabellendefinitionen

Protokollnachrichten werden unter bestimmten Bedingungen in einer Tabelle in der Protokollierungsdatenbank aufgezeichnet. Diese Bedingungen hängen von der Protokollierungsstufe ab, die Sie im Webportal konfigurieren.

Informationen zu Protokollierungsstufen finden Sie unter „Protokollnachrichten“ auf Seite 16.

Wenn sich ein Benutzer bei der IBM Cognos -Software anmeldet, wird eine Sitzungs-ID in allen Protokollnachrichten zugeordnet und aufgezeichnet. Sie können die Sitzungs-ID verwenden, um alle Aktionen zu identifizieren, die von einem Benutzer ausgeführt werden.

Tabelle COGIPF_ACTION

Speichert Informationen zu Operationen, die für Objekte ausgeführt werden.

Tabelle 161. Tabellenspalten, Beschreibungen und Datentypen von COGIPF_ACTION

Spaltenname	Beschreibung	Datentyp
COGIPF_HOST_ IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)
COGIPF_HOST_ PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_PROC_ID	Die vom Betriebssystem zugeordnete Prozess-ID.	INTEGER
COGIPF_LOCAL TIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	Die Zeitzone, Offset von GMT	INTEGER
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR (255) NOT NULL
COGIPF_STEPID	Die alphanumerische Kennung für den Schritt innerhalb einer Jobausführung (leer, wenn keine vorhanden ist)	VARCHAR (255)

Tabelle 161. Tabellenspalten, Beschreibungen und Datentypen von COGIPF_ACTION (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_ SUBREQUESTID	Die alphanumerische Kennung der Teilanforderung für die Komponente.	VARCHAR (255)
COGIPF_THREADID	Die alphanumerische Kennung des Threads, auf dem die Anforderung ausgeführt wird.	VARCHAR (255)
COGIPF_ COMPONENTID	Der Name der Komponente, die die Angabe generiert.	VARCHAR (64)
COGIPF_ BUILDNUMMER	Die Hauptbuildnummer für die Komponente, die die Angabe generiert.	INTEGER
COGIPF_ LOG_LEVEL	Die Höhe der Indikation	INTEGER
COGIPF_ OPERATION	Die Aktion, die für das Objekt ausgeführt wurde	VARCHAR (255)
COGIPF_ TARGET_TYPE	Das Objekt, auf dem die Operation ausgeführt wird.	VARCHAR (255)
COGIPF_ TARGET_PATH	Zielobjektpfad	VARCHAR (1024)
COGIPF_STATUS	Der Status der Operation: leer, wenn die Ausführung noch nicht abgeschlossen ist, Erfolg, Warnung oder Fehler.	VARCHAR (255)
COGIPF_ ERRORDETAILS	Fehlerdetails	VARCHAR (2000)

COGIPF_AGENTBUILD-Tabelle

Speichert Informationen über die Zustellung von Agentenmailen.

Tabelle 162. COGIPF_AGENTBUILD-Tabellenspalten, Beschreibungen und Datentypen		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_ HOST_IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)
COGIPF_HOST_PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_PROC_ID	Die vom Betriebssystem zugeordnete Prozess-ID.	INTEGER
COGIPF_ LOCALTIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde.	TIMESTAMP

Tabelle 162. COGIPF_AGENTBUILD-Tabellenspalten, Beschreibungen und Datentypen (Forts.)

Spaltenname	Beschreibung	Datentyp
COGIPF_TIMEZONE_ OFFSET	Die Zeitzone, Offset von GMT	INTEGER
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR (255) NOT NULL
COGIPF_STEPID	Die alphanumerische Kennung für den Schritt innerhalb einer Jobausführung (leer, wenn keine vorhanden ist)	VARCHAR (255)
COGIPF_ SUBREQUESTID	Die alphanumerische Kennung der Teilanforderung für die Komponente.	VARCHAR (255)
COGIPF_THREADID	Die alphanumerische Kennung des Threads, auf dem die Anforderung ausgeführt wird.	VARCHAR (255)
COGIPF_ COMPONENTID	Der Name der Komponente, die die Angabe generiert.	VARCHAR (64)
COGIPF_BUILD NUMBER	Die Hauptbuildnummer für die Komponente, die die Angabe generiert.	INTEGER
COGIPF_LOG_LEVEL	Die Höhe der Indikation	INTEGER
COGIPF_OPERATION	Die Operation	VARCHAR (128)
COGIPF_ TARGET_TYPE	Das Objekt, auf dem die Operation ausgeführt wird.	VARCHAR (255)
COGIPF_TARGET_ NAME	Der Zielname.	VARCHAR (512)
COGIPF_ TARGET_PATH	Zielpfad	VARCHAR (1024)
COGIPF_STATUS	Der Status der Operation: Leerzeichen, Erfolg, Warnung oder Fehler.	VARCHAR (255)
COGIPF_ ERRORDETAILS	Fehlerdetails	VARCHAR (2000)
COGIPF_AGENT_ PATH	Der Agentenname	VARCHAR (1024)

Tabelle 162. COGIPF_AGENTBUILD-Tabellenspalten, Beschreibungen und Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_ SCHEDULETIME	Die Zielzeitplanzeit	INTEGER
COGIPF_USER	Der Benutzer, der den Agenten erstellt hat.	VARCHAR (512)
COGIPF_EMAIL	Die E-Mail-Adresse	VARCHAR (512)

COGIPF_AGENTRUN-Tabelle

Speichert Informationen über die Agentenaktivität einschließlich Tasks und Zustellung.

Tabelle 163. COGIPF_AGENTRUN, Tabellenspalten, Beschreibungen und Datentypen		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_ HOST_IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)
COGIPF_HOST_PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_PROC_ID	Die vom Betriebssystem zugeordnete Prozess-ID.	INTEGER
COGIPF_ LOCALTIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde.	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	Die Zeitzone, Offset von GMT	INTEGER
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR (255) NOT NULL
COGIPF_STEPID	Die alphanumerische Kennung für den Schritt innerhalb einer Jobausführung (leer, wenn keine vorhanden ist)	VARCHAR (255)
COGIPF_ SUBREQUESTID	Die alphanumerische Kennung der Teilanforderung für die Komponente.	VARCHAR (255)
COGIPF_THREADID	Die alphanumerische Kennung des Threads, auf dem die Anforderung ausgeführt wird.	VARCHAR (255)

Tabelle 163. COGIPF_AGENTRUN, Tabellenspalten, Beschreibungen und Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_ COMPONENTID	Der Name der Komponente, die die Angabe generiert.	VARCHAR (64)
COGIPF_BUILD NUMBER	Die Hauptbuildnummer für die Komponente, die die Angabe generiert.	INTEGER
COGIPF_LOG_LEVEL	Die Höhe der Indikation	INTEGER
COGIPF_OPERATION	Die Operation	VARCHAR (128)
COGIPF_ TARGET_TYPE	Das Objekt, auf dem die Operation ausgeführt wird.	VARCHAR (255)
COGIPF_ TARGET_PATH	Zielpfad	VARCHAR (1024)
COGIPF_STATUS	Der Status der Operation: Leerzeichen, Erfolg, Warnung oder Fehler.	VARCHAR (255)
COGIPF_ ERROR_DETAILS	Fehlerdetails	VARCHAR (2000)
COGIPF_AGENTPATH	Der Agentenname	VARCHAR (1024)
COGIPF_ SCHEDULETIME	Die Zielzeitplanzeit	INTEGER
COGIPF_TARGET_ NAME	Der Zielname.	VARCHAR (512)
COGIPF_USER	Der Benutzer, der den Agenten erstellt hat.	VARCHAR (512)
COGIPF_EMAIL	Die E-Mail-Adresse	VARCHAR (512)
COGIPF_MESSAGEID	Die Identifizierung der Nachricht	VARCHAR (255)

COGIPF_ANNOTATIONSERVICE-Tabelle

Speichert Prüfinformationen zu Anmerkungsserviceoperationen.

Weitere Informationen finden Sie unter Kapitel 4, „Systemleistungsmetriken”, auf Seite 25.

Tabelle 164. COGIPF_ANNOTATIONSERVICE-TABELLENSPALTEN, -beschreibungen und -Datentypen		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_ HOST_IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)

Tabelle 164. COGIPF_ANNOTATIONSERVICE-TABELLENSPALTEN, -beschreibungen und -Datentypen (Forts.)

Spaltenname	Beschreibung	Datentyp
COGIPF_HOST_PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_PROC_ID	Die vom Betriebssystem zugeordnete Prozess-ID.	INTEGER
COGIPF_ LOCALTIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	Die Zeitzone, Offset von GMT	INTEGER
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR (255) NOT NULL
COGIPF_STEPID	Die alphanumerische Kennung des Schritts, leer, wenn keine	VARCHAR (255)
COGIPF_SUBREQUESTID	Die alphanumerische Kennung der Unteranforderung.	VARCHAR (255)
COGIPF_ THREADID	Die alphanumerische Kennung des Threads, auf dem die Anforderung ausgeführt wird.	VARCHAR (255)
COGIPF_ COMPONENTID	Der Name der Komponente, die die Angabe generiert.	VARCHAR (64)
COGIPF_BUILDNUMBER	Die Hauptbuildnummer für die Komponente, die die Angabe generiert.	INTEGER
COGIPF_ LOG_LEVEL	Die Höhe der Indikation	INTEGER
COGIPF_OPERATION	Die Aktion, die für das Objekt ausgeführt wurde	VARCHAR (255)
COGIPF_TARGET_TYPE	Der Zieltyp	VARCHAR (255)
COGIPF_ TARGET_PATH	Der Objektpfad	VARCHAR (1024)
COGIPF_ ANMERKUNG	Die alphanumerische Kennung der Anmerkung	BIGINT

Tabelle 164. COGIPF_ANNOTATIONSERVICE-TABELLENSPALTEN, -beschreibungen und -Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_USER	Die Benutzer-ID des Benutzers, der die Operation für die Anmerkung ausgeführt hat, z. B. Erstellen, Aktualisieren oder Löschen.	VARCHAR (1024)
COGIPF_PARENT_ID	Die Identifikation des übergeordneten Objekts.	VARCHAR (1024)
COGIPF_ CREATION_TIME	Das Datum und die Uhrzeit der Erstellung der Anmerkung.	TIMESTAMP
COGIPF_ UPDATE_TIME	Das Datum und die Uhrzeit, zu dem die Anmerkung aktualisiert wurde.	TIMESTAMP

Tabelle COGIPF_EDITQUERY

Speichert Informationen zu Abfrageausführungen.

Tabelle 165. COGIPF_EDITQUERY-Tabellenspalten, Beschreibungen und Datentypen		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_ HOST_IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)
COGIPF_HOST_PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_PROC_ID	Die vom Betriebssystem zugeordnete Prozess-ID.	INTEGER

Tabelle 165. COGIPF_EDITQUERY-Tabellenspalten, Beschreibungen und Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_ LOCALTIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde. Während der Bericht ausgeführt wird, ist dies der Zeitpunkt, an dem die Berichtsausführung gestartet wurde. Nachdem die Ausführung des Berichts abgeschlossen ist, ist dies die Endzeit der Berichtsausführung. Informationen zum Überprüfen, ob die Ausführung abgeschlossen ist, finden Sie unter COGIPF_STATUS. Ein leerer Eintrag bedeutet eine unvollständige Ausführung. Ein ausgefüllter Eintrag bedeutet die Ausführung der Ausführung. Um die Ausführungsstartzeit für einen Bericht zu berechnen, der die Ausführung bereits abgeschlossen hat, subtrahieren Sie COGIPF_RUNTIME von COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	Die Zeitzone, Offset von GMT	INTEGER
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR (255) NOT NULL
COGIPF_STEPID	Die alphanumerische Kennung für den Schritt innerhalb einer Jobausführung (leer, wenn keine vorhanden ist)	VARCHAR (255)
COGIPF_ SUBREQUESTID	Die alphanumerische Kennung der Teilanforderung für die Komponente.	VARCHAR (255)
COGIPF_THREADID	Die alphanumerische Kennung des Threads, auf dem die Anforderung ausgeführt wird.	VARCHAR (255)
COGIPF_ COMPONENTID	Der Name der Komponente, die die Angabe generiert.	VARCHAR (64)
COGIPF_ BUILDNUMMER	Die Hauptbuildnummer für die Komponente, die die Angabe generiert.	INTEGER
COGIPF_LOG_LEVEL	Die Höhe der Indikation	INTEGER

Tabelle 165. COGIPF_EDITQUERY-Tabellenspalten, Beschreibungen und Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_ TARGET_TYPE	Das Objekt, auf dem die Operation ausgeführt wird.	VARCHAR (255)
COGIPF_ QUERYPATH	Der Berichtspfad	VARCHAR (1024)
COGIPF_STATUS	Der Status der Operation: Leerzeichen, Erfolg, Warnung oder Fehler.	VARCHAR (255)
COGIPF_ ERRORDETAILS	Fehlerdetails	VARCHAR (2000)
COGIPF_RUNTIME	Die Anzahl der Millisekunden, die für die Ausführung der Abfrage benötigt wurden.	INTEGER
COGIPF_ QUERYNAME	Der Name des Berichts, der abgefragt wurde.	VARCHAR (512)
COGIPF_PACKAGE	Das Paket, dem der Bericht zugeordnet ist.	VARCHAR (1024)
COGIPF_MODEL	Das Modell, dem der Bericht zugeordnet ist.	VARCHAR (512)

COGIPF_HUMANTASKSERVICE-Tabelle

Speichert Prüfinformationen zu Benutzertaskserviceoperationen (Tasks und entsprechende Taskstatus).

Weitere Informationen finden Sie unter Kapitel 4, „Systemleistungsmetriken”, auf Seite 25.

Tabelle 166. COGIPF_HUMANTASKSERVICE-Tabellenspalten, Beschreibungen und Datentypen		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_ HOST_IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)
COGIPF_HOST_PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_PROC_ID	Die vom Betriebssystem zugeordnete Prozess-ID.	INTEGER
COGIPF_ LOCALTIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde.	TIMESTAMP
COGIPF_ TIMEZONE_OFFSET	Die Zeitzone, Offset von GMT	INTEGER
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)

Tabelle 166. COGIPF_HUMANTASKSERVICE-Tabellenspalten, Beschreibungen und Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR (255)
COGIPF_STEPID	Die alphanumerische Kennung für den Schritt innerhalb einer Jobausführung (leer, wenn keine vorhanden ist)	VARCHAR (255)
COGIPF_SUBREQUESTID	Die alphanumerische Kennung der Unteranforderung.	VARCHAR (255)
COGIPF_ THREADID	Die alphanumerische Kennung des Threads, auf dem die Anforderung ausgeführt wird.	VARCHAR (255)
COGIPF_ BUILDNUMMER	Die Hauptbuildnummer für die Komponente, die die Angabe generiert.	INTEGER
COGIPF_ OPERATION	Die Aktion, die für das Objekt ausgeführt wurde, z. B. ADD, UPDATE	VARCHAR (128)
COGIPF_TARGET_TYPE	Der Zieltyp	VARCHAR (255)
COGIPF_ TARGET_PATH	Der Objektpfad	VARCHAR (1024)
COGIPF_STATUS	Der Status der Operation: leer, wenn die Ausführung noch nicht abgeschlossen ist, Erfolg, Warnung oder Fehler.	VARCHAR (50)
COGIPF_ LOGENTRYID	Der Primärschlüssel, der verwendet wird, um die Tabellen COGIPF_HUMANTASKSERVICE und COGIPF_HUMANTASKSERVICE _DETAIL zu verknüpfen	VARCHAR (50) NOT NULL
COGIPF_TASKID	Die Task-ID	VARCHAR (50)
COGIPF_ TRANSACTION_TYPE	Die Operation, die speziell für den Human Task-Service ausgeführt wird, z. B. 'Claim', 'setPriority', 'getTaskInfo', 'changeSubscription'.	VARCHAR (255)
COGIPF_USER	Der Benutzer, der die Transaktion in COGIPF_TRANSACTION_TYPE ausgeführt hat.	VARCHAR (255)
COGIPF_TASK_PRIORITY	Die Priorität der Task: · 1 = hoch · 3 = mittel · 5 = niedrig	INTEGER

Tabelle 166. COGIPF_HUMANTASKSERVICE-Tabellenspalten, Beschreibungen und Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_TASK_STATUS	Der Status der Aufgabe: leer, wenn die Ausführung noch nicht abgeschlossen ist, Erfolg, Warnung oder Fehler.	VARCHAR (255)
COGIPF_TASK_ ACTIVATION_TIME	Die Zeit, zu der die Task aktiviert wurde. Ein Datums-/Uhrzeitwert, der in der Datenbank in längerer numerischer Form gespeichert wird.	BIGINT
COGIPF_TASK_ EXPIRATION_TIME	Das Datum und die Uhrzeit, zu dem die Task abgelaufen ist	BIGINT
COGIPF_TASKNAME	Der Name der Task.	NTEXT
COGIPF_TASK_SUBJECT	Das Thema der Aufgabe	NTEXT
COGIPF_TASK_ BESCHREIBUNG	Die Beschreibung der Task.	NTEXT
COGIPF_TASK_ TIMEZONEID	Die Zeitzonen-ID der Task.	VARCHAR (50)
COGIPF_TASK_ ACTUAL_OWNER	Der Eigner der Task	VARCHAR (255)
COGIPF_TASK_ INITIATOR	Der Initiator (Ersteller) der Task.	VARCHAR (255)
COGIPF_TASK_CLASS _NAME	Der Name der Taskklasse, für die die Task eine Instanz von ist.	VARCHAR (255)
COGIPF_TASK_ CLASS_OPERATION	Die Aktion, die für das Objekt ausgeführt wurde	VARCHAR (255)
COGIPF_TASK_ COMMENT	Kommentare, die sich auf die Task beziehen	VARCHAR (2048)

COGIPF_HUMANTASKSERVICE_DETAIL Tabelle

Speichert zusätzliche Details zu Benutzertaskserviceoperationen (nicht unbedingt erforderlich für jeden Prüfeintrag, z. B. Benachrichtigungsdetails und Benutzerrollendetails).

Weitere Informationen finden Sie unter Kapitel 4, „Systemleistungsmetriken”, auf Seite 25.

Tabelle 167. COGIPF_HUMANTASKSERVICE_DETAIL-Tabellenspalten, -beschreibungen und -Datentypen		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_ HOST_IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)

Tabelle 167. COGIPF_HUMANTASKSERVICE_DETAIL-Tabellenspalten, -beschreibungen und -Datentypen (Forts.)

