IBM Cognos Analytics
Version 11.1

Verwaltung - Benutzerhandbuch

©

Produktinformation

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

Copyright

Inhaltsverzeichnis

Kapitel 1. Verwalten von Personen

In IBM® Cognos Analytics können Sie die Benutzerauthentifizierung und den Zugriff auf Inhalte und Produktfunktionen verwalten.

Der Administrator, der die Cognos Analytics-Anwendung konfiguriert, richtet die ersten Sicherheitseinstellungen ein. Dazu gehört das Konfigurieren von Authentifizierungsprovidern, um die vorhandene Sicherheitsinfrastruktur Ihres Unternehmens nutzen zu können. Jeder Authentifizierungsprovider, der für die Verwendung mit Cognos Analytics konfiguriert ist, wird als Namespace oder externer Namespace bezeichnet.

Neben Namespaces, die die externen Authentifizierungsprovider darstellen, verfügt IBM Cognos Analytics über einen integrierten, internen Namespace mit dem Namen **Cognos**. Der **Cognos**-Namespace erleichtert den Prozess der Administration von Zugriffsberechtigungen und der Bereitstellung von Inhalten. Schließlich, wenn die Option **Easy Install** verwendet wurde, um IBM Cognos Analytics zu installieren, können Sie Benutzer im Namespace **Cognos-Benutzer** erstellen.

Cognos Analytics kann zudem für den anonymen Zugriff konfiguriert werden, bei dem Benutzer für den Zugriff auf die Anwendung weder Benutzernamen noch Kennwort bereitstellen müssen. Informationen zum Aktivieren des anonymen Zugriffs finden Sie in der Veröffentlichung *IBM Cognos Analytics - Installation und Konfiguration*.

Wichtig: Möglicherweise verfügt Ihre Umgebung über eine große Anzahl an Benutzern. Es hat sich bewährt, die Benutzer in Ordnern zu gruppieren, wobei jeder Ordner maximal 1000 Benutzer enthalten sollte.

Die Administrationsberechtigung **Benutzer, Gruppen und Rollen** ist für das Verwalten von Konten erforderlich. Weitere Informationen finden Sie unter „Funktionen” auf Seite 124.

Cognos-Namespace und Namespace 'Cognos-Benutzer'

Der **Cognos**-Namespace enthält vordefinierte Objekte, die das Einrichten erster Sicherheitseinstellungen erleichtern. Der Namespace **Cognos-Benutzer** ermöglicht es Ihnen, Benutzer zu erstellen und zu verwalten, die nicht Teil eines authentifizierten externen Namespace sind.

Die vordefinierten Objekte und andere Features des Cognos-Namespace verwenden Sie für das fortlaufende Sicherheitsmanagement.

Der **Cognos**-Namespace kann Gruppen und Rollen enthalten. Eine Gruppe ist eine Sammlung von Benutzern. Benutzer können entweder Mitglieder eines authentifizierten externen Namespace oder des Namespace **Cognos-Benutzer** sein, wenn die Option **Easy Install** zum Installieren von IBM Cognos Analytics verwendet wurde. Mitglieder von Gruppen können Benutzer und andere Gruppen sein. Eine Rolle ist eine Sammlung von Funktionen, die die Tasks identifizieren, zu deren Ausführung ein Benutzer berechtigt ist. Mitglieder von Rollen können Benutzer, Gruppen und andere Rollen sein. Ein Benutzer kann mehreren Gruppen oder Rollen angehören. Wenn ein Benutzer Mitglied von mehreren Gruppen ist, werden die Zugriffsberechtigungen zusammengeführt.

Im folgenden Diagramm ist die Struktur von Gruppen und Rollen im **Cognos**-Namespace dargestellt.