Spaltenname	Beschreibung	Datentyp
COGIPF_HOST_PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR (255)
COGIPF_STEPID	Die alphanumerische Kennung des Schritts, leer, wenn keine	VARCHAR (255)
COGIPF_SUBREQUESTID	Die alphanumerische Kennung der SUBanforderung.	VARCHAR (255)
COGIPF_ TASKID	Die alphanumerische Kennung der Task.	VARCHAR (50)
COGIPF_ LOGENTRYID	Der Primärschlüssel, der verwendet wird, um die Tabellen COGIPF_ HUMANTASKSERVICE und COGIPF_HUMANTASKSERVICE _DETAIL zu verknüpfen	VARCHAR (50) NOT NULL
COGIPF_NOTIFICATION_DETAILS	Details zu Benachrichtigungs-E-Mails über die Task	NTEXT
COGIPF_HUMANROLE_USER	Die Benutzer-ID des Benutzers, der eine Rolle für eine Task ausführt. Kombiniert mit COGIPF_HUMANROLE, um die Rolle des Benutzers für die Task zu definieren	VARCHAR (255)
COGIPF_HUMANROLE_ROLE	Die Rolle des Benutzers Kombiniert mit COGIPF_HUMAN_USER, um die Rolle des Benutzers für die Task zu definieren	VARCHAR (50)
COGIPF_SUBSCRIPTION_ OPERATION	Die Subskriptionsoperation, z. B. SUBSCRIBE oder UNSUBSCRIBE	VARCHAR (50)
COGIPF_SUBSCRIPTION_EVENT	Das Taskereignis, für das der Benutzer subskribiert oder abonniert.	SMALLINT
COGIPF_SUBSCRIPTION_USER	Der Benutzer, der ein Taskereignis subskribiert oder abschließt.	VARCHAR (255)
COGIPF_TASK_MESSAGE	Die Tasknachricht	NTEXT

Tabelle 167. COGIPF_HUMANTASKSERVICE_DETAIL-Tabellenspalten, -beschreibungen und -Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_TASK_MESSAGE_TYPE	Der Typ der Nachricht, die in COGIPF_TASK_MESSAGE gespeichert ist. Gültige Werte sind 'INPUT', 'OUTPUT' oder 'FAULT'.	VARCHAR (20)
COGIPF_DETAIL_ID	Die Folgenummer des Detaildatensatzes.	VARCHAR (50) NOT NULL

Tabelle COGIPF_NATIVEQUERY

Speichert Informationen zu Abfragen, die von IBM Cognos -Software zu anderen Komponenten bereitgestellt werden.

Tabelle 168. COGIPF_NATIVEQUERY-Tabellenspalten, -beschreibungen und -Datentypen		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_HOST_ IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)
COGIPF_HOST_ PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_PROC_ID	Die vom Betriebssystem zugeordnete Prozess-ID.	INTEGER
COGIPF_ LOCALTIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	Die Zeitzone, Offset von GMT	INTEGER
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR (255) NOT NULL
COGIPF_STEPID	Die alphanumerische Kennung für den Schritt innerhalb einer Jobausführung (leer, wenn keine vorhanden ist)	VARCHAR2 (255)
COGIPF_ SUBREQUESTID	Die alphanumerische Kennung der Teilanforderung für die Komponente.	VARCHAR (255)

Tabelle 168. COGIPF_NATIVEQUERY-Tabellenspalten, -beschreibungen und -Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_THREADID	Die alphanumerische Kennung des Threads, auf dem die Anforderung ausgeführt wird.	VARCHAR (255)
COGIPF_ COMPONENTID	Der Name der Komponente, die die Angabe generiert.	VARCHAR (64)
COGIPF_ BUILDNUMMER	Die Hauptbuildnummer für die Komponente, die die Angabe generiert.	INTEGER
COGIPF_LOG_LEVEL	Die Höhe der Indikation	INTEGER
COGIPF_ REQUESTSTRING	Die Abfrageanforderungszeichenfolge, die an andere Komponenten gestellt wurde.	NTEXT (1G)

COGIPF_PARAMETER-Tabelle

Speichert Parameterinformationen, die von einer Komponente protokolliert werden.

Tabelle 169. COGIPF_PARAMETER, Tabellenspalten, Beschreibungen und Datentypen		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR (255) NOT NULL
COGIPF_STEPID	Die alphanumerische Kennung für den Schritt innerhalb einer Jobausführung (leer, wenn keine vorhanden ist)	VARCHAR (255)
COGIPF_OPERATION	Die Aktion, die für das Objekt ausgeführt wurde	VARCHAR (255)
COGIPF_TARGET_ TYPE	Das Objekt, auf dem die Operation ausgeführt wird.	VARCHAR (255)
COGIPF_ PARAMETERNAME	Der Name des Parameters, der von einer Komponente protokolliert wird.	VARCHAR (255)
COGIPF_ PARAMETERWERT	Der Wert des Parameters, der von einer Komponente protokolliert wird.	VARCHAR (512)
COGIPF_LOCALTIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde.	TIMESTAMP

Tabelle 169. COGIPF_PARAMETER, Tabellenspalten, Beschreibungen und Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)
COGIPF_SUBREQUESTID	Die alphanumerische Kennung der Teilanforderung für die Komponente.	VARCHAR (255)
COGIPF_PARAMETER_VALUE_BLOB	Eingabeaufforderungsparameter und Berichtslaufoptionen	NTEXT

Tabelle COGIPF_RUNJOB

Speichert Informationen zu Jobausführungen.

Tabelle 170. Tabellenspalten, Beschreibungen und Datentypen von COGIPF_RUNJOB		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_HOST_IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)
COGIPF_HOST_PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_PROC_ID	Die vom Betriebssystem zugeordnete Prozess-ID.	INTEGER
COGIPF_ LOCALTIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde. Während der Bericht ausgeführt wird, ist dies der Zeitpunkt, an dem die Berichtsausführung gestartet wurde. Nachdem die Ausführung des Berichts abgeschlossen ist, ist dies die Endzeit der Berichtsausführung. Informationen zum Überprüfen, ob die Ausführung abgeschlossen ist, finden Sie unter COGIPF_STATUS. Ein leerer Eintrag bedeutet eine unvollständige Ausführung. Ein ausgefüllter Eintrag bedeutet die Ausführung der Ausführung. Um die Ausführungsstartzeit für einen Bericht zu berechnen, der die Ausführung bereits abgeschlossen hat, subtrahieren Sie COGIPF_RUNTIME von COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	Die Zeitzone, Offset von GMT	INTEGER
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR (255) NOT NULL
COGIPF_STEPID	Die alphanumerische Kennung für den Schritt innerhalb einer Jobausführung (leer, wenn keine vorhanden ist)	VARCHAR (255)
COGIPF_SUBREQUESTID	Die alphanumerische Kennung der Teilanforderung für die Komponente.	VARCHAR (255)

Tabelle 170. Tabellenspalten, Beschreibungen und Datentypen von COGIPF_RUNJOB (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_THREADID	Die alphanumerische Kennung des Threads, auf dem die Anforderung ausgeführt wird.	VARCHAR (255)
COGIPF_COMPONENTID	Der Name der Komponente, die die Angabe generiert.	VARCHAR (64)
COGIPF_BUILDNUMBER	Die Hauptbuildnummer für die Komponente, die die Angabe generiert.	INTEGER
COGIPF_LOG_LEVEL	Die Höhe der Indikation	INTEGER
COGIPF_TARGET_TYPE	Das Objekt, auf dem die Operation ausgeführt wird.	VARCHAR (255)
COGIPF_JOBPATH	Der Jobpfad	VARCHAR (512)
COGIPF_STATUS	Der Status der Operation: Leerzeichen, Erfolg, Warnung oder Fehler.	VARCHAR (255)
COGIPF_ ERRORDETAILS	Fehlerdetails	VARCHAR (2000)
COGIPF_RUNTIME	Die Anzahl der Millisekunden, die für die Ausführung des Jobs benötigt wurden.	INTEGER

Tabelle COGIPF_RUNJOBSTEP

Speichert Informationen zum Jobabschnitt.

Tabelle 171. Tabellenspalten, Beschreibungen und Datentypen von COGIPF_RUNJOBSTEP		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_HOST_IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)
COGIPF_HOST_PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_PROC_ID	Die vom Betriebssystem zugeordnete Prozess-ID.	INTEGER

Tabelle 171. Tabellenspalten, Beschreibungen und Datentypen von COGIPF_RUNJOBSTEP (Forts.)

Spaltenname	Beschreibung	Datentyp
COGIPF_ LOCALTIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde. Während der Bericht ausgeführt wird, ist dies der Zeitpunkt, an dem die Berichtsausführung gestartet wurde. Nachdem die Ausführung des Berichts abgeschlossen ist, ist dies die Endzeit der Berichtsausführung. Informationen zum Überprüfen, ob die Ausführung abgeschlossen ist, finden Sie unter COGIPF_STATUS. Ein leerer Eintrag bedeutet eine unvollständige Ausführung. Ein ausgefüllter Eintrag bedeutet die Ausführung der Ausführung. Um die Ausführungsstartzeit für einen Bericht zu berechnen, der die Ausführung bereits abgeschlossen hat, subtrahieren Sie COGIPF_RUNTIME von COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	Die Zeitzone, Offset von GMT	INTEGER
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR (255) NOT NULL
COGIPF_STEPID	Die alphanumerische Kennung für den Schritt innerhalb einer Jobausführung (leer, wenn keine vorhanden ist)	VARCHAR (255)
COGIPF_SUBREQUESTID	Die alphanumerische Kennung der Teilanforderung für die Komponente.	VARCHAR (255)
COGIPF_THREADID	Die alphanumerische Kennung des Threads, auf dem die Anforderung ausgeführt wird.	VARCHAR (255)
COGIPF_COMPONENTID	Der Name der Komponente, die die Angabe generiert.	VARCHAR (64)
COGIPF_BUILDNUMBER	Die Hauptbuildnummer für die Komponente, die die Angabe generiert.	INTEGER
COGIPF_LOG_LEVEL	Die Höhe der Indikation	INTEGER
COGIPF_ ZIELTYP	Das Objekt, auf dem die Operation ausgeführt wird.	VARCHAR (255)

Tabelle 171. Tabellenspalten, Beschreibungen und Datentypen von COGIPF_RUNJOBSTEP (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_JOBSTEPPATH	Der Jobschrittpfad	VARCHAR (512)
COGIPF_STATUS	Der Status der Operation: Leerzeichen, Erfolg, Warnung oder Fehler.	VARCHAR (255)
COGIPF_ERRORDETAILS	Fehlerdetails	VARCHAR (2000)
COGIPF_RUNTIME	Die Anzahl an Millisekunden, die für die Ausführung des Jobschritts verwendet wurden.	INTEGER

Tabelle COGIPF_RUNREPORT

Speichert Informationen zu Berichtsausführungen.

Tabelle 172. COGIPF_RUNREPORT-Tabellenspalten, Beschreibungen und Datentypen		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_HOST_IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)
COGIPF_HOST_PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_PROC_ID	Die vom Betriebssystem zugeordnete Prozess-ID.	INTEGER
COGIPF_ LOCALTIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde. Während der Bericht ausgeführt wird, ist dies der Zeitpunkt, an dem die Berichtsausführung gestartet wurde. Nachdem die Ausführung des Berichts abgeschlossen ist, ist dies die Endzeit der Berichtsausführung. Informationen zum Überprüfen, ob die Ausführung abgeschlossen ist, finden Sie unter COGIPF_STATUS. Ein leerer Eintrag bedeutet eine unvollständige Ausführung. Ein ausgefüllter Eintrag bedeutet die Ausführung der Ausführung. Um die Ausführungsstartzeit für einen Bericht zu berechnen, der die Ausführung bereits abgeschlossen hat, subtrahieren Sie COGIPF_RUNTIME von COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	Die Zeitzone, Offset von GMT	INTEGER

Tabelle 172. COGIPF_RUNREPORT-Tabellenspalten, Beschreibungen und Datentypen (Forts.)

Spaltenname	Beschreibung	Datentyp
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR (255) NOT NULL
COGIPF_STEPID	Die alphanumerische Kennung für den Schritt innerhalb einer Jobausführung (leer, wenn keine vorhanden ist)	VARCHAR (255)
COGIPF_SUBREQUESTID	Die alphanumerische Kennung der Teilanforderung für die Komponente.	VARCHAR (255)
COGIPF_THREADID	Die alphanumerische Kennung des Threads, auf dem die Anforderung ausgeführt wird.	VARCHAR (255)
COGIPF_COMPONENTID	Der Name der Komponente, die die Angabe generiert.	VARCHAR (64)
COGIPF_BUILDNUMBER	Die Hauptbuildnummer für die Komponente, die die Angabe generiert.	INTEGER
COGIPF_LOG_LEVEL	Die Höhe der Indikation	INTEGER
COGIPF_TARGET_TYPE	Das Objekt, auf dem die Operation ausgeführt wird. Zu den Werten gehören: · Report ReportService ist ein interaktiver Bericht · PromptForward ReportService ist ein Bericht, der nach einer Eingabeaufforderung generiert wird. · PromptBackward ReportService ist ein Bericht, der generiert wurde, nachdem der Benutzer auf die vorherige Eingabeaufforderungsseite verschoben wurde. · Bericht 'BatchReportService' ist ein Stapelbericht oder ein geplanter Ausführungsbericht. **Hinweis**: Der Wert dieser Spalte wird in zwei Teilen ausgedrückt: der Objektart der Ausführung und von dem Service, von dem der Bericht ausgeführt wird, z. B. "BerichtsberichtService" und "AbfrageBatchReportService".	VARCHAR (255)
COGIPF_REPORTPATH	Der Berichtspfad	VARCHAR (1024)

Tabelle 172. COGIPF_RUNREPORT-Tabellenspalten, Beschreibungen und Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_STATUS	Der Status der Operation: Leerzeichen, Erfolg, Warnung oder Fehler.	VARCHAR (255)
COGIPF_ERRORDETAILS	Fehlerdetails	VARCHAR (2000)
COGIPF_RUNTIME	Die Anzahl der Millisekunden, die für die Ausführung des Berichts benötigt wurden.	INTEGER
COGIPF_REPORTNAME	Der Name des Berichts, der ausgeführt wurde.	VARCHAR (512)
COGIPF_PACKAGE	Das Paket, dem der Bericht zugeordnet ist.	VARCHAR (1024)
COGIPF_MODEL	Das Modell, dem der Bericht zugeordnet ist.	VARCHAR (512)

COGIPF_THRESHOLD_VIOLATIONS-Tabelle

Speichert Informationen zu Schwellenwertverstößen für Systemmesswerte.

Weitere Informationen finden Sie unter Kapitel 4, „Systemleistungsmetriken”, auf Seite 25.

Tabelle 173. COGIPF_THRESHOLD_VIOLATIONS-Tabellenspalten, -beschreibungen und -Datentypen		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_ HOST_IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)
COGIPF_HOST_PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_PROC_ID	Die vom Betriebssystem zugeordnete Prozess-ID.	INTEGER
COGIPF_ LOCALTIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde.	TIMESTAMP
COGIPF_TIMEZONE OFFSET	Die Zeitzone, Offset von GMT	INTEGER
COGIPF_COMPONENTID	Die alphanumerische Kennung der Komponente.	VARCHAR (64)
COGIPF_BUILDNUMBER	Die alphanumerische Kennung des Builds.	INTEGER
COGIPF_LOG_LEVEL	Die Protokollierungsstufe. Sollte immer 1 sein, um sicherzustellen, dass Informationen zum Schwellenwertverstoß verfügbar sind.	INTEGER
COGIPF_ OPERATION	Ein Schwellenwert für den Messwert wurde überschritten.	VARCHAR (128)
COGIPF_TARGET_TYPE	Der Zieltyp	VARCHAR (255)
COGIPF_ TARGETNAME	Der Zielname.	VARCHAR (512)

Tabelle 173. COGIPF_THRESHOLD_VIOLATIONS-Tabellenspalten, -beschreibungen und -Datentypen (Forts.)

Spaltenname	Beschreibung	Datentyp
COGIPF_ TARGET_PATH	Der Zielpfad des Dispatchers, der den Schwellenwertmanager konatriniert.	VARCHAR (1024)
COGIPF_RESOURCE_ TYPE	Der Ressourcentyp, der den Schwellenwert überschreitet.	VARCHAR (128)
COGIPF_ RESOURCE_PATH	Der Pfad der Ressource, der den Schwellenwert überschritten hat.	VARCHAR (512)
COGIPF_METRIC_NAME	Der Name der Metrik.	VARCHAR (255)
COGIPF_METRIC_VALUE	Der Wert der Metrik.	VARCHAR (128)
COGIPF_METRIC_ GESUNDHEIT	Der Status der Metrik: Gut, Durchschnitt oder Arme	VARCHAR (128)
COGIPF_LOWER_AVG_ THRSHLD	Die untere durchschnittliche Schwellenwerteinstellung. Wenn COGIPF_LOWER_AVG_THRSHLD_XCL den Wert 1 hat, ist die Metrikbewertung durchschnittlich, wenn die Metrik kleiner als diese Schwellenwerteinstellung ist. Die Metrikbewertung ist gut, wenn die Metrik größer oder gleich diesem Wert ist. Wenn COGIPF_LOWER_AVG_THRSHLD_XCL den Wert 0 (null) hat, ist die Metrikbewertung ein Durchschnittswert, wenn der Messwert kleiner-gleich diesem Wert ist. Die Metrikbewertung ist gut, wenn der Messwert größer als dieser Wert ist.	VARCHAR (128)
COGIPF_LOWER_AVG_ THRSHLD_EXCL	Das Flag, das angibt, ob die Schwellenwerteinstellung in COGIPF_LOWER_AVG_THRSHLD bei der Bestimmung der Metrikbewertung enthalten ist. Wenn es 0 ist, wird die Schwellenwerteinstellung eingeschlossen, wenn die Metrikbewertung bestimmt wird. Wenn es sich um 1 handelt, wird die Schwellenwerteinstellung nicht berücksichtigt, wenn die Metrikbewertung bestimmt wird.	DECIMAL (1, 0)

Tabelle 173. COGIPF_THRESHOLD_VIOLATIONS-Tabellenspalten, -beschreibungen und -Datentypen (Forts.)

Spaltenname	Beschreibung	Datentyp
COGIPF_LOWER_POOR_ THRSHLD	Die untere Einstellung für den unteren Schwellenwert. Wenn COGIPF_LOWER_POOR_THRSHLD_XCL den Wert 1 hat, ist die Metrikbewertung schlecht, wenn die Metrik kleiner als diese Schwellenwerteinstellung ist. Wenn COGIPF_LOWER_POOR_THRSHLD_XCL den Wert 0 (null) hat, ist die Metrikbewertung schlecht, wenn der Messwert kleiner oder gleich diesem Wert ist.	VARCHAR (128)
COGIPF_LOWER_POOR_ THRSHLD_EXCL	Das Flag, das angibt, ob die Schwellenwerteinstellung in COGIPF_LOWER_POOR_THRSHLD bei der Bestimmung der Metrikbewertung enthalten ist. Wenn es 0 ist, wird die Schwellenwerteinstellung eingeschlossen, wenn die Metrikbewertung bestimmt wird. Wenn es sich um 1 handelt, wird die Schwellenwerteinstellung nicht berücksichtigt, wenn die Metrikbewertung bestimmt wird.	DECIMAL (1, 0)
COGIPF_UPPER_AVG_ THRSHLD	Die obere durchschnittliche Schwellenwerteinstellung Wenn COGIPF_UPPER_AVG_THRSHLD_XCL den Wert 1 hat, ist die Metrikbewertung schlecht, wenn die Metrik kleiner als diese Schwellenwerteinstellung ist. Wenn COGIPF_UPPER_AVG_THRSHLD_XCL den Wert 0 (null) hat, ist die Metrikbewertung durchschnittlich, wenn die Metrik größer als oder gleich diesem Wert ist. Die Metrikbewertung ist gut, wenn der Messwert kleiner oder gleich diesem Wert ist.	VARCHAR (128)
COGIPF_UPPER_AVG_ THRSHLD_EXCL	Das Flag, das angibt, ob die Schwellenwerteinstellung in COGIPF_UPPER_AVG_THRSHLD bei der Bestimmung der Metrikbewertung enthalten ist. Wenn es 0 ist, wird die Schwellenwerteinstellung eingeschlossen, wenn die Metrikbewertung bestimmt wird. Wenn es sich um 1 handelt, wird die Schwellenwerteinstellung nicht berücksichtigt, wenn die Metrikbewertung bestimmt wird.	DECIMAL (1, 0)

Tabelle 173. COGIPF_THRESHOLD_VIOLATIONS-Tabellenspalten, -beschreibungen und -Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_UPPER_POOR_ THRSHLD	Die Einstellung des oberen schlechten Schwellenwerts. Wenn COGIPF_UPPER_POOR_THRSHLD_XCL den Wert 1 hat, ist die Metrikbewertung schlecht, wenn die Metrik kleiner als diese Schwellenwerteinstellung ist. Wenn COGIPF_UPPER_POOR_THRSHLD_XCL den Wert 0 (null) hat, ist die Metrikbewertung schlecht, wenn der Messwert größer oder gleich diesem Wert ist.	VARCHAR (128)
COGIPF_UPPER_POOR_ THRSHLD_EXCL	Das Flag, das angibt, ob die Schwellenwerteinstellung in COGIPF_UPPER_POOR_THRSHLD bei der Bestimmung der Metrikbewertung enthalten ist. Wenn es 0 ist, wird die Schwellenwerteinstellung eingeschlossen, wenn die Metrikbewertung bestimmt wird. Wenn es sich um 1 handelt, wird die Schwellenwerteinstellung nicht berücksichtigt, wenn die Metrikbewertung bestimmt wird.	DECIMAL (1, 0)

COGIPF_USERLOGON-Tabelle

Speichert Benutzeranmelde-und Abmeldeinformationen.

Tabelle 174. COGIPF_USERLOGON-Tabellenspalten, -beschreibungen und -Datentypen		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_CAMID	CAMID des Benutzers	VARCHAR (512)
COGIPF_ HOST_IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)
COGIPF_ HOST_PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_PROC_ID	Die vom Betriebssystem zugeordnete Prozess-ID.	INTEGER
COGIPF_ LOCALTIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	Die Zeitzone, Offset von GMT	INTEGER
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)

Tabelle 174. COGIPF_USERLOGON-Tabellenspalten, -beschreibungen und -Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR (255) NOT NULL
COGIPF_STEPID	Die alphanumerische Kennung für den Schritt innerhalb einer Jobausführung (leer, wenn keine vorhanden ist)	VARCHAR (255)
COGIPF_ SUBREQUESTID	Die alphanumerische Kennung der Teilanforderung für die Komponente.	VARCHAR (255)
COGIPF_THREADID	Die alphanumerische Kennung des Threads, auf dem die Anforderung ausgeführt wird.	VARCHAR (255)
COGIPF_ COMPONENTID	Der Name der Komponente, die die Angabe generiert.	VARCHAR (64)
COGIPF_ BUILDNUMMER	Die Hauptbuildnummer für die Komponente, die die Angabe generiert.	INTEGER
COGIPF_LOG_LEVEL	Die Höhe der Indikation	INTEGER
COGIPF_STATUS	Der Status der Operation: Leerzeichen, Erfolg, Warnung oder Fehler.	VARCHAR (255)
COGIPF_ ERRORDETAILS	Fehlerdetails	VARCHAR (2000)
COGIPF_ LOGON_OPERATION	Anmeldung, Abmeldung oder Anmeldung abgelaufen	VARCHAR (255)
COGIPF_USERNAME	Der Anzeigename des Benutzers.	VARCHAR2 (255)
COGIPF_USERID	Der Benutzername des Benutzers.	VARCHAR (255)
COGIPF_ NAMESPACE	Die Namespace-ID	VARCHAR (255)
COGIPF_REMOTE_IPADDR	Die IP-Adresse des Benutzers.	VARCHAR (128)
COGIPF_TENANTID	Die Tenant-ID	VARCHAR (255)

COGIPF_VIEWREPORT-Tabelle

Speichert Informationen zu Anforderungen für Berichtsanzeigen.

Tabelle 175. COGIPF_VIEWREPORT-Tabellenspalten, Beschreibungen und Datentypen		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_HOST_IPADDR	Die Host-IP-Adresse, an der die Protokollnachricht generiert wird.	VARCHAR (128)
COGIPF_HOST_PORT	Die Nummer des Host-Ports.	INTEGER
COGIPF_PROC_ID	Die vom Betriebssystem zugeordnete Prozess-ID.	INTEGER
COGIPF_ LOCALTIMESTAMP	Das lokale Datum und die lokale Uhrzeit, zu der die Protokollnachricht generiert wurde. Während der Bericht ausgeführt wird, ist dies der Zeitpunkt, an dem die Berichtsausführung gestartet wurde. Nachdem die Ausführung des Berichts abgeschlossen ist, ist dies die Endzeit der Berichtsausführung. Informationen zum Überprüfen, ob die Ausführung abgeschlossen ist, finden Sie unter COGIPF_STATUS. Ein leerer Eintrag bedeutet eine unvollständige Ausführung. Ein ausgefüllter Eintrag bedeutet die Ausführung der Ausführung. Um die Ausführungsstartzeit für einen Bericht zu berechnen, der die Ausführung bereits abgeschlossen hat, subtrahieren Sie COGIPF_RUNTIME von COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	Die Zeitzone, Offset von GMT	INTEGER
COGIPF_SESSIONID	Die alphanumerische Kennung der Benutzersitzung.	VARCHAR (255)
COGIPF_REQUESTID	Die alphanumerische Kennung der Anforderung.	VARCHAR2 (255) NOT NULL
COGIPF_STEPID	Die alphanumerische Kennung für den Schritt innerhalb einer Jobausführung (leer, wenn keine vorhanden ist)	VARCHAR (255)
COGIPF_SUBREQUESTID	Die alphanumerische Kennung der Teilanforderung für die Komponente.	VARCHAR (255)
COGIPF_THREADID	Die alphanumerische Kennung des Threads, auf dem die Anforderung ausgeführt wird.	VARCHAR (255)
COGIPF_COMPONENTID	Der Name der Komponente, die die Angabe generiert.	VARCHAR (64)
COGIPF_BUILDNUMBER	Die Hauptbuildnummer für die Komponente, die die Angabe generiert.	INTEGER
COGIPF_LOG_LEVEL	Die Höhe der Indikation	INTEGER
COGIPF_TARGET_TYPE	Das Objekt, auf dem die Operation ausgeführt wird.	VARCHAR (255)
COGIPF_REPORTPATH	Der Berichtspfad	VARCHAR (1024)
COGIPF_STATUS	Der Status der Operation: Leerzeichen, Erfolg, Warnung oder Fehler.	VARCHAR (255)

Tabelle 175. COGIPF_VIEWREPORT-Tabellenspalten, Beschreibungen und Datentypen (Forts.)		
Spaltenname	**Beschreibung**	**Datentyp**
COGIPF_ERRORDETAILS	Fehlerdetails	VARCHAR (2000)
COGIPF_REPORTNAME	Der Name des Berichts, der angezeigt wurde.	VARCHAR (512)
COGIPF_PACKAGE	Das Paket, dem der Bericht zugeordnet ist	VARCHAR (1024)
COGIPF_REPORTFORMAT	Das Format des Berichts. Weitere Informationen finden Sie unter „Berichtsformate” auf Seite 367 .	VARCHAR (255)
COGIPF_MODEL	Das Modell, dem der Bericht zugeordnet ist.	VARCHAR (512)

Anhang G. Konfiguration der erweiterten Einstellungen

Sie können erweiterte Einstellungen global, für die gesamte IBM Cognos-Umgebung oder einzeln für einen Dispatcher oder einen Dispatcherservice konfigurieren. Die beste Methode besteht darin, die Einstellungen global anzugeben und anschließend die Werte für bestimmte Dispatcher oder Dispatcher-Services anzupassen, falls erforderlich.

Erweiterte Einstellungen sind dem Konfigurationseintrag in IBM Cognos Administration zugeordnet. Die Einstellungen werden in den Kategorien "Protokollierung", "Tuning", "Umgebung" und "Administrator" zusammengefasst.

Wenn Sie die erweiterten Einstellungen global für den Konfigurationseintrag angeben, werden die von Ihnen angegebenen Werte von allen enthaltenen Einträgen übernommen, es sei denn, die Eigenschaft des enthaltenen Eintrags wird so eingestellt, dass die globalen Einstellungen überschrieben werden. Sie können die globalen Einstellungen überschreiben, um angepasste Werte für bestimmte Einträge zur Verfügung zu stellen. Dies kann jedoch den Verwaltungsaufwand erhöhen.

Sie müssen über die folgenden Zugriffsberechtigungen für den Konfigurationseintrag und die betroffenen untergeordneten Einträge verfügen, um erweiterte Einstellungen zu ändern:

- Lese-und Schreibberechtigung für den Eintrag, den Sie aktualisieren möchten
- Berechtigungen für das übergeordnete Element des Eintrags, den Sie aktualisieren möchten

Erweiterte Einstellungen global konfigurieren

Sie können erweiterte Einstellungen global für die gesamte IBM Cognos-Umgebung konfigurieren.

Informationen zu diesem Vorgang

Die Werte, die Sie angeben, werden von allen enthaltenen Einträgen übernommen. Sie können die globalen Werte überschreiben, indem Sie angepasste Werte auf der Ebene des Dispatchers oder Dispatchers angeben.

Wenn der Konfigurationseintrag untergeordnete Einträge mit Einstellungen enthält, die die globalen Einstellungen überschreiben, können die angepassten Einstellungen für die untergeordneten Einträge zurückgesetzt werden, um die Standardwerte zu verwenden.

Sie können erweiterte Einstellungen global für die Kategorien "logging", "tuning", "environment" und "administrator überschreiben" konfigurieren.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Dispatcher und Services**.
2. Klicken Sie in der Symbolleiste auf der **Konfiguration** -Seite auf das Symbol **Eigenschaften festlegen-Konfiguration**  .
3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Wenn Sie die Liste der Einstellungen filtern möchten, wählen Sie in der Liste **Kategorie** eine Kategorie aus.
5. Wählen Sie die erforderliche Einstellung in der Liste aus, und geben Sie einen Wert auf eine der folgenden Arten an:
   - Geben Sie einen Wert ein
   - Einen Wert aus einer Liste auswählen

- Klicken Sie auf **Bearbeiten** und fügen Sie einen Parameternamen und einen Parameterwert hinzu

6. Optional: Wenn Sie die untergeordneten Einträge so zurücksetzen möchten, dass sie die Standardeinstellungen verwenden, wählen Sie das Kontrollkästchen **Konfigurationseinstellungen für alle untergeordneten Einträge löschen** aus.
7. Klicken Sie auf **OK**.
8. Stoppen und starten Sie die IBM Cognos -Services, um die Werte anzuwenden. Weitere Informationen finden Sie im *IBM Cognos Analytics Installations-und Konfigurationshandbuch.* .

Erweiterte Einstellungen für bestimmte Dispatcher konfigurieren

Sie können erweiterte Einstellungen für einen bestimmten Dispatcher konfigurieren. Auf diese Weise können Sie angepasste Konfigurationseinstellungen für den Dispatcher angeben, die die für die IBM Cognos-Umgebung angegebenen globalen Konfigurationseinstellungen überschreiben.

Informationen zu diesem Vorgang

Wenn der Dispatcher untergeordnete Einträge mit Einstellungen enthält, die die globalen Einstellungen überschreiben, können Sie die angepassten Einstellungen für die untergeordneten Einträge zurücksetzen, um die Standardwerte zu verwenden.

Sie können erweiterte Einstellungen auf einer Dispatcherebene für die folgenden Kategorien angeben: Protokollierung, Optimierung und Umgebung.

Wichtig: Bestimmte erweiterte Einstellungen, die der Kategorie "Umgebung" zugeordnet sind, können nicht auf der Dispatcherebene angegeben werden. Sie müssen global oder für einen Dispatcherservice angegeben werden.

Weitere Informationen finden Sie unter „Erweiterte Einstellungen global konfigurieren” auf Seite 517 und „Erweiterte Einstellungen für bestimmte Services konfigurieren” auf Seite 519 .

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Dispatcher und Services**.
2. Suchen Sie den Dispatcher, und klicken Sie in der Spalte **Aktionen** auf das Symbol **Eigenschaften festlegen**  .
3. Klicken Sie auf die Registerkarte **Einstellungen** .
4. Wenn Sie die Liste der Einstellungen filtern möchten, wählen Sie in der Liste **Kategorie** eine Kategorie aus.
5. Wählen Sie eine Konfigurationseinstellung aus der Liste aus, und geben Sie einen Wert auf eine der folgenden Arten an:
   - Geben Sie einen Wert ein
   - Einen Wert aus einer Liste auswählen
   - Klicken Sie auf **Bearbeiten**, wählen Sie das Kontrollkästchen **Über den übergeordneten Eintrag erfasste Einstellungen außer Kraft setzen** aus, und fügen Sie den Parameternamen und den Parameterwert hinzu.
6. Optional: Wenn Sie die angepassten Einstellungen für die untergeordneten Einträge zurücksetzen möchten, um die Standardeinstellungen zu verwenden, wählen Sie das Kontrollkästchen **Konfigurationseinstellungen für alle untergeordneten Einträge löschen** aus.
7. Klicken Sie auf **OK**.
8. Stoppen und starten Sie die IBM Cognos -Services, um die Werte anzuwenden. Weitere Informationen finden Sie im *IBM Cognos Analytics Installations-und Konfigurationshandbuch.* .

Erweiterte Einstellungen für bestimmte Services konfigurieren

Sie können erweiterte Einstellungen für bestimmte Dispatcher-Services, wie z. B. den AgentService, konfigurieren. Auf diese Weise können Sie angepasste Konfigurationseinstellungen für den Service angeben, die die für die IBM Cognos-Umgebung angegebenen globalen Konfigurationseinstellungen überschreiben.

Informationen zu diesem Vorgang

Sie können erweiterte Einstellungen für einen Dispatcher-Service für die folgenden Kategorien festlegen: Protokollierung, Optimierung und Umgebung.

Weitere Informationen finden Sie unter „Erweiterte Einstellungen global konfigurieren" auf Seite 517 und „Erweiterte Einstellungen für bestimmte Dispatcher konfigurieren" auf Seite 518.

Vorgehensweise

1. Klicken Sie in **IBM Cognos Administration**auf der Registerkarte **Konfiguration** auf **Dispatcher und Services**.
2. Klicken Sie auf den Namen des Dispatchers.
3. Suchen Sie in der Liste der Dispatcher-Services den erforderlichen Service, und klicken Sie in der Spalte **Aktionen** auf das Symbol **Eigenschaften festlegen**  .
4. Klicken Sie auf die Registerkarte **Einstellungen** .

   Sie können die Liste der Einstellungen nach **Kategorie**filtern. Die Auswahlmöglichkeiten für die Kategorie sind: **Alle**, **Umwelt**, **Protokollierung**und **Optimierung**.
5. Definieren Sie die Einstellung auf eine der folgenden Arten:
   - Suchen Sie die Einstellung, die Sie anpassen möchten, und geben Sie einen Wert für die Einstellung in dem bereitgestellten Bereich ein oder wählen Sie sie aus.
   - Wenn die Einstellung nicht aufgelistet ist, klicken Sie für **Erweiterte Einstellungen**auf den zugehörigen **Bearbeiten** -Link. Wählen Sie in der angezeigten Seite das Kontrollkästchen **Über den übergeordneten Eintrag erfasste Einstellungen außer Kraft setzen** aus und fügen Sie den Namen und den Wert für die Einstellung hinzu.
6. Klicken Sie auf **OK**.
7. Stoppen und starten Sie die IBM Cognos -Services, um die Werte anzuwenden. Weitere Informationen finden Sie im *IBM Cognos Analytics Installation und Konfiguration*.

Größere E-Mail-Anhänge aktivieren

Sie können die anwendbaren Cognos-Services konfigurieren, um IBM Cognos Analytics-Benutzern die Möglichkeit zu geben, größere Anhänge per E-Mail zu senden. Wenn Benutzer Probleme mit E-Mail-Anhängen haben, müssen Sie unter Umständen die Standardeinstellung für die MB-Größe für nicht komprimierte E-Mail-Anhänge ändern.

Informationen zu diesem Vorgang

Wenn Benutzer E-Mail-Anhänge, die größer sind als die Standardgröße für die MB-Größe, für nicht komprimierte E-Mail-Anhänge verwenden, können die folgenden Probleme auftreten:

- Eine leere Berichtsdatei wird an die E-Mail angehängt. In der Ausführungshistorie des Berichts werden keine Probleme angezeigt, und der gesamte Prozess scheint erfolgreich zu verlaufen.
- Der Lieferservice weist E-Mail-Anhänge zurück, auch wenn sie nach der Komprimierung nicht zu groß sind.
- Anhänge werden immer komprimiert oder immer unkomprimiert.