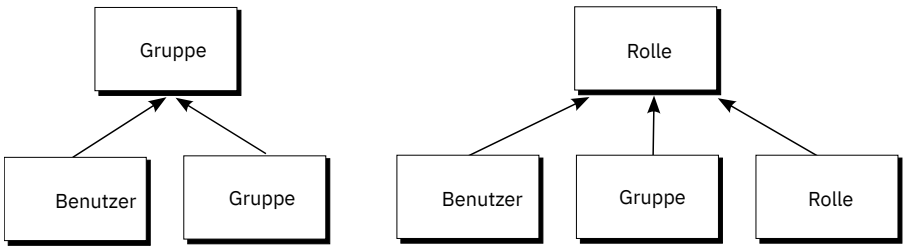


Abbildung 1. Struktur von Gruppen und Rollen

Sie können Gruppen und Rollen im **Cognos**-Namespace erstellen. Der Namespace **Cognos-Benutzer** ist nur verfügbar, wenn bei der Installation von IBM Cognos Analytics die Option **Easy Install** verwendet wurde. Wenn diese Option verfügbar ist, können Sie Benutzer im Namespace **Cognos-Benutzer** erstellen.

Vordefinierte und integrierte Objekte im Cognos-Namespace

Die ursprünglichen Zugriffsberechtigungen werden auf alle vordefinierten Objekte angewendet. Sie können die Berechtigungen über die Objekteigenschaften ändern.

Anonym
Diese Benutzerberechtigung ist für die Erstkonfiguration bestimmt, bei der der anonyme Zugriff aktiviert ist und Benutzer nicht zum Angeben von Berechtigungsnachweisen aufgefordert werden. Wenn der anonyme Zugriff in Cognos Configuration inaktiviert ist, melden sich Benutzer unter Verwendung der eigenen Berechtigungsnachweise an.

Alle authentifizierten Benutzer
Diese Gruppe stellt Benutzer dar, die durch Authentifizierungsprovider authentifiziert wurden. Die Mitgliedschaft dieser Gruppe wird vom Produkt verwaltet und kann nicht angezeigt oder geändert werden.

Alle
Diese Gruppe umfasst alle authentifizierten Benutzer und das Benutzerkonto 'Anonym'. Die Mitgliedschaft dieser Gruppe wird vom Produkt verwaltet und kann nicht angezeigt oder geändert werden. Sie können die Gruppe 'Alle' zum schnellen Einrichten von Standardberechtigungen verwenden. Wenn Sie beispielsweise einen Bericht schützen möchten, können Sie der Gruppe 'Alle' die Berechtigungen zum Lesen, Schreiben oder Ausführen für den Bericht erteilen. Nachdem dieser Zugriffsschutz besteht, können Sie anderen Benutzern, Gruppen oder Rollen Zugriff auf den Bericht erteilen und die Gruppe 'Alle' aus der Sicherheitsrichtlinie für diesen Bericht entfernen.

Analysis-Benutzer
Mitglieder dieser Rolle besitzen dieselben Zugriffsberechtigungen wie Konsumenten. Darüber hinaus können sie IBM Cognos Analysis Studio verwenden.

Analytics-Administratoren

Mitglieder besitzen dieselben Zugriffsberechtigungen wie Analytics-Explorer. Darüber hinaus haben sie Zugriff auf:

- **Verwalten** > **Datenserververbindungen**
- **Datenquellenverbindungen** in der Administrationkonsole
- IBM Cognos Software Development Kit.

Diese Rolle ist nur nach einer angepassten Installation verfügbar.

Analytics-Explorer

Mitglieder besitzen dieselben Zugriffsberechtigungen wie Analytics-Benutzer. Darüber hinaus können sie auf Cognos Analysis for Microsoft Excel, Cognos Framework Manager, Cognos Cube Designer und Dynamic Query Analyzer, Transformer sowie TM1 Writeback, das mit FLBI TM1-Server verwendet wird, zugreifen.

Diese Rolle ist nur nach einer angepassten Installation verfügbar.