Das Verhalten von E-Mail-Anhängen wird durch die Einstellungen für E-Mail-Anhänge gesteuert. Sie können die folgenden Einstellungen für die zugehörigen Cognos-Services konfigurieren:

DeliveryService

Die maximale Größe einer E-Mail-Nachricht für den Bereitstellungsservice in MB.

Die Einstellung wird auf einen höheren Wert gesetzt als alle anderen Einstellungen für E-Mail-Anhänge oder bei dem Standardwert 0 links. Um eine beliebige Größe des E-Mail-Anhangs zu ermöglichen, verwenden Sie den Standardwert 0.

Die maximale Größe eines nicht komprimierten E-Mail-Anhangs für den Bereitstellungsservice in MB.

Anhänge, die den angegebenen Grenzwert überschreiten, werden komprimiert, bevor sie gesendet werden. Ein Wert größer als 0 bedeutet, dass der Bereitstellungsservice die Ausgabe komprimiert (zip), wenn die Anschlussgröße höher als der angegebene Wert ist.

Wenn Sie einen Wert für den unkomprimierten E-Mail-Anhang festlegen, sollten Sie einen Erweiterungsfaktor für die Base64-Codierung zulassen. Durch diese Erweiterung wird die Befestigungsgröße um einen Faktor von ca. 4/3 erhöht. Wenn also ein Bericht mit einer Größe von 3 MB groß ist, kann der angehängte Bericht in der E-Mail fast 4 MB groß werden, nachdem die Base64-Codierung für die Übertragung von Internet-Übertragung angewendet wird.

Diese Erweiterung richtet sich nach dem Inhalt der angehängten Berichtsdaten und variiert entsprechend. Sie sollten diesen Erweiterungsfaktor berücksichtigen, wenn Sie entscheiden, was die Maximalwerte sein sollen.

AgentService

Die maximale Größe eines nicht komprimierten E-Mail-Anhangs für den Agentenservice in MB.

Anhänge, die den angegebenen Grenzwert überschreiten, werden nicht gesendet.

Standardwert: 15

BatchReportService

Die maximale Größe eines nicht komprimierten E-Mail-Anhangs für den Stapelberichtsservice in MB.

Anhänge, die den angegebenen Grenzwert überschreiten, werden nicht gesendet.

Standardwert: 15

ReportService

Die maximale Größe eines nicht komprimierten E-Mail-Anhangs für den Berichtsservice in MB.

Anhänge, die den angegebenen Grenzwert überschreiten, werden nicht gesendet.

Standardwert: 15

Vorgehensweise

1. Führen Sie die Schritte im Abschnitt „Erweiterte Einstellungen für bestimmte Services konfigurieren" auf Seite 519aus.
2. Geben Sie für die **DeliveryService**einen Wert für die Einstellung **Die maximale Größe eines nicht komprimierten E-Mail-Anhangs für den Bereitstellungsservice in MB.** an. Um eine beliebige Größe des E-Mail-Anhangs zu ermöglichen, verwenden Sie den Standardwert 0.
3. Geben Sie für die **AgentService**-, **BatchReportService**-oder **ReportService**einen Wert für die zugeordnete E-Mail-Anhangseinstellung an.
4. Wenn mehr als ein Dispatcher konfiguriert ist, führen Sie für jeden Dispatcher die gleichen Schritte aus.

Referenz für erweiterte Einstellungen

In diesem Abschnitt werden die erweiterten Einstellungen für IBM Cognos -Services beschrieben.

Erweiterte Einstellungen des Agentenservice

In diesem Abschnitt werden die erweiterten Einstellungen für den Agentenservice beschrieben.

asv.preview.maxRows

Gibt die maximale Anzahl von Zeilen an, die in einer **Alle anzeigen** -Anforderung von IBM Cognos Event Studio angezeigt werden sollen.

Datentyp:
Ganze Zahl

Standardwert:
500

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

housekeeping.run.startup

Gibt an, ob Statusobjekte aus zuvor ausgeführten Tasks beim Start aus dem Content-Store entfernt werden. Bei 'false' wird die Bereinigung nur in dem Intervall ausgeführt, das von 'housekeeping.run.interval' angegeben wurde.

Datentyp:
Boolesch

Standardwert:
Falsch

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

housekeeping.run.interval

Gibt das Intervall (in Stunden) an, in dem die Housekeeping-Operationen für die zuvor ausgeführten Agenten ausgeführt werden. Dieser Wert wird nur verwendet, wenn 'housekeeping.run.startup' auf 'false' gesetzt ist.

Datentyp:
Ganze Zahl

Standardwert:
12

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

primary.wait.asv

Gibt die Zeit (in Sekunden) für den primären Warteschwellenwert für den Agentenservice an. Diese Einstellung wird verwendet, wenn ein Wert in der Anforderung nicht festgelegt ist.

Datentyp:
Ganze Zahl

Standardwert:
120

secondary.threshold

Gibt die Zeit (in Sekunden) für den sekundären Warteschwellenwert für asynchrone Anforderungen an. Der Agentenservice verwendet diesen Service nur bei der Ausführung seiner Tasks (Rss-, Berichts-, SQL- und Web-Service-Tasks).

Datentyp:
Ganze Zahl

Standardwert:
30

Erweiterte Einstellungen für Content Manager-Service

In diesem Abschnitt werden die erweiterten Einstellungen für den Content Manager-Service beschrieben.

CM.CMSync_CheckActiveTime

Gibt den Zeitraum an, innerhalb dessen ein aktiver Content Manager den Standby-Modus wechselt, wenn ein anderer Content Manager aktiv wird.

Datentyp:
Ganze Zahl

Standardwert:
10000

CM.CMSync_NegotiationTime

Gibt die Übernahme-Wahlzeit in Millisekunden an.

Die Wahlzeit ist die Wartezeit, nachdem eine Content Manager-Instanz fehlgeschlagen ist, bevor andere Content Manager-Instanzen versuchen, der aktive Service zu werden. Dieser Zeitraum stellt sicher, dass eine andere Content Manager-Serviceinstanz nicht aktiv wird, es sei denn, der ursprüngliche Content Manager schlägt wirklich fehl.

Datentyp:
Ganze Zahl

Standardwert:
2000

CM.CMSync_NegotiationTimeForStartUp

Gibt die Startzeit für den Start in Millisekunden an, nachdem ein Computer heruntergefahren wurde.

Bei dieser Wahlzeit handelt es sich um die Wartezeit, während der der Standardinhaltsmanager gestartet werden soll, bevor andere Standby-Content-Manager-Instanzen versuchen, zu starten. Auf diese Weise wird sichergestellt, dass der bevorzugte Content Manager nach dem Herunterfahren des Computers gestartet wird.

Datentyp:
Ganze Zahl

Standardwert:
60000

CM.CMSync_PingTimeout

Gibt die maximale Zeit (in Millisekunden) an, in der ein beschäftigter Content Manager eine Antwort senden soll.

Nach Ablauf des Zeitlimitintervalls beginnt der Wahlprozess, einen neuen Content Manager aus den Standby-Content-Manager-Instanzen auszuwählen, falls es irgendwelche Instanzen gibt.

Datentyp:
Ganze Zahl

Standardwert:
120000

CM.CMSync_ShortNetworkInterruptionTime

Gibt eine kurze Zeit für die Netzunterbrechung in Millisekunden an, in der die Funktionsübernahme nicht ausgeführt wird.

Datentyp:
Ganze Zahl

Standardwert:
`3000`

CM.DbConnectPoolMax

Gibt die maximale Anzahl gleichzeitiger Datenbankverbindungen an, die für den Content Store zulässig sind.

Gültige Einstellungen sind -1, oder 5 bis 2147483647, oder die Datenbankeinstellung; der Wert ist kleiner.

Eine Einstellung von -1 bedeutet, dass Verbindungen unbegrenzt sind.

Diese Einstellung gilt nur für die Einstellungen des Content Manager-Verbindungspools. Wenn Sie über andere Services verfügen, die auf denselben Content-Store zugreifen, kann es zu mehr gleichzeitigen Datenbankverbindungen kommen, als in diesem Parameter angegeben wurden.

Datentyp:
Ganze Zahl

Standardwert:
`-1`

CM.DbConnectPoolTimeout

Gibt die maximale Zeit (in Millisekunden) an, die ein Thread darauf wartet, dass eine Verbindung aus dem Pool verfügbar ist.

Eine Einstellung von 0 gibt an, dass Threads nie auf eine Verbindung warten, wenn eine Verbindung nicht sofort verfügbar ist. Eine Einstellung von -1 bedeutet, dass die Wartezeit unbegrenzt ist.

Datentyp:
Ganze Zahl

Standardwert:
`-1`

CM.DbConnectPoolIdleTime

Gibt die minimale Zeit (in Millisekunden) an, die eine Verbindung im Pool inaktiv bleibt.

Diese Einstellung ist nur gültig, wenn der Wert für die Einstellung `DbConnectPoolCleanUpPeriod` positiv ist.

Eine Einstellung von 0 oder -1 gibt an, dass inaktive Verbindungen beim Neustart von Content Manager geschlossen werden.

Datentyp:
Ganze Zahl

Standardwert:
`300000`

CM.DbConnectPoolCleanUpPeriod

Gibt die Zeit (in Millisekunden) zwischen Aufrufen eines Bereinigungsthreads an, der inaktive Verbindungen in dem Pool schließt, die die Einstellung von `DbConnectPoolIdleTime`überschreiten.

Eine Einstellung von 0 oder -1 gibt keinen Bereinigungsthread an.

Datentyp:
Ganze Zahl

Standardwert:
300000

CM.DeploymentIncludeConfiguration

Gibt an, ob Konfigurationsobjekte während der Implementierung aus dem gesamten Content-Store-Archiv importiert werden sollen.

Zu diesen Objekten gehören Dispatcher und die Konfigurationsordner, die zum Gruppieren von Dispatchern verwendet werden. Sie können beispielsweise die Konfiguration importieren, weil Sie über eine Reihe von erweiterten Einstellungen für Ihre Services verfügen, die Sie aus der Quellenumgebung herausführen möchten.

Für beste Ergebnisse importieren Sie keine Konfigurationsobjekte. Konfigurieren Sie Disponenten in Ihrer Zielumgebung, bevor Sie Daten aus einer Quellenumgebung importieren.

Datentyp:
Boolesch

Standardwert:
Falsch

CM.DeploymentSkipAllReportOutput

Wenn diese Einstellung auf Wahrgesetzt ist, werden die Berichtsausgaben und ihre untergeordneten Objekte (Grafik und Seite) in **Mein Inhalt** und **Teaminhalt** weder exportiert noch importiert. Verwenden Sie diese Einstellung, um die Größe der Content-Store-Archive zu reduzieren und die Implementierungsleistung zu verbessern.

Datentyp:
Boolesch

Standardwert:
Falsch

CM.DeploymentSkipUserReportOutput

Wenn diese Einstellung auf Wahrgesetzt ist, werden die Berichtsausgaben und ihre untergeordneten Objekte (Grafik und Seite) unter Benutzerkonten nicht exportiert oder importiert. Verwenden Sie diese Einstellung, um die Größe der Content-Store-Archive zu reduzieren und die Implementierungsleistung zu verbessern.

Datentyp:
Boolesch

Standardwert:
Falsch

CM.DeploymentDetailErrorsOnly

Wenn diese Einstellung auf Wahrgesetzt ist, generiert diese Einstellung nur Zusammenfassung und Fehlerinformationen für Paket-und Ordnerimplementierungen. Standardmäßig generiert Content Manager vollständige Details für Paket-und Ordnerimplementierungshistorien. Verwenden Sie diese Option, um die Größe der Content-Store-Archive zu reduzieren und die Implementierungsleistung zu verbessern.

Datentyp:
Boolesch

Standardwert:
Falsch

CM.DeploymentDetailEntireContent

Wenn diese Einstellung auf `Wahr`gesetzt ist, werden in dieser Einstellung vollständige Details für eine gesamte Bereitstellungshistorie des Content Store generiert. Standardmäßig generiert Content Manager nur Zusammenfassung und Fehlerinformationen für eine gesamte Content-Store-Implementierung.

Datentyp:
Boolesch

Standardwert:
`Falsch`

CM.DeploymentUpdateScheduleCredential

Wenn diese Option auf "true" gesetzt ist und die Option **Übernahme-Eigentumsrecht** während des Imports eines Bereitstellungsarchivs verwendet wird, wird die Berechtigungsnachweiseigenschaft aller importierten Zeitplanobjekte so geändert, dass sie auf den Berechtigungsnachweis verweist, der in dem Konto enthalten ist, das für den Import der Implementierung verwendet wird.

Datentyp:
Boolesch

Standardwert:
`Falsch`

CM.OutPutLocation

Gibt die Position des Dateisystems an, in dem generierte Berichtsausgaben gespeichert werden.

Jede Ausgabedatei hat auch einen Ausgabedeskriptor mit demselben Namen, mit einer XML-Erweiterung.

Alte Berichtsversionen werden nicht gelöscht, wenn eine neue Version gespeichert wird. Sie müssen den Inhalt des Ausgabeverzeichnisses verwalten, um nur die von Ihnen gewünschten Berichtsversionen zu behalten.

Berichtsausgaben werden immer in das Verzeichnis geschrieben, das für die einzelnen Delivery Service-Instanzen konfiguriert ist. Um zu vermeiden, dass Berichtsausgaben an mehrere Positionen geschrieben werden, stellen Sie sicher, dass Sie entweder nur eine Instanz des Bereitstellungsservice ausführen oder alle Serviceinstanzen für die Verwendung einer gemeinsam genutzten Netzdateiposition konfigurieren. Jeder Dispatcher, auf dem der Bereitstellungsservice ausgeführt wird, muss Zugriff auf das Dateisystem haben oder auf allen Systemen inaktiviert sein, die nicht zum Speichern der Berichtsausgabe bestimmt sind.

Datentyp:
Zeichenfolge

Standardwert:
`Keine`

CM.OutputScript

Gibt die Position und den Namen eines externen Scripts an, das jedes Mal ausgeführt wird, wenn eine Berichtsausgabe gespeichert wird.

Bei den Scriptparametern handelt es sich um die Berichtsausgabe-und Ausgabedeskriptordateinamen.

Datentyp:
Zeichenfolge

Standardwert:
`Keine`

CM.OutputByBurstKey

Gibt an, ob die Ausgaben auf dem Dateisystem nach Berstschlüssel organisiert werden sollen.

Wenn diese Eigenschaft auf `Wahr`gesetzt ist, wird die Ausgabe in ein Unterverzeichnis mit demselben Namen wie der Burstschlüssel gestellt.

Datentyp:
Boolesch

Standardwert:
`Falsch`

CM.SecurityQueryRequiresRead

Steuert, ob Content Manager einen Leseberechtigungsfilter für Abfrageergebnisse für externe Namensbereiche erzwingt.

Wenn diese Option aktiviert ist, kann Content Manager das Browsen von externen Namespaces verhindern, wenn die Richtlinie für externe Namespaces auch aktualisiert wird, um Benutzern oder Gruppen Leseberechtigung zu verweigern.

Datentyp:
Boolesch

Standardwert:
`Falsch`

CM.SortCollation

Der Name der datenbankspezifischen Sortierfolge, die für die Sortierung in einigen Datenbanken verwendet wird, wie z. B. Oracle und SQL Server.

Wenn diese Option leer ist, verwendet die Datenbank ihre Standardsortierfolge.

Wenn Sie beispielsweise in Oracle die Sortierfolge als Binär auf Datenbankebene angeben, müssen Sie denselben Sortierfolgswert in der Verbindungszeichenfolge angeben.

Eine Beispielverbindungszeichenfolge für eine Oracle-Datenbank, die die Beispieldatenbank 'gosl' verwendet, ist: `ORACLE@GOSL0703@GOSL/GOSL0703@COLSEQ= Binär`

Informationen zu unterstützten Sortierfolgen finden Sie in der Oracle-und SQL Server-Dokumentation.

Der Wert `CM.SortCollation` hat keine Auswirkung auf Content Manager, die mit IBM Db2 -oder Sybase-Datenbanken ausgeführt werden.

Datentyp:
Zeichenfolge

Standardwert:
`Keine`

CM.UpdateInitialContentNamesAfterImport

Fügt lokalisierte Objektnamen für zuvor nicht unterstützte Ländereinstellungen hinzu.

Wenn Sie ein Upgrade auf IBM Cognos Analytics von IBM Cognos Business Intelligence Version 10.1.1 oder früher durchführen möchten und einen Content Store importieren möchten, der mit einer älteren Version von Cognos BI erstellt wurde, verwenden Sie diese erweiterte Einstellung, um sicherzustellen, dass alle Objektnamen ordnungsgemäß lokalisiert werden.

Die folgenden Locales sind betroffen: Katalanisch, Kroatisch, Dänisch, Griechisch, Kasachisch, Norwegisch, Slowakisch, Slowenisch und Thailändisch. Die Unterstützung für diese Ländereinstellungen wurde in den IBM Cognos Business Intelligence-Versionen 10.1.1 und 10.2 hinzugefügt. Wenn Ihr Content Store mit einer früheren Version erstellt wurde und die Einstellung CM.UpdateInitialContentNamesAfterImport nicht vor dem Import des Content Store angegeben wurde, werden einige Objektnamen möglicherweise in Englisch und nicht in der angegebenen Sprache angezeigt.

Geben Sie die betroffenen Ländereinstellungen an, die jeweils durch ein Komma voneinander getrennt werden. Für slowenische und kroatische Inhaltslocales beispielsweise: `sl, hr`

Anmerkung: Entfernen Sie diese erweiterte Einstellung, wenn die Unterstützung für den älteren Content Store nicht mehr benötigt wird, da dieser Einstellung eine Auswirkung auf die Leistung zugeordnet ist.

Datentyp:
Zeichenfolge

Standardwert:
`Keine`

Allgemeine Konfigurationseinstellungen

In diesem Abschnitt werden die erweiterten Einstellungen beschrieben, die für alle Services gelten.

trustedSession.pool.max

Gibt die maximale Anzahl vertrauenswürdiger Sitzungen an, die gleichzeitig verwendet werden können. Vertrauenswürdige Sitzungen verwenden einen internen Sicherheitsmechanismus, um die Kommunikation von internen Komponenten zu verschlüsseln.

Die Sitzungen werden als Ressourcenpool implementiert.

Datentyp:
Ganze Zahl

Standardwert:
`100`

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

axis.timeout

Gibt den Zeitlimitwert (in Sekunden) für den internen Achsenserver an. Dies ist der Zeitpunkt, an dem die Axis auf eine Antwort auf Serviceaufrufe warten wird, bevor sie das Zeitlimit überschritten haben.

Axis ist ein Open-Source-Tool zum Konvertieren von XML-Objekten in Java -Objekte.

Datentyp:
Ganze Zahl

Standardwert:
`0`

COGADMIN.filterInteractiveActivitiesOfUnknownUsers

Gibt an, ob Aktivitäten in IBM Cognos Administration ausgeblendet werden, wenn der Benutzer nicht über die Berechtigung zum Anzeigen des Benutzers verfügt, der die Aktivität ausführt.

Datentyp:
Boolesch

Standardwert:
`Falsch`

COGADMIN.restrictInteractiveActivitiesToSystemAdministrators

Gibt an, ob interaktive Aktivitäten in IBM Cognos Administration auf Systemadministratoren beschränkt sind.

Wenn diese Einstellung auf `Wahr`gesetzt ist, stellt das Tool 'Aktuelle Aktivitäten' nur Systemadministratoren ohne Systemadministratoren den Zugriff auf Hintergrundaktivitäten zur Verfügung.

Datentyp:
Boolesch

Standardwert:
Falsch

DISP.InteractiveProcessUseLimit

Erzwingt das Senden von Anforderungen an einen Berichtsserver-Prozess nach der vorgeschriebenen Begrenzung.

Wenn Sie beispielsweise die Begrenzung auf 500 setzen, zwingt der Dispatcher den Dispatcher, Anforderungen nach 500 Anforderungen an einen Prozess zu senden.

Datentyp:
Ganze Zahl

Standardwert:
0

DISP.BatchProcessUseLimit

Erzwingt das Senden von Anforderungen an einen Stapelberichtsserver-Prozess nach der vorgeschriebenen Begrenzung.

Datentyp:
Ganze Zahl

Standardwert:
0

VIEWER_CW_BACKWARDS_COMPATIBLE_DRILL

Gibt an, ob die traditionelle Drillfunktionalität in IBM Cognos Workspace verwendet wird.

Diese Einstellung ist standardmäßig nicht angegeben, und die aktuelle Drillup-und Abwärtsfunktionalität wird in Cognos Workspace verwendet.

Wenn diese Einstellung auf Wahrgesetzt ist, wird die Drillfunktionalität in Cognos Workspace auf sein Verhalten in Version 10.2.0 und früher zurückgesetzt.

Wenn diese Einstellung auf Falschgesetzt ist, wird die aktuelle Cognos Workspace-Drillfunktionalität verwendet.

Geben Sie diese Einstellung auf der Konfigurationsebene Ihres Systems an. Nicht für einzelne Services festlegen.

Datentyp:
Boolesch

Standardwert:
Falsch

Erweiterte Einstellungen für Präsentationsservice

In diesem Abschnitt werden die erweiterten Einstellungen für den Präsentationsservice beschrieben.

CPSMaxCacheSizePerPortlet

Gibt die Anzahl der Markup-Fragmente an, die für jedes Portlet pro Seite pro Benutzer zwischengespeichert werden.

Ein Wert von 5 mit 1000 Benutzern, 10 Seiten und 4 Portlets pro Seite kann beispielsweise maximal 200000 Einträge im Cache generieren (1000 x 10 x 4 x 5).

Die folgenden Einstellungen sind gültig:

- -1 speichert eine unbegrenzte Anzahl von Markups.
- 0 inaktiviert das Markup-Caching.

· 1 oder eine ganze Zahl größer als 1 begrenzt die Anzahl der Markups auf die angegebene Zahl.

Datentyp:
Ganze Zahl

Standardwert:
`-1`

properties.config.cps.cache.timeToIdleSeconds

Gibt die Dauer (in Sekunden) an, in der die Seitenmarkup-Fragmente während einer Inaktivitätsdauer im Cache gespeichert werden.

Wenn die Seite während dieser Zeit nicht aufgerufen wird, werden die Cacheinhalte gelöscht.

Die auf der Platte gespeicherten Cachedaten können verschlüsselt werden, wenn der Wert von **Temporäre Dateien verschlüsseln** unter dem Ordner **Umwelt** in der Konfiguration von IBM Cognos auf **Wahr** gesetzt ist.

Datentyp:
Ganze Zahl

Standardwert:
`1800 (30 Minuten)`

properties.config.cps.cache.timeToLiveSeconds

Gibt die Dauer (in Sekunden) an, in der Seitenmarkup-Fragmente im Cache gespeichert werden.

Nach der angegebenen Zeit wird die Markup gelöscht, auch wenn der Cache noch aktiv ist.

Die auf der Platte gespeicherten Cachedaten können verschlüsselt werden, wenn der Wert von **Temporäre Dateien verschlüsseln** unter dem Ordner **Umwelt** in der Konfiguration von **IBM** Cognos auf Wahr gesetzt ist.

Datentyp:
Ganze Zahl

Standardwert:
`86400 (24 Stunden)`

properties.config.cps.cache.checkExpiryIntervalSeconds

Gibt die Dauer (in Sekunden) an, die die Häufigkeit angibt, mit der das System auf abgelaufene Markup-Fragmente im Cache prüft.

Die auf der Platte gespeicherten Cachedaten können verschlüsselt werden, wenn der Wert von **Temporäre Dateien verschlüsseln?** unter dem Ordner **Umwelt** in der Konfiguration von IBM Cognos auf **Wahr** gesetzt ist.

Datentyp:
Ganze Zahl

Standardwert:
`300 (5 Minuten)`

xts.tempdir

Gibt die Position des Ordners auf dem lokalen Laufwerk an, in dem die Markup-Fragmente gespeichert werden.

Der Wert kann ein beliebiger Pfad auf dem lokalen Laufwerk sein. Wenn kein Wert angegeben ist, wird der Standardarbeitsbereich des Anwendungsservers verwendet.

Datentyp:
Zeichenfolge

Standardwert:
Leer

CPSPropagatePassport

Gibt an, ob die Passport-ID von IBM Cognos als URL-Parameter übertragen wird.

Wenn diese Option auf 0 gesetzt ist, verhindert diese Markierung die Übertragung der IBM Cognos -Passport-ID als URL-Parameter.

Ein anderer Wert als 0 ermöglicht die Übertragung der Pass-ID.

Datentyp:

Standardwert:
Keine

CPSPropagateTicket

Gibt an, ob die IBM Cognos -Konfigurationsticket-ID als URL-Parameter übertragen wird.

Wenn diese Option auf 0 gesetzt ist, verhindert diese Markierung die Übertragung der IBM Cognos -Konfigurationsticket-ID als URL-Parameter.

Ein anderer Wert als 0 ermöglicht die Übertragung der Ticket-ID.

Datentyp:

Standardwert:
Keine.

CPSProtocolScheme

Überschreibt das Protokollschema, das bei der Generierung des WSDL-Endpunkts (Web Service Definition Language) für Portal Services for Web Services Remote Portlets (WSRP) Producers verwendet wird.

Um WSDL für WSRP zu generieren, verwendet Portal Services das im Parameter IBM Cognos Configuration Gateway angegebene Protokollschema. Wenn es mehrere Gateways gibt, die nicht alle mit demselben Protokollschema konfiguriert werden können, z. B. http oder https, überschreibt dieser Parameter alle anderen Einstellungen.

Gültige Einstellungen sind HTTP und HTTPS .

Datentyp:
Zeichenfolge

Standardwert:
Keine

portal.showTenantInfoForAllUsers

Wenn diese Eigenschaft auf 'true' gesetzt ist, können Benutzer, die keine Administratorberechtigungen besitzen, Tenantinformationen anzeigen.

Auf der Seite "Eigenschaften festlegen" wird beispielsweise der Tenant eines Objekts angezeigt. In Objektlisten können Benutzer das Tenantfeld anzeigen.

Die Nutzer sind nicht in der Lage, die Mieterschaft zu verändern oder Mieter zu verkörpern.

Datentyp:
Boolesch

Standardwert:
Falsch

Erweiterte Einstellungen für Bereitstellungsservice

In diesem Abschnitt werden die erweiterten Einstellungen für den Bereitstellungsservice beschrieben.

emf.archive.filetimestamp.enabled

Zwingt die Zeitmarke für archivierte Dateien.

Datentyp:
Boolesch

Standardwert:
`Wahr`

max.smtp.connections

Gibt die maximale Anzahl der SMTP-Verbindungen an.

Diese Einstellung begrenzt die Anzahl der Threads, die der Bereitstellungsservice zum Senden von Nachrichten spawn kann.

Gültige Einstellungen sind ganze Zahlen größer oder gleich 1.

Datentyp:
Ganze Zahl

Standardwert:
`10`

Tipp: Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

primary.wait.dls

Gibt den Schwellenwert für die primäre Wartezeit (in Sekunden) für den Bereitstellungsservice an.

Diese Einstellung wird verwendet, wenn ein Wert in einer Anforderung nicht festgelegt ist.

Wenn die Einstellung kleiner als 0 ist, wird sie ignoriert. Wenn die Einstellung 0 ist, wartet der Client auf unbestimmte Zeit.

Datentyp:
Ganze Zahl

Standardwert:
`120`

smtp.reconnection.delay

Gibt das Zeitintervall (in Sekunden) an, bevor der Versuch unternommen wird, die Verbindung zu einem SMTP-Server wiederherzustellen.

Datentyp:

Standardwert:
`10`

Tipp: Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

enable.tide.metrics.smtpqueue

Aktiviert die Erfassung und Anzeige der Messwerte für den Bereitstellungsservice in der Administrationskonsole von IBM Cognos .

Die folgenden Metriken werden verfolgt:

- Zeit in Warteschlangenhochwasserzeichen
- Zeit in Warteschlange mit niedrigem Wasserzeichen

· Zeit in Warteschlange

· Anzahl Warteschlangenanforderungen

· Hochwasserzeichen für Warteschlangenlänge

· Untere Grenze für Warteschlangenlänge

Datentyp:
Boolesch

Standardwert:
`Falsch`

dls.connection.pool.force.clean

Erzwingt die Bereinigung der SMTP-Transportverbindungen. Auf diese Weise wird vermieden, dass die Methode close () aufgerufen werden muss, was zu Wartezeiten führt. Stattdessen werden Variablen einfach auf null gesetzt.

Datentyp:
Boolesch

Standardwert:
`Falsch`

Auf 'true' setzen, um eine Bereinigung zu erzwingen.

Tipp: Nachdem Sie Änderungen angewendet haben, müssen Sie auf "true" setzen, um die Einstellung zu testen.

dls.connection.pool.used

Gibt an, ob der DLS-Transportverbindungspool verwendet wird.

Datentyp:
Boolesch

Standardwert:
`Wahr`

Auf 'true' setzen, um den Verbindungspool zu verwenden.

Tipp: Setzen Sie den Wert auf "false", damit der Verbindungspool nicht verwendet wird. Das Ergebnis ist, dass jede E-Mail DLS veranlasst, eine neue SMTP-Transportverbindung mit dem E-Mail-Server zu öffnen. Dies kann hilfreich sein, wenn die Mail-Server-Sockets nach jeder Verwendung gelöscht werden.

Fehler beim Anpassen der Fehlerbehandlung auf dem SMTP-Mail-Server

Die Art und Weise, in der ein SMTP-Mail-Server Fehler verarbeitet, kann sich je nach der Implementierung des Mail-Servers unterscheiden. Aus diesem Grund können Sie die Aktionen anpassen, die der Bereitstellungsservice ausführen soll, wenn er bestimmte Fehler feststellt, indem Sie SMTP-Regeln in einer XML-Datei einrichten.

Eine Gruppe von Standardregeln für die Fehlerbehandlung wird in einer Beispieldatei gespeichert, die mit der IBM Cognos -Software bereitgestellt wird. Um die Regeln anzupassen, sollten Sie eine Kopie dieser Datei erstellen und diese ändern. Anschließend konfigurieren Sie den Bereitstellungsservice für die Verwendung dieser Datei.

Vorgehensweise

1. Bearbeiten Sie die vorhandene Datei *Installationsposition*`\configuration\smtpRules-default.xml` oder erstellen Sie eine neue angepasste SMTP-Regeldatei und fügen Sie sie in den Ordner *Installationsposition*`\configuration` ein.
2. Öffnen Sie die erforderliche Datei in einem XML-oder Texteditor.

3. Ändern Sie die Datei, um die Regeln anzupassen.
4. Klicken Sie auf **Verwalten**, **Verwaltungskonsole**.
5. Klicken Sie auf der Registerkarte **Status** auf **System**.
6. Klicken Sie im Dropdown-Menü **Alle Server** auf **Dienstleistungen**, **Zustellung**.
7. Klicken Sie im Dropdown-Menü neben **DeliveryService**auf **Eigenschaften festlegen**.
8. Klicken Sie auf die Registerkarte **Einstellungen** .
9. Klicken Sie neben **Umwelt**auf **Bearbeiten**.
10. Geben Sie in der Spalte **Parameter** den Parameternamen **smtp.rules.properties.location**ein.
11. Geben Sie in der Spalte **Wert** den Namen der angepassten XML-Datei ein, die Sie verwenden.
12. Geben Sie in der Spalte **Parameter** den Parameternamen **smtp.rules.properties.reread**ein.

    Obwohl dies nicht obligatorisch ist, ist es nützlich, diesen Parameter für Testzwecke festzulegen, damit die SMTP-Regeln für jede Anforderung gelesen werden.
13. Geben Sie in der Spalte **Wert** den Wert **Wahr**ein.
14. Klicken Sie auf **OK**.
15. Klicken Sie auf der Seite **Eigenschaften festlegen** auf **OK**.

    Wenn Sie das Testen der Regeln abgeschlossen haben, müssen Sie den Parameter smtp.rules.properties.reread zurücksetzen.
16. Wiederholen Sie die Schritte 6 bis 11, um auf die erweiterten Einstellungen zuzugreifen.
17. Geben Sie in der Spalte **Wert** für den Parameter smtp.rules.properties.reread den Wert **Falsch**ein.
18. Klicken Sie auf **OK**.

SMTP-Regeln

Verwenden Sie den Tag < smtpRule >, um eine SMTP-Regel und den Tag < smtpError > zu definieren, um den Fehlercode zu definieren, für den Sie eine Regel anwenden.

Beispiel:

```
<smtpRule>
    <smtpError>
        <errorCode>502</errorCode>
    </smtpError>
```

```
    ...
```

```
    <smtpError>
```

```
        <errorCode>550</errorCode>
    </smtpError>
```

```
    ...
```

```
</smtpRule>
```

Hinweis: Die Priorität der Regeln wird durch die Reihenfolge bestimmt, in der sie in der XML-Datei angezeigt werden.

Sie können die folgenden Typen von SMTP-Fehlern definieren:

· Transportfehler

  Beispiel: Es gibt keine Verbindung zum Mail-Server, der Mail-Server ist nicht vorhanden oder nicht ordnungsgemäß konfiguriert, oder der Benutzer hat keinen Zugriff auf den Mail-Server.

  Verwenden Sie `< transport> true < /transport>` , um diese Art von Fehler in Ihre Regeln einzuschließen.

· Empfängerfehler

Es gibt z. B. ungültige Empfänger, zu viele Empfänger oder keine Empfänger.

Verwenden Sie < invalidRecipients> true < /invalidRecipients> , um diese Art von Fehler in Ihre Regeln einzuschließen.

· andere angegebene Fehler

Jeder Standard-SMTP-Fehlercode, der vom Mail-Server generiert wird.

Verwenden Sie < errorCode> nnn < /errorCode> , um diese Art von Fehler in Ihre Regeln einzuschließen.

Die folgenden Aktionen können für jeden Fehlertyp ausgeführt werden und sind als Verhalten in der XML-Datei definiert:

· Verhalten erneut senden

Gibt an, wie oft eine E-Mail (n) und das erneute Sendeintervall in Sekunden (x) erneut gesendet werden sollen.

Verwenden Sie < resendet number="n "delaySeconds =" x " /> , um dieses Verhalten anzuwenden.

Hinweis: Um eine E-Mail auf unbestimmte Zeit erneut zu senden, verwenden Sie < resendet number="-1 ">.

· E-Mail-Verhalten beibehalten

Gibt an, ob der Bereitstellungsservice die fehlgeschlagene E-Mail in einer separaten Warteschlange halten soll, nachdem sie die erforderliche Anzahl von Malen erneut gesendet hat und nicht erfolgreich ist. Die Warteschlange wird als SMTPBackupQueue bezeichnet.

Hinweis: Es werden keine weiteren Aktionen für E-Mails in der Sicherungswarteschlange ausgeführt. Um E-Mails von SMTPBackupQueue in die reguläre SMTPQueue-Warteschlange hinzuzufügen, müssen Sie den Warteschlangennamen in der Datenbanktabelle ändern und den Server erneut starten.

Verwenden Sie < keepMail> true < /keepMail> , um dieses Verhalten anzuwenden.

· Mail-Verhalten

Ermöglicht Ihnen die Anpassung der E-Mail-Benachrichtigung, die gesendet wird, wenn eine E-Mail-Zustellung fehlgeschlagen ist.

Verwenden Sie das Tag < failMail> , um dieses Verhalten anzuwenden.

Es gibt zwei weitere optionale Attribute, die Sie zum Angeben des E-Mail-Benachrichtigungssubjekts (< subjekt>) und des Empfängers (< recipients>) verwenden können.

Tipp: Wenn Sie diese Tags weglassen, wird die E-Mail-Benachrichtigung standardmäßig an die ursprüngliche Empfängerliste mit dem Betreff "Senden fehlgeschlagen:" gesendet.

Um alle aktuellen Empfänger zu entfernen, verwenden Sie < Empfänger sendToCurrentRecipients = " false">.

Wenn Sie eine E-Mail-Benachrichtigung an den Agenteneigner senden möchten, verwenden Sie < owner> true < /owner> und verwenden Sie bei Bedarf < Empfängeradresse= "name@address.com"> , um eine E-Mail-Adresse anzugeben.

· Standardverhalten

Definiert die Aktion, die ausgeführt werden soll, wenn keine übereinstimmende Regel gefunden wird.

Verwenden Sie das Tag < defaultSmtpBehaviour > , um dieses Verhalten anzuwenden.

Beispiele-SMTP-Regeln

Das erste Beispiel zeigt, wie eine Regel für das Standardverhalten eingerichtet wird.

Hier versucht der Bereitstellungsservice, die nicht zustellbare E-Mail dreimal in stündlichen Intervallen erneut zu senden. Wenn der Fehler nicht erfolgreich ist, sendet er eine E-Mail-Benachrichtigung unter Verwendung des Standardverhaltens für das Fehlverhalten der E-Mail.

```
<defaultSmtpBehaviour>
    <smtpBehaviour name="default">
        <keepMail>false</keepMail>
        <resends number="3" delaySeconds="3600" />
        <failMail />
    </smtpBehaviour>
 </defaultSmtpBehaviour>
```

Das zweite Beispiel zeigt, wie eine Regel für einen Transportfehler eingerichtet wird. Hier sendet der Lieferdienst die E-Mail auf unbestimmte Zeit in 30 Sekunden zurück, bis sie erfolgreich ist.

```
<smtpRule>
    <smtpError>
        <transport>true</transport>
    </smtpError>
    <smtpBehaviour name="transport">
        <keepMail>false</keepMail>
        <resends number="-1" delaySeconds="30" />
    </smtpBehaviour>
</smtpRule>
```

Das dritte Beispiel zeigt, wie eine Regel für einen Empfängerfehler eingerichtet wird. Hier wird die E-Mail-Benachrichtigung an den Agenteneigner unter Verwendung der E-Mail-Adresse gesendet, die in der Benutzer-ID gespeichert ist. Die ursprünglichen E-Mail-Empfänger werden aus der Empfängerliste entfernt.

```
<smtpRule>
    <smtpError>
        <invalidRecipients>true</invalidRecipients>
    </smtpError>
    <smtpBehaviour name="invalidRecips">
        <keepMail>false</keepMail>
        <failMail>
            <recipients sendToCurrentRecipients="false">
                <owner>true</owner>
            </recipients>
        </failMail>
    </smtpBehaviour>
 </smtpRule>
```

Das vierte Beispiel zeigt, wie eine Regel für einen angegebenen Fehlercode eingerichtet wird. Hier wird die nicht zugestellte E-Mail immer dann an die Sicherungswarteschlange gesendet, wenn Fehler 550 auftreten. Es bleibt dort, bis Sie es manuell verarbeiten. Ein angepasstes E-Mail-Subjekt wird für die Benachrichtigung über die Fehlermail eingerichtet.

```
<smtpRule>
    <smtpError>
        <errorCode>550</errorCode>
    </smtpError>
    <smtpBehaviour name="specialErrorCode-550">
        <keepMail>true</keepMail>
        <failMail>
            <subject>Error code 550 keep mail</subject>
        </failMail>
    </smtpBehaviour>
</smtpRule>
```

Erweiterte Einstellungen für Dispatcher-Service

In diesem Abschnitt werden die erweiterten Einstellungen für den Dispatcher beschrieben.

DISP.InteractiveProcessUseLimit

Erzwingt das Senden von Anforderungen an einen Berichtsserver-Prozess nach der vorgeschriebenen Begrenzung.

Wenn Sie beispielsweise die Begrenzung auf 500 setzen, zwingt der Dispatcher den Dispatcher, Anforderungen nach 500 Anforderungen an einen Prozess zu senden.

Datentyp:
Ganze Zahl

Standardwert:
`0`

DISP.BatchProcessUseLimit

Erzwingt das Senden von Anforderungen an einen Stapelberichtsserver-Prozess nach der vorgeschriebenen Begrenzung.

Datentyp:

Standardwert:
`0`

Erweiterte Einstellungen für Event-Management-Service

In diesem Abschnitt werden die erweiterten Einstellungen für den Event-Management-Service beschrieben.

run.task.max.thread

Gibt die maximale Anzahl der Threads an, die für die Übertragung geplanter Anforderungen an eine Haltewarteschlange zugeordnet sind.

Wenn der Event-Management-Service eine Task ausführt, wird die Task in eine Warteschlange gestellt, die auf Ressourcen wartet, um sie auszuführen. Ein Thread wird erstellt, um die Anforderung für den Scheduler-Thread des Event-Management-Service zu verarbeiten.

Standardwert: 20

Datentyp:
Ganze Zahl

Standardwert:
`20`

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

authenticate_when_scheduled

Legt fest, ob ein RunAt-Anforderungsheader für die `Ausführen` -Berechtigung für das Objekt, das ausgeführt werden soll, überprüft wird.

Wenn eine Prüfung erforderlich ist und die Prüfung fehlschlägt, wird eine Ausnahmebedingung ausgelöst.

Wenn diese Option festgelegt ist, schlägt diese Prüfung auch fehl, wenn der Benutzer über die Berechtigungen verfügt, aber die Berechtigungsnachweise, die zum Ausführen der Task zu einem geplanten Zeitpunkt erforderlich sind, nicht abgerufen werden können.

Datentyp:
Boolesch

Standardwert:
`Falsch`

enable.tide.metrics.jobqueue

Aktiviert die Erfassung und Anzeige bestimmter Messwerte für den Ereignisverwaltungsservice in der IBM Cognos Administration.

Die folgenden Metriken sind enthalten:

- Zeit in Warteschlangenhochwasserzeichen
- Zeit in Warteschlange mit niedrigem Wasserzeichen
- Zeit in Warteschlange
- Anzahl Warteschlangenanforderungen
- Hochwasserzeichen für Warteschlangenlänge
- Untere Grenze für Warteschlangenlänge

Datentyp:
Boolesch

Standardwert:
`Falsch`

ems.action.requires.permissions.check

Erzwingt die Prüfung von Objektberechtigungen.

Wenn diese Option aktiviert ist, muss ein Aufrufender mit der Benutzerfunktion canUseMonitorActivityTool auch eine der folgenden Bedingungen erfüllen, bevor die Methode runSpecification () für den Ereignisverwaltungsservice aufgerufen wird:

- Der Account des Aufrufenden muss mit dem Accountberechtigungsnachweis übereinstimmen, der für die Planung des Ereignisses verwendet wird.
- Der Aufrufende muss über Durchquerung-und Ausführungsberechtigungen für das Zielobjekt verfügen.

Datentyp:
Boolesch

Standardwert:
`Falsch`

emf.schedule.validation.enabled

Prüft die Zeitplaneigenschaften wie Startdatum, Enddatum, Datentypen und Benutzerkontoberechtigungsnachweise, wenn Content Manager Anforderungen zum Hinzufügen oder Aktualisieren von Zeitplänen verarbeitet. Inaktiviert ungültige Zeitpläne.

Details zu inaktivierten Zeitplänen werden in Protokolldateien protokolliert.

Datentyp:
Boolesch

Standardwert:
`Falsch`

emf.dls.attachment.timestamp.enabled

Wenn diese Eigenschaft auf "true" gesetzt ist, haben E-Mail-Anhänge Berichtsnamen mit einer Zeitmarke für Datum. Das Standardformat für die Zeitmarke ist jjjj.MM.dd, wobei yyyy die vierstellige Jahreszahl ist, MM die zweistellige Monatsangabe und dd der zweistellige Tag ist.

Wenn Sie beispielsweise den Bericht Jahresergebnis in einer Nachricht anhängen, hat die E-Mail, die gesendet wird, den folgenden Anhang: Jahresergebnis-2014.07.15.pdf.

Legen Sie diese erweiterte Eigenschaft fest, wenn Sie eine Datums-Zeitmarke hinzufügen müssen, um Anhänge in E-Mails zu melden. Ändern Sie optional das Standardformat für Datum und Uhrzeit, indem Sie die erweiterte Eigenschaft 'emf.dls.attachment.timestamp.format' festlegen.

Datentyp:
Boolesch

Standardwert:
Falsch

emf.dls.attachment.timestamp.format

Gibt das Datum/Zeit-Format an, das den Berichtsnamen in E-Mail-Anhängen hinzugefügt wird, wenn die erweiterte Eigenschaft "emf.dls.attachment.timestamp.enabled" auf "true" gesetzt ist.

Mögliche Werte sind verschiedene Datumsformate. Zum Beispiel hat der 15.07.2014 das Format dd.MM.yyyy und 140704120856-0700 hat das Format jjMMttHHmmssZ. Weitere Informationen zu SimpleDateFormat finden Sie auf der Oracle-Website. Verwenden Sie keine Schrägstriche oder Sonderzeichen im Format.

Datentyp:
Zeichenfolge

Standardwert:
jjjj-MM-tt

emf.preview.max.items

Verwenden Sie diese Einstellung, um die maximale Anzahl der Ereignisse zu erhöhen, die in der Ereignisliste angezeigt werden können.

Die Erhöhung dieses Werts kann sich auf die Leistung des Systems auswirken, das mehr Daten lesen und die Daten in der Benutzerschnittstelle wiedergeben muss.

Datentyp:
Ganze Zahl

Standardwert:
50

Erweiterte Einstellungen für Jobservice

In diesem Abschnitt werden die erweiterten Einstellungen für den Jobservice beschrieben.

primary.wait.js

Gibt die Zeit (in Sekunden) für den primären Warteschwellenwert für den Job-Service an.

Dieser Wert wird verwendet, wenn ein Wert in der Anforderung nicht festgelegt ist.

Datentyp:
Ganze Zahl

Standardwert:
120

Erweiterte Einstellungen für den Metrikmanagerservice

In diesem Abschnitt werden die erweiterten Einstellungen für den Service für den Metrikmanager beschrieben.

initialConnections

Gibt die Anzahl der Verbindungen an, die erstellt werden sollen, wenn der Verbindungspool initialisiert wird.

Datentyp:
Ganze Zahl

Standardwert:
5

Tipp: Sie müssen den Service erneut starten, damit diese Einstellungen wirksam werden.

incrementConnections

Gibt die Anzahl der Verbindungen an, die erhöht werden sollen, wenn der Verbindungspool erhöht werden muss.

Datentyp:
Ganze Zahl

Standardwert:
5

Tipp: Sie müssen den Service erneut starten, damit diese Einstellungen wirksam werden.

maximumConnections

Gibt die maximale Anzahl der Verbindungen an, die dieser Pool verwenden kann.

Datentyp:
Ganze Zahl

Standardwert:
200

Tipp: Sie müssen den Service erneut starten, damit diese Einstellungen wirksam werden.

Erweiterte Einstellungen für Monitor-Service

In diesem Abschnitt werden die erweiterten Einstellungen für den Überwachungsservice beschrieben.

emf.scheduling.priority.capability.check.disabled

Wenn diese Option auf "True" gesetzt ist, wird eine geplante Task mit der in der Task angegebenen Priorität ausgeführt, unabhängig davon, ob der Benutzer über die Funktion "Zeitplanpriorität" verfügt. Wenn diese Option auf False (Standard) gesetzt ist, wird der Zeitplan für die Tasks als Standardpriorität ausgeführt.

Dieses Szenario kann auftreten, wenn eine Benutzertask von einem Administrator geändert wird, um eine höhere Priorität zu haben.

Datentyp:
Boolesch

Standardwert:
`Falsch`

enable.session.affinity

Gibt an, ob die Sitzungsaffinität aktiviert ist.

Diese Einstellung wird in Verbindung mit der erweiterten Einstellung von `session.affinity.services` verwendet.

Datentyp:
Boolesch

Standardwert:
`Falsch`

event.check.active

Gibt an, ob die Konsistenzprüfung aktiv ist.

Mögliche Werte: 1 für 'true', '0' (oder 'Alles andere') für 'false'

Datentyp:
Ganze Zahl

Standardwert:
`0`

event.check.interval

Gibt das Intervall (in Minuten) an, wenn eine Konsistenzprüfung durchgeführt wird, um sicherzustellen, dass der Monitor-Service-Datensatz von Ereignissen mit der im Content-Store übereinstimmt.

Ein Ereigniskonsistenzchecker-Thread bereinigt alle Diskrepanzen.

Datentyp:
Ganze Zahl

Standardwert:
`10`

event.finished.check.active

Aktiviert oder inaktiviert den Massenbereinigungsprozess für abgeschlossene Tasks in NC-Tabellen. Der Prozess verwendet das Script `BulkFinishedTaskCleanerThread` . Das Script wird vom Monitor-Service eingeleitet, wenn der Service als Teil des Cognos-Service-Starts gestartet wird.

Wenn das System erkennt, dass diese Eigenschaft aktiviert ist, wird das Bereinigungsscript aus `BulkCleanStmtsObjectFactory`geladen. Das Script ist datenbankspezifisch und wird in einer einzigen Transaktion ausgeführt, um alle fertigen Datensätze zu löschen, die die Entfernungskriterien erfüllen.

Datentyp:
Boolesch

Standardwert:
`Wahr`

event.finished.check.interval

Gibt das Intervall (in Sekunden) an, in dem der Massenbereinigungsprozess auf abgeschlossene Tasks in NC-Tabellen prüft. Die Aufgaben, die vor mehr als 24 Stunden erledigt wurden, sind Kandidaten für die Massenbereinigung.

Der Standardwert ist 3600 Sekunden (1 Stunde), aber im Idealfall sollten es 86400 Sekunden (24 Stunden) sein.

Datentyp:
Ganze Zahl

Standardwert:
`3600`

event.finished.check.threshold

Definiert die maximale Anzahl der beendeten Tasks in den NC-Tabellen, die zum Entfernen ausgewählt werden.

Datentyp:
Ganze Zahl

Standardwert:
`10`

primary.wait.ms

Gibt den Schwellenwert für die primäre Wartezeit (in Sekunden) für den Überwachungsservice an.

Diese Einstellung wird verwendet, wenn ein Wert in der Anforderung nicht festgelegt ist.

Datentyp:
Ganze Zahl

Standardwert:
120

session.affinity.services

Wenn enable.session.affinity auf Wahrgesetzt ist, gibt diese Einstellung die Services an, die für die Sitzungsaffinität konfiguriert werden sollen.

In einem N/N-1-Szenario wird diese Einstellung nur von den folgenden IBM Cognos Planning-Services unterstützt: PlanungsverwaltungConsoleService, PlanningDataService, PlanungRuntimeServiceund PlanungTaskService. Andernfalls wird diese Einstellung in einer homogenen verteilten Umgebung von allen Services unterstützt.

Verwenden Sie den obligatorischen Parameter Servicename , um den Service (en) anzugeben. Um mehrere Services zu konfigurieren, trennen Sie die einzelnen Services jeweils mit einem Semikolon (;). Hier zwei Beispiele:

- serviceName=planningTaskService
- serviceName=planningTaskService; serviceName=planningDataService

Zwei optionale Parameter stellen spezifisere Konfigurationsmöglichkeiten bereit:

- serverGroup: Gibt den Namen der Servergruppe an.
- numThreads: Gibt die maximal zulässige Anzahl gleichzeitig ablaufender Tasks an. Der Standardwert ist 2.

Parameter müssen durch ein Komma (,) getrennt werden. Beispiel:

```
serviceName=planningTaskService,serverGroup=mygroup,numThreads=4
```

Datentyp:
Zeichenfolge

Standardwert:
Keine

sds.instance.interval

Gibt das Aktualisierungsintervall (in Sekunden) für Serviceinstanzen an, die registriert werden sollen, damit sie aktiv sind.

Der Überwachungsservice verwendet diesen Mechanismus, um festzustellen, ob andere Überwachungsservices aktiv sind. Wenn ein Überwachungsservice fehlschlägt, kann ein anderer Überwachungsservice für den fehlgeschlagenen Service die Bereinigung durchführen, einschließlich der Aktualisierung der Historie für fehlgeschlagene Tasks.

Services können wählen, um für einen anderen Dienst zu bereinigen, wenn dieser Service seine Registrierung nicht innerhalb einer angemessenen Frist aktualisiert hat. Derzeit ist dieser Grenzwert doppelt so hoch wie die Einstellung sds.instance.interval .

Datentyp:
Ganze Zahl

Standardwert:
30

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

enable.tide.metrics.taskqueue

Aktiviert die Erfassung und Anzeige bestimmter Messwerte für den Überwachungsservice in der IBM Cognos Administration.

Die folgenden Metriken sind enthalten:

· Zeit in Warteschlangenhochwasserzeichen

· Zeit in Warteschlange mit niedrigem Wasserzeichen

· Zeit in Warteschlange

· Anzahl Warteschlangenanforderungen

· Hochwasserzeichen für Warteschlangenlänge

· Untere Grenze für Warteschlangenlänge

Datentyp:
Boolesch

Standardwert:
`Falsch`

sdk.service.poll.interval

Die Zeitdauer in Sekunden, die der Monitor-Service wartet, bevor er eine Clientanwendungsanforderung erneut an einen Verbindungsservice-Service anstellt.

Datentyp:
Ganze Zahl

Standardwert:
`30`

advanced.history.write

Gibt an, ob die letzten Histogramme mit dem erweiterten (erweiterten) Thread-Pool geschrieben werden.

Wenn `Wahr`, werden die letzten Historien mit mehreren Threads geschrieben. Wenn `Falsch`, werden die letzten Histogramme in einem einzelnen Thread geschrieben.

Datentyp:
Boolesch

Standardwert:
`Wahr`

advanced.parent.history.threads

Die Anzahl der Worker-Threads, die zum Erstellen von Stammverlaufsobjekten im Content-Store verwendet werden.

Setzen Sie `advanced.history.write` auf `Wahr` , um diese Einstellung zu aktivieren.

Datentyp:
Ganze Zahl

Standardwert:
2

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

advanced.child.history.threads

Die Anzahl der Threads, die zum Erstellen von untergeordneten Protokollobjekten für Schritte im Content Store verwendet werden.

Setzen Sie `advanced.history.write` auf `Wahr` , um diese Einstellung zu aktivieren.

Datentyp:
Ganze Zahl

Standardwert:
5

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

write.child.histories

Steuert das Schreiben von untergeordneten Protokollobjekten in den Content-Store.

Wenn `Wahr`, werden die endgültigen Protokollobjekte für alle untergeordneten Tasks geschrieben. Wenn `Falsch`nur das letzte Protokollobjekt für die Stammtask geschrieben wird und die Verlaufsobjekte für die untergeordneten Tasks gelöscht werden. Sie können diese Einstellung verwenden, um die Leistung für Tasks zu verbessern, bei denen die Schreibzeit für untergeordnete Protokollobjekte sehr hoch ist.

Datentyp:
Boolesch

Standardwert:
`Wahr`

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

write.child.histories.during.failover

Gibt an, ob bei einem Failover endgültige Protokollobjekte für eine Task in den Content-Store geschrieben werden.

Wenn der Wert von `write.child.histories` auf `Wahr`gesetzt ist, werden untergeordnete Protokollobjekte und Verlaufsobjekte für Roottasks geschrieben.

Datentyp:
Boolesch

Standardwert:
`Wahr`

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

connection.tracker.use

Verfolgt die Verbindungsverwendung.

Wenn `Wahr`verwendet wird, werden Java-Proxy-Objekte verwendet, um die Aktivitäten von JDBC-Objekten zu verfolgen.

Datentyp:
Boolesch

Standardwert:
`Falsch`

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

connection.write.maxwaittime

Die maximale Zeit (in Sekunden), die ein Objekt wartet, um eine Lese-/Schreibverbindung vom JDBC-Verbindungspool abzurufen.

Datentyp:
Ganze Zahl

Standardwert:
10

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

connection.write.maxConnections

Die maximale Anzahl der im Verbindungspool verwendeten JDBC-Verbindungen für das Lesen und Schreiben.

Jede Wertegruppe, die kleiner als das Minimum ist, hat keine Auswirkung und der angegebene Mindestwert wird angewendet.

Mindestwert: 5

Datentyp:
Ganze Zahl

Standardwert:
10

connection.read.maxwaittime

Die maximale Zeit (in Sekunden), die ein Objekt wartet, um eine schreibgeschützte Verbindung vom JDBC-Verbindungspool abzurufen.

Datentyp:
Ganze Zahl

Standardwert:
10

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

connection.read.maxConnections

Die maximale Anzahl schreibgeschützter JDBC-Verbindungen, die in dem Verbindungspool verwendet werden.

Jeder Wert, der kleiner als der Mindestwert ist, hat keine Auswirkung, und der angegebene Mindestwert wird angewendet.

Datentyp:
Ganze Zahl

Standardwert:
8

Anmerkung:

Sie müssen den Service erneut starten, damit diese Einstellung wirksam wird.

Erweiterte Einstellungen für Abfrageservice

In diesem Abschnitt werden die erweiterten Einstellungen für den Abfrageservice beschrieben. Dieser Service unterstützt den dynamischen Abfragemodus.

qsMaxCrossjoinInteractiveOrderOfMagnitude

Gibt die Größenordnung der maximalen Anzahl von Zellen für eine interaktive Abfrage an, z. B. ein Dashboard oder eine Exploration.

Der Standardwert ist 5, wodurch Visualisierungen mit 100000 Zellenwerten möglich sind. Diese Einstellung verhindert, dass der Abfrageservice versucht, eine überhöhte Anzahl von Zellen zu laden, die dazu führen könnte, dass die Abfrageausführung austoben kann. Außerdem wird verhindert, dass der Abfrageservice aus den Rekurses und dem Absturz läuft.

Anmerkung: Wenn eine Visualisierung die maximal zulässige Anzahl von Zellen überschreitet, wird die folgende Fehlernachricht angezeigt:

Fehler XQE-MDX-0020-Die Abfrage: *query_name* erfordert mehr Ressourcen als zulässig. Die geschätzte Anzahl der Zellen *nnnnnn* überschreitet den zulässigen Wert von 100000. Wenden Sie Filter auf projizierte Gruppen an, um die Anzahl der Zellen zu reduzieren.

In diesem Fall sollte der Benutzer die Sätze filtern, bevor er sie projiziert.

Datentyp:
Ganze Zahl

Standardwert:
5

qs.queryExecution.flintServer.loadingPolicy

Gibt die Laderichtlinie für den Compute-Service an. Dieser Service kann gestartet werden, wenn der Abfrageservice gestartet wird, oder verzögert werden, bis eine Abfrage erforderlich ist, für die der Rechenservice erforderlich ist.

Wenn ein Cognos Application-Tier-Server einen großen Prozentsatz des verfügbaren RAM verwendet und keine Workload, die hochgeladene Dateien oder Dateien verwendet, den Prozess verzögert, bis der Server gestartet wird, ist eine kleine Speicherersparnis möglich.

Die folgenden Werte können verwendet werden:

- `Einsatz` -Der Rechenservice wird gestartet, wenn der Abfrageservice gestartet wird.
- `faul` -Der Rechenservice wird verzögert, bis eine Abfrage erforderlich ist, für die dieser Co-Prozess erforderlich ist.

Datentyp:
Zeichenfolge

Standardwert:
`Einsatz`

qs.queryExecution.flintServer.maxHeap

Gibt die maximale Speichermenge an, die der Compute-Service verwenden darf.

Der Wert kann 4096 (Standardwert) oder eine positive ganze Zahl größer als 4096 sein. Die Verwendung eines höheren Werts ist möglicherweise erforderlich, wenn Workloads mehr Speicher benötigen, um abgeschlossen zu werden.

Datentyp:
Positive ganze Zahl

Standardwert:
4096

qs.queryExecution.flintServer.minHeap

Die Mindestspeicherkapazität, die der Compute-Service verwenden darf.

Der Wert kann 1024 (Standardwert) oder eine positive ganze Zahl größer als 1024 sein.

Datentyp:
Positive ganze Zahl

Standardwert:
`1024`

qs.queryExecution.flintServer.sparkThreads

Gibt die maximale Anzahl von Threads an, die der Compute-Service für Serviceabfragen verwenden kann.

Der angegebene Wert muss eine positive ganze Zahl größer als 1 sein.

Datentyp:
Positive ganze Zahl

qs.queryExecution.flintServer.extraJavaOptions

Gibt zusätzliche Parameter an, die an den Compute-Service übergeben werden können.

Datentyp:
Zeichenfolge

Erweiterte Einstellungen für Berichtsservice und Stapelberichtsservice

In diesem Abschnitt werden die erweiterten Einstellungen für den Berichtsservice und den Stapelberichtsservice beschrieben.

BDS.split.maxKeysPerChunk

Gibt die maximale Schlüsselgrenze für die Verarbeitung von Burstberichten an. Wenn Sie den Schlüsselgrenzwert festlegen, können Sie komplexe SQL-Klauseln vermeiden, wenn die Einstellung RSVP.BURST_DISTRIBUTION auf `Wahr`gesetzt ist. Der Wert von `0` legt keinen Grenzwert für diesen Parameter fest.

Datentyp:
Positive ganze Zahl

Standardwert:
`1000`

EnableChartTransparencyIE

Gibt an, ob Diagramme Internet Explorer-Anzeigefilter verwenden, um die Transparenz zu aktivieren.

Datentyp:
Boolesch

Standardwert:
`Wahr`

HyperlinkButtonNewWindow

Gibt an, dass ein neues Fenster erstellt wird, wenn auf eine Hyperlink-Schaltfläche geklickt wird.

Datentyp:
Boolesch

Standardwert:
`Falsch`

HyperlinkMultipleToolbars

Gibt an, dass doppelte Symbolleisten in HTML-Berichten zulässig sind. Auf "false" gesetzt, um doppelte Symbolleisten aus dem Erscheinen zu entfernen.

Datentyp:
Boolesch

Standardwert:
`Wahr`

RSVP.ATTACHMENTENCODING.BASE64EXTENDED

Gibt an, ob die Base64-Codierung bei der Generierung von Berichtsausgaben im MHT-oder XWLA-Format verwendet wird.

In einigen Fällen, wenn benutzerdefinierte Anwendungen das Ausgabeformat `MHT` oder `XLWA` für Berichte angeben, können Probleme mit Zeilenendezeichen, die in der XML-Ausgabe verwendet werden, Anwendungen daran hindern, den Bericht zu öffnen.

Datentyp:
Boolesch

Standardwert:
`Falsch`

RSVP.BURST_DISTRIBUTION

Gibt an, ob Burstberichte parallel oder sequenziell ausgeführt werden. Wenn Sie den Standardwert von `Falsch`verwenden, werden die Jobs nacheinander ausgeführt, was mehr Zeit in Anspruch nimmt.

Diese Einstellung entspricht der Burstoption **Parallel ausführen** in der Benutzerschnittstelle. Diese Einstellung ist nur gültig, wenn **Parallel ausführen** auf **Standard**gesetzt ist. Wenn die Option **Parallel ausführen** auf **Inaktiviert** oder **Aktiviert**gesetzt ist, überschreibt sie diese Einstellung.

Datentyp:
Boolesch

Standardwert:
`Falsch`

RSVP.BURST_QUERY_PREFETCH

Wenn Sie diese Option auf `Wahr`setzen, aktivieren Sie das Vorablesezugriff für Abfragen. Dadurch werden die Burstberichtsausgaben sehr viel schneller erzeugt, da die Abfragen parallel zur Berichtswiedergabe ausgeführt werden. Diese Einstellung gilt nur für relationale Modelle für den dynamischen Abfragemodus.

Datentyp:
Boolesch

Standardwert:
`Falsch`

RSVP.CHARTS.ALTERNATECOLOURS

Gibt an, dass jede Diagramminstanz Farben in der Palettenreihenfolge zuordnet und nicht versucht, die Farbe von Elementen von einer Diagramminstanz in eine andere zu erhalten.

Datentyp:
Boolesch

Standardwert:
`Falsch`

RSVP.CONCURRENTQUERY.ENABLEDFORINTERACTIVEOUTPUT

Ermöglicht die gleichzeitige Abfrageausführung, wenn der Berichtsservice interaktive Ausgabe erstellt.

Datentyp:
Boolesch

Standardwert:
Falsch

RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT

Gibt die maximale Anzahl an Abfrageausführungs-Helfern für jeden Bericht an. Dieser Parameter wird verwendet, um zu verhindern, dass ein einzelner Bericht alle verfügbaren Helfer für die Abfrageausführung konsumiert.

Datentyp:
Ganze Zahl

Standardwert:
1

RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS

Ermöglicht die gleichzeitige Ausführung von Abfragen und legt die maximale Anzahl von Abfrageausführungs-Helfern für jeden Berichtsservice oder Stapelberichtsserviceprozess fest. Der Standardwert ist 0. Dies bedeutet, dass die gleichzeitige Ausführung von Abfragen inaktiviert ist.

Datentyp:
Ganze Zahl

Standardwert:
0

RSVP.CSV.DELIMITER

Gibt das für die CSV-Ausgabe verwendete Feldbegrenzerzeichen an.

Datentyp:
Zeichenfolge

Standardwert:
TABULATORTASTE

RSVP.CSV.ENCODING

Gibt die Codierung an, die beim Generieren der CSV-Ausgabe verwendet wird.

Datentyp:
Zeichenfolge

Standardwert:
utf-16le

RSVP.GROUP_METADATA_REQUESTS

Gibt an, ob Metadatenanforderungen nach Möglichkeit gruppiert werden, um die Leistung zu verbessern. Benutzer können die Gruppierung von Metadatenanforderungen inaktivieren, indem sie diesen Parameter auf 'false' setzen.

Datentyp:
Boolesch

Standardwert:
Wahr

RSVP.CSV.MIMETYPE

Gibt den MIME-Typ an, der der CSV-Ausgabe zugeordnet wird.

Datentyp:
Zeichenfolge

Standardwert:
`application/vnd.ms-excel/`

RSVP.CSV.QUALIFIER

Gibt das Zeichenfolgequalifikationsmerkmal an, das für die CSV-Ausgabe verwendet wird.

Datentyp:
Zeichenfolge

Standardwert:
"

RSVP.CSV.REPEAT_XTAB_LABELS

Gibt an, ob die Kantenbeschriftungen in einem verschachtelten Kreuztabellenbericht wiederholt werden sollen.

Datentyp:
Boolesch

Standardwert:
`Falsch`

RSVP.CSV.TERMINATOR

Gibt den Zeilenabschlusszeichen an, der für die CSV-Ausgabe verwendet wird.

Datentyp:
Zeichenfolge

Standardwert:
LF

RSVP.DRILL.clearAllMappedParamsOnMismatch

Gibt an, wie die Zuordnung von übergebenen Parameterwerten während einer Drillthrough-Operation verarbeitet wird, wenn einige Parameter nicht zugeordnet werden können. Die Parameterzuordnung wird fortgesetzt (Standardeinstellung), oder die gesamte Zuordnung wird gelöscht und der Benutzer wird zur Eingabe von Werten aufgefordert.

Wenn Sie diese Eigenschaft auf 1 setzen, werden alle anderen zugeordneten Parameter aus der Zuordnungstabelle entfernt, wenn ein Parameter nicht zugeordnet werden kann. Dies kann dazu führen, dass alle fehlenden Parameter erneut angefordert werden. Wenn Sie diese Eigenschaft auf 0 setzen, wenn ein Parameter nicht zugeordnet werden kann, während die Drillthrough-Komponente versucht, die Parameter zuzuordnen, ist die Zuordnung der verbleibenden Parameter nicht betroffen.

Datentyp:
Ganze Zahl

Standardwert:
`0`

RSVP.CSV.TRIMSPACES

Gibt an, dass abschließende Leerzeichen aus der CSV-Ausgabe entfernt werden.

Datentyp:
Boolesch

Standardwert:
`Falsch`

RSVP.DRILL.DynamicFilterUsesBusinessKey

Gibt ein dynamisches Drillthrough-Filterverhalten an. Setzen Sie diese Option auf 1 , wenn Sie einen Drillthrough durchführen möchten, um einen Filter zu generieren, der den Member Business Key anstelle des standardmäßigen Member Caption verwendet.

Datentyp:
Positive ganze Zahl

Standardwert:
`0`

RSVP.DRILL.ExtractSourceContextFromRequest

Gibt an, ob der Berichtsserver versucht, die Metadaten für die Parameter der Drillthrough-Anforderung aus dem Quellenkontext der Anforderung zu extrahieren, anstatt eine neue Metadatenanforderung auszugeben. Durch diese Art der Verarbeitung wird die Leistung einer Drillthrough-Operation verbessert. Es wird standardmäßig aktiviert.

Wenn Sie diese Eigenschaft auf 0 setzen, werden Metadatenanforderungen immer ausgegeben.

Datentyp:
Ganze Zahl

Standardwert:
`1`

RSVP.EXCEL.EXCEL_XLS2007_ENABLE_SHARED_STRINGS_TABLE_SIZE_LIMIT

Diese Einstellung legt fest, ob RSVP.EXCEL.EXCEL_2007_XLS2007_SHARED_STRINGS_TABLE_SIZE_LIMIT aktiviert ist.

Datentyp:
Boolesch

Standardwert:
`Wahr`

RSVP.EXCEL.EXCEL_2007_LARGE_WORKSHEET

Aktiviert die Unterstützung für große Arbeitsblätter von Microsoft Excel 2007. Wenn diese Option auf `Wahr`gesetzt ist, werden Arbeitsblätter mit bis zu 1.048.576 Zeilen unterstützt.

Datentyp:
Boolesch

Standardwert:
`Falsch`

RSVP.EXCEL.EXCEL_2007_OUTPUT_FRAGMENT_SIZE

Passt die interne Speicherfragmentgröße in Zeilen an, die der IBM Cognos Analytics -Server generiert, bevor er auf eine Platte gelöscht wird. Diese Eigenschaft kann nützlich sein, wenn Probleme auftreten, z. B. bei der Ausführung von Speicherausgriffen, wenn Berichte mit dem Standardwert generiert werden. Möglicherweise müssen die Werte gesenkt werden, damit der Bericht erfolgreich ausgeführt werden kann.

Datentyp:
Ganze Zahl

Standardwert:
`45000` (unverbindlich)

RSVP.EXCEL.EXCEL_2007_XLS2007_SHARED_STRINGS_TABLE_SIZE_LIMIT

Diese Einstellung legt fest, ob die gemeinsam genutzten Zeichenfolgen in der Excel-Ausgabe begrenzt werden sollen. Durch die Begrenzung von gemeinsam genutzten Zeichenfolgen wird die Dateigröße der Excel-Ausgabe erhöht. Wenn gemeinsam genutzte Zeichenfolgen unbegrenzt und zu hoch sind, kann dies zu Leistungsproblemen bei Excel führen.

Datentyp:
Ganze Zahl

Standardwert:
`10000`

RSVP.EXCEL.EXCEL_2007_WORKSHEET_MAXIMUM_ROWS

Gibt die Anzahl der Zeilen an, die ausgegeben werden sollen, bevor sie in ein neues Arbeitsblatt versetzt werden.

Datentyp:
Ganze Zahl

RSVP.EXCEL.PAGEGROUP_WSNAME_ITEMVALUE

Gibt an, dass bei der Erzeugung von Ausgabe in Microsoft Excel 2007-Format und Seitenumbrüchen die Arbeitsblattregisterkarten für die Datenelemente benannt werden, die zum Ausbrechen der Seiten verwendet werden.

Anmerkung: Diese Eigenschaft gilt nicht für Analysis Studio.

Datentyp:
Boolesch

Standardwert:
`Falsch`

RSVP.EXCEL.XLS2007_ALLOW_WRAPPING_SINGLE_CELL

Gibt an, ob Text innerhalb einer Zelle in Excel-Ausgaben eingeschlossen wird.

Datentyp:
Boolesch

Standardwert:
`Falsch`

RSVP.EXCEL.XLS2007_COLUMN_WIDTH_CONTROL

Verhindert das Zusammenführen von Zellen in Excel 2007-Berichtsausgaben, wenn Sie die Werte für die Größe und den Überlauf für eine Spalte festlegen.

Datentyp:
Boolesch

Standardwert:
`Falsch`

RSVP.EXCEL.XLS2007_FULLDECIMALPRECISION

Wenn diese Option auf 'true' gesetzt ist, werden Zahlen in der Excel-Ausgabe mit bis zu 15 Dezimalstellen wiedergegeben. Wenn der Wert auf "false" (Standardwert) gesetzt ist, können die Zahlen maximal 12 Dezimalstellen enthalten.

Datentyp:
Boolesch

Standardwert:
Falsch

RSVP.EXCEL.XLS2007_PRINT_MEDIA

Gibt an, ob der Stil Don't Print (Don't Print) auf Excel 2007-Berichtsausgaben angewendet wird.

Datentyp:
Boolesch

Standardwert:
Wahr

RSVP.FILE.EXTENSION.XLS

Gibt an, dass XLS als Dateierweiterung im XLS-Ausgabeformat E-Mail-Anhänge anstelle von HTML verwendet werden soll.

Datentyp:
Zeichenfolge

Standardwert:
Falsch

RSVP.PARAMETER_CACHE

Gibt an, ob das Caching von Parametern auf Serverebene aktiviert oder inaktiviert ist. Standardmäßig ist das Caching von Parametern aktiviert.

Wenn RSVP eine getParameters-Anforderung ausgibt, speichert er die Ergebnisse in einem untergeordneten Objekt unter dem Berichtsobjekt in IBM Cognos Content Manager. Auf diese Weise kann der Cache erstellt oder aktualisiert werden, ohne dass die Berichtsspezifikation geändert werden muss. Wenn RSVP Parameterinformationen benötigt, verwendet er die zwischengespeicherten Informationen von Content Manager. Wenn der Cache die von RSVP erforderlichen Informationen nicht enthält, ruft RSVP die Abfrageengine direkt auf, um die Informationen abzurufen.

Der Cache wird durch die Erstellung einer ReportService-SOAP-Anforderung ("getParameters") für den Stapelberichtsservice mit der Ausführungsoption `http://developer.cognos.com/ceba/constants/runOptionEnum#createParameterCache`gefüllt. Wenn RSVP feststellt, dass der Cache fehlt oder veraltet ist, wirkt sich die Erstellung des Cache nicht auf die Ausführung des Berichts aus, da der Cache durch eine unabhängige Anforderung erstellt wird. Da die Anforderung jedoch vom Stapelberichtsservice verarbeitet wird, wird ein Protokolleintrag erstellt, der in der Ausführungshistorie eines Berichts sichtbar ist.

Die Cache-Erstellung wird ausgelöst, wenn ein Bericht erstellt oder von Cognos Analytics Reporting aktualisiert wird, sowie wenn ein Bericht ausgeführt wird und RSVP den vorhandenen Cache bestimmt, der veraltet ist. RSVP verwendet die Version des Moduls oder des Stammmodells des Berichts, um festzustellen, ob der Cache veraltet ist.

Datentyp:
Boolesch

Standardwert:
Wahr

RSVP.PARAMETERS.LOG

Gibt an, ob die Berichtslaufoptionen und die Eingabeaufforderungsparameter beim Protokollierungssystem protokolliert werden müssen.

Datentyp:
Boolesch

Standardwert:
Falsch

RSVP.PARAMETERS.SAVE

Gibt an, dass Eingabeaufforderungswerte, die von einem Benutzer eingegeben werden, automatisch gespeichert werden.

Datentyp:
Boolesch

Standardwert:
`Falsch`

RSVP.PRINT.POSTSCRIPT

Gibt an, welche Schnittstelle zum Drucken von PDF-Dokumenten aus einem UNIX -Betriebssystem verwendet werden soll. Wenn diese Option auf `Falsch`gesetzt ist, wird die Adobe -Acrobat-PDF-Schnittstelle verwendet. Andernfalls wird die interne Postscript-Schnittstelle verwendet.

Datentyp:
Boolesch

Standardwert:
`Wahr`

RSVP.PROMPT.CASTNUMERICSEARCHKEYTOSTRING

Gibt an, dass numerische Datenelemente in ein Zeichenfolgeformat (varchar) konvertiert werden sollen. Dies kann erforderlich sein, wenn Ihre Datenquelle numerische Datenelemente nicht in Zeichenfolgen konvertiert.

Datentyp:
Boolesch

Standardwert:
`Wahr`

RSVP.PROMPT.EFFECTIVEPROMPTINFO.IGNORE

Inaktiviert die Ausgabe des Attributs `effectivePromptInfo` in Metadatenanforderungen und inaktiviert das Verschieben der Eingabeaufforderungsinformationen von unter dem Attribut "caption" einer Ebene auf das Niveau selbst. Dies ist das Standardverhalten.

Datentyp:
Boolesch

Standardwert:
`Falsch`

RSVP.PROMPT.RECONCILIATION

Gibt eine systemweite Konfiguration an, die definiert, wie Abfragen und Abfragegruppen verarbeitet werden.

Eine Beschreibung der möglichen Werte dieser Einstellung finden Sie im Artikel zum Festlegen der Priorisierung von Abfragen in der *IBM Cognos Analytics Administration and Security Guide* .

Datentyp:
Ganze Zahl oder Zeichenfolge

Standardwert:
`0` oder `VOLLSTÄNDIG`

RSVP.PROMPT.RECONCILIATION.CHUNKSIZE

Gibt die Chunkgröße an, wenn der Wert der Einstellung RSVP.PROMPT.DATENABGLEICH `CHUNKED GRUPPIERT` oder `CHUNKED`ist.

Datentyp:
Positive ganze Zahl

Standardwert:
5

RSVP.PROMPTCACHE.LOCALE

Gibt die Ländereinstellung an, die anstelle der im Bericht angegebenen Ländereinstellung verwendet werden soll, wenn Eingabeaufforderungscachedaten erstellt, aktualisiert oder verwendet werden. Dies bedeutet, dass für jeden Bericht unabhängig von der Ländereinstellung des Berichtsbenutzers ein einzelner Eingabeaufforderungscache verwendet wird.

Datentyp:
Zeichenfolge

RSVP.RENDER.PDF_FONT_SWITCHING

Gibt an, dass jedes Zeichen in einer Zeichenfolge in der bevorzugten Schriftart angezeigt wird. Die bevorzugte Schriftart ist eine beliebige Schriftart, die in einer Berichtsspezifikation aufgelistet ist, gefolgt von den Schriftarten, die in der Cascading Style Sheet-Datei (css) für globale Stile aufgelistet sind. Wenn ein Zeichen in der bevorzugten Schriftart nicht verfügbar ist, wird es mit der nächsten Schriftart in der Liste angezeigt.

In früheren Versionen wurde eine Schriftart nur verwendet, wenn alle Zeichen in einer Zeichenfolge mit dieser Schriftart angezeigt werden konnten. Ausgehend von IBM Cognos Business Intelligence 10.1 wird die bevorzugte Schriftart auf Zeichenebene angewendet. Als Ergebnis kann ein Wort mit verschiedenen Schriftarten angezeigt werden, oder es können einige Schriftarten größer sein, was zu einer Wortumhüllung führen kann.

Setzen Sie den Parameterwert auf "false", um das Schriftartwählverhalten früherer Versionen wiederherzustellen.

Datentyp:
Boolesch

Standardwert:
`Wahr`

RSVP.RENDER.ROUNDING

Gibt die Rundungsregel für die Datenformatierung an.

In früheren Versionen wurde die `halfeven` -Regel beim Runden von Zahlen verwendet. Diese Regel wird häufig in der Buchführung verwendet. Präzisionsregeln in einigen Regionen erfordern jedoch unterschiedliche Rundungsregeln, z. B. die Regel `HalfUp` . Ab Version IBM Cognos Business Intelligence 10.2.0 können Sie eine Rundungsregel auswählen, die den Genauigkeitsregeln in Ihrer Organisation entspricht.

Die folgenden Rundungsregeln sind verfügbar:

halfeven
Rundet den nächsten Nachbarn ab, bei dem ein äquidistanter Wert auf den nächsten Nachbarn gerundet wird.

HalfDown
Rundet zum nächsten Nachbarn ab, bei dem ein äquidistanter Wert abgerundet wird.

HalfUp
Rundet zum nächsten Nachbarn ab, bei dem ein äquidistanter Wert aufgerundet wird.

Obergrenze
Rundet auf eine positivere Zahl ab.

Fußboden
Rundet auf eine negative Zahl ab.

Inaktiv
Rundet auf Null ab.

Bis
Rundet von Null ab.

Datentyp:
Zeichenfolge

Standardwert:
`halfeven`

RSVP.RENDER.VALIDATEURL

Specifies whether IBM Cognos Application Firewall validation is imposed on URLs that are contained within a report specification (including URLs on image tags, buttons, hyperlinks, and background images in CSS rules) or are specified by the cssURL run option of the report.

Wenn diese Option auf `Wahr` und CAF in aktiviert gesetzt ist, erfolgt die Validierung mit den folgenden Regeln:

- Vollständig qualifizierte oder absolute URLs:

  `protocol://host [:port] /path [?abfrage]`

  Dabei ist `Protokoll` entweder 'http' oder 'https', und der `Host` wird anhand der gültigen Domänenliste validiert.

- URLs relativ zum Installationswebstammverzeichnis des Servers:

  `/< Installationsstammverzeichnis> /.*`

  Dabei ist `< Installationsstammverzeichnis >` der Gateway-Dateipfad, der aus dem Gateway-URI in IBM Cognos Configuration übernommen wird. Beispiel: `/ibmcognos/ps/portal/images/action_delete.gif`

- Eine der folgenden spezifisch zulässigen URLs:
  - `about: leer` (Groß-/Kleinschreibung wird nicht beachtet)
  - `JavaScript:window.close ()` (Groß-/Kleinschreibung muss nicht beachtet werden, mit oder ohne abschließenden Semikolon)
  - `JavaScript:parent.close ()` (Groß-/Kleinschreibung muss nicht beachtet werden, mit oder ohne abschließenden Semikolon)
  - `JavaScript:history.back ()` (Groß-/Kleinschreibung muss nicht beachtet werden, mit oder ohne abschließenden Semikolon)
  - `parent.cancelErrorPage ()` (Groß-/Kleinschreibung muss nicht beachtet werden, mit oder ohne abschließenden Semikolon)
  - `doCancel ()` (Groß-/Kleinschreibung muss nicht beachtet werden, mit oder ohne abschließenden Semikolon)

Datentyp:
Boolesch

Standardwert:
`Falsch`

RSVP.REPORTSPEC.LOG

Gibt an, ob Berichtsspezifikationen in dem Protokollierungssystem protokolliert werden müssen.

Datentyp:
Boolesch

Standardwert:
`Falsch`

Erweiterte Einstellungen des Repository-Service

In diesem Abschnitt werden die erweiterten Einstellungen für den Repository-Service beschrieben.

repository.maxCacheDocSize

Die maximale Größe eines einzelnen Berichts in MB, der im Cache gespeichert werden kann.

Der Wert muss eine positive ganze Zahl (größer als 0) sein. Berichte, die größer sind als die angegebene Größe, werden nicht zwischengespeichert und werden aus dem Repository abgerufen.

Datentyp:
Ganze Zahl

Standardwert:
`10`

Erweiterte UDA-Einstellungen

In diesem Abschnitt werden erweiterte Einstellungen für Universal Data Access (UDA) beschrieben.

Die folgenden Datenbanknamen werden in den erweiterten UDA-Einstellungen erkannt:

- SYBASE ASE
- IBM Db2
- INFORMIX
- MICROSOFT SQL SERVER
- NETEZZASQL
- NCLUSTER
- WEBSPHERE CLASSIC FEDERATION
- GREENPLUM
- INTERBASE
- INGRES
- SYBASE-IQ
- INGRES_VECTORWISE
- PARACCEL
- POSTGRESQL
- TERADATA
- VERTICA DATABASE
- ORACLE
- SAP R3
- XML

Wenn der Datenbankname nicht erkannt wird, wird die Einstellung nicht gelesen. Wenn Sie über andere Datenbanken verfügen, die nicht aufgelistet sind, oder wenn Ihre ODBC-Treiber einen anderen Datenbanknamen zurückgeben, verwenden Sie den Datenbanknamen, der aus dem Attribut SQL_DBMS_NAME des ODBC-Attributs SQLGetInfo () abgerufen wird.

UDA.CALL_ODBC_SQLNUMRESULTCOLS

Ruft die Spaltenanzahl ab, die für eine Abfrage festgelegt ist.

Syntax:
UDA.CALL_ODBC_SQLNUMRESULTCOLS= "Datenbankname: Boolescher Wert"

Datentyp:
Boolesch

Standardwert:
Wahr

UDA.CONVERT_TIMESTAMP_LITERAL_TO_DATE_LITERAL

Da die Spalte 'Oracle DATE' die Datums-und Uhrzeitteile enthält, meldet die UDA den Oracle DATE-Datentyp als TIMESTAMP.

IBM Cognos behandelt die Oracle DATE-Spalte als TIMESTAMP und generiert ein TIMESTAMP-Literal in dem Filter.

Wenn Sie die Spalte DATE und das Literal TIMESTAMP vergleichen, fügt die Oracle-Optimierung in der Spalte DATE eine interne Funktion hinzu, um den Vergleich kompatibel zu machen. Dies wirkt sich auf die Leistung von Oracle aus.

Dieser Eintrag ist nur für Oracle spezifisch. Wenn der boolesche Wert auf 'true' gesetzt ist, konvertiert die UDA das TIMESTAMP-Literal mit dem Wert 0 in ein DATE-Literal. Oracle verwendet die Indexsuche in einer DATE-Spalte.

Syntax:
UDA.CONVERT_TIMESTAMP_LITERAL_TO_DATE_LITERAL= "Datenbankname: Boolescher Wert"

Datentyp:
Boolesch

Standardwert:
Falsch

UDA.INCLUDE_DST_TIMEZONE

Verwenden Sie diese Einstellung, um die Sommerzeit (Sommerzeit) in der Zeitmarke mit der Zeitzonendatenart einzuschließen.

Wenn diese Einstellung auf "true" gesetzt ist, wird DST in alle Operationen eingeschlossen, die die Zeitmarke des Datentyps mit der Zeitzone verwenden, z. B. "current_timestamp". Wenn diese Einstellung falsch ist, wird DST von solchen Operationen ausgeschlossen.

Syntax:
UDA.INCLUDE_DST_TIMEZONE= Boolescher Wert

Datentyp:
Boolesch

Standardwert:
Wahr

UDA.NATIVE_SQL_IN_CTE

Steuert, wie das native SQL im Befehlstabellenausdruck einer WITH-Klausel verarbeitet wird.

Wenn der boolesche Wert auf KEEP gesetzt ist, wird die native SQL als Teil einer Klausel WITH auf die zugrunde liegende Datenbank übertragen.

Wenn der boolesche Wert auf "PT" gesetzt ist, wird das native SQL als natives SQL-DurchgriffsSQL betrachtet. Die SQL selbst wird in die Datenbank übertragen.

Wenn der boolesche Wert auf DT gesetzt ist, wird die Klausel WITH entfernt, und alle Befehlstabellenausdrücke werden in abgeleitete Tabellen konvertiert.

Syntax:
UDA.NATIVE_SQL_IN_CTE= "Datenbankname: Zeichenfolgewert"

Datentyp:
Boolesch

Standardwert:
KEEP

UDA.PARSE_ANSI_NUMERIC_LITERAL

Gibt an, ob der UDA-SQL-Parser das numerische Literal mit Dezimalzeichen (z. B. 1,23) als exakten numerischen Wert (z. B. Dezimalzahl) oder als ungefährer Wert (z. B. doppelt) liest.

Wenn die Einstellung wahr ist, liest der UDA-SQL-Parser das numerische Literal mit Dezimalzeichen als exakten numerischen Wert. Werte mit der Anzahl der Ziffern kleiner als 9 werden als ganze Zahl mit Maßstab gelesen. Werte mit der Anzahl der Ziffern 10-18 werden als Quad mit Maßstab gelesen. Werte mit der Anzahl der Ziffern 19-77 werden als Dezimalzahl (Genauigkeit, Maßstab) gelesen. Der Wert mit der Anzahl der Ziffern größer als 77 wird als doppelt gelesen. Wenn die Einstellung "false" ist, liest der UDA-SQL-Parser das numerische Literal mit Dezimalzeichen als Double.

Syntax:
UDA.PARSE_ANSI_NUMERIC_LITERAL= Boolescher Wert

Datentyp:
Boolesch

Standardwert:
`Wahr`

UDA.PARSE_STRING_LITERAL_AS_VARCHAR

Diese Einstellung gibt an, ob ein Zeichenfolgeliteral als Zeichendatentyp oder als varchar-Datentyp geparst wird.

Wenn der Einstellungswert 'false' ist, liest der UDA-SQL-Parser das Zeichenfolgeliteral als char und das Zeichenfolgeliteral mit dem Präfix N als nchar. Wenn der Einstellungswert 'true' ist, liest der UDA-SQL-Parser das Zeichenfolgeliteral als varchar und das Zeichenfolgeliteral mit dem Präfix N als nvarchar.

Syntax:
UDA.PARSE_STRING_LITERAL_AS_VARCHAR= Boolescher Wert

Datentyp:
Boolesch

Standardwert:
`Falsch`

UDA.REPREPARE_QUERY_FOR_PARAMETER_VALUE

Gibt an, ob die UDA-ODBC-Gateways die Abfrage für jeden Parameterwert erneut vorbereiten.

Syntax:
UDA.REPREPARE_QUERY_FOR_PARAMETER_VALUE= "Datenbankname: Boolescher Wert"

Datentyp:
Boolesch

Standardwert:
`Falsch`

UDA.SET_READONLY_TRANSACTION_AUTOCOMMIT

Wenn Sie mehrere Datenbanken anhängen, müssen Sie diese Eigenschaft auf "true" setzen, um den Modus für automatische Festschreibung für eine einzelne Datenbank zu aktivieren, wenn die Datenbank Transaktionen mit automatischer Festschreibung unterstützt.

Wenn eine der Datenbanken in der Zuordnungsoperation keine automatische Festschreibung von Transaktionen unterstützt, unterstützt die Zuordnungsoperation diese Transaktionen standardmäßig nicht für alle Datenbanken. Wenn Sie diese Eigenschaft auf 'true' setzen, aktivieren Sie die automatische Festschreibung für schreibgeschützte Transaktionen. Der Wert 'false' inaktiviert diese Funktionalität.

Wenn eine Datenbank keine automatischen Commit-Transaktionen unterstützt, kann die Aktivierung dieser Funktionalität die folgende Ausnahme auslösen:

```
UDA-SQL-0178 Der "Start" Parameterblockoption wird nicht unterstützt.
```

Syntax:
UDA.SET_READONLY_TRANSACTION_AUTOCOMMIT= "Datenbankname: Boolescher Wert"

Datentyp:
Boolesch

Standardwert:
`Falsch`

UDA.THREADSTART_TIMEOUT

Gibt ein Zeitlimit in Sekunden an, in dem darauf gewartet wird, dass ein Thread in der UDA-API sqlAOpen gestartet wird. In der API sqlAOpen verwendet die UDA einen separaten Thread, um eine Ergebnismenge zu erstellen, so dass die Ergebnismenge durch die API sqlCancelOpen abgebrochen werden konnte.

Für die Rückwärtsfunktion wird die erweiterte Eigenschaft UDA_THREADSTART_TIMEOUT, die in der Konfiguration von Cognos festgelegt ist, weiterhin unterstützt. Wenn die erweiterte Eigenschaft UDA.THREADSTART_TIMEOUT in den erweiterten Einstellungen jedoch vorhanden ist, wird die erweiterte Eigenschaft UDA_THREADSTART_TIMEOUT von Cognos Configuration ignoriert.

Syntax:
UDA.THREADSTART_TIMEOUT= numerischer Wert

Datentyp:
Positive ganze Zahl (1-600)

Standardwert:
`20`