Analytics-Benutzer

Mitglieder besitzen dieselben Zugriffsberechtigungen wie Analytics-Anzeigeberechtigte. Sie können neue Berichte, Dashboards, Storys, neue Jobs, Datenserververbindungen und Datenmodule erstellen. Sie können Berichte ausführen, auf Eingabeaufforderungen antworten und Dateien hochladen. Außerdem können Sie auf Cognos for Microsoft Office, Cognos Workspace, Cognos Insight, Cognos Event Studio, Cognos Query Studio und Cognos Analysis Studio zugreifen.

Diese Rolle ist nur nach einer angepassten Installation verfügbar.

Autoren
Mitglieder dieser Rolle besitzen dieselben Zugriffsberechtigungen wie Abfragebenutzer und Analysis-Benutzer. Sie können Reporting, Query Studio und Analysis Studio verwenden und öffentlichen Inhalt, zum Beispiel Berichte und Berichtsausgaben, speichern.

Konsumenten
Mitglieder dieser Rolle können öffentlichen Inhalt, zum Beispiel Berichte, lesen und ausführen.

Verzeichnisadministratoren
Mitglieder dieser Rolle können die Inhalte von Namespaces verwalten. Im Cognos-Namespace verwalten sie Gruppen, Konten, Kontakte, Verteilerlisten, Datenquellen und Drucker.

Analytics-Anzeigeberechtigte

Mitglieder besitzen dieselben Zugriffsberechtigungen wie Abfragebenutzer und Analysis-Benutzer. Sie können Reporting, Query Studio und Analysis Studio verwenden und öffentlichen Inhalt wie Berichte, Dashboards und Storys speichern.

Diese Rolle ist nur nach einer angepassten Installation verfügbar.

Bibliotheksadministratoren
Mitglieder dieser Rolle können auf die Inhalte der Registerkarte **Bibliothek** in IBM Cognos Administration zugreifen und diese importieren und verwalten.

Mobile-Administratoren
Mitglieder dieser Rolle können IBM Cognos Analytics Mobile Reports verwalten.

Mobile-Benutzer
Mitglieder dieser Rolle können auf IBM Cognos-Inhalte, wie beispielsweise Berichte, über IBM Cognos Analytics Mobile Reports zugreifen.

Modellierer
Mitglieder dieser Rolle haben Zugriff auf webbasierte Modellierungsfunktionen.

Portaladministratoren
Mitglieder dieser Rolle können die Cognos-Portlets und andere Portlets verwalten. Dazu gehört auch das Anpassen von Portlets, das Definieren von Portlet-Stilen und das Festlegen von Zugriffsberechtigungen für Portlets.

PowerPlay-Administratoren
Mitglieder dieser Rolle können den öffentlichen Inhalt verwalten, auf den sie über uneingeschränkten Zugriff verfügen. Darüber hinaus können Sie IBM Cognos PowerPlay verwalten und verwenden.

PowerPlay-Benutzer
Mitglieder dieser Rolle besitzen dieselben Zugriffsberechtigungen wie Konsumenten. Darüber hinaus können Sie IBM Cognos PowerPlay verwenden.

Abfragebenutzer
Mitglieder dieser Rolle besitzen dieselben Zugriffsberechtigungen wie Konsumenten. Darüber hinaus können Sie IBM Cognos Query Studio verwenden.

Leser
Mitglieder dieser Rolle verfügen über Lesezugriff auf IBM Cognos-Software. Sie können durch bestimmte Teile des Content Store navigieren, gespeicherte Berichtsausgaben im Portal anzeigen und bestimmte Berichtsoptionen verwenden, wie beispielsweise Drillthrough.

Berichtsadministratoren
Mitglieder dieser Rolle können den öffentlichen Inhalt verwalten, auf den sie über uneingeschränkten Zugriff verfügen. Darüber hinaus können Sie IBM Cognos Analysis Reporting und IBM Cognos Query Studio verwenden.

Serveradministratoren
Mitglieder dieser Rolle können Server, Dispatcher und Jobs verwalten.

Systemadministratoren

Mitglieder dieser Rolle gelten als Rootbenutzer oder Superuser. Sie können auf sämtliche Objekte im Content Store zugreifen und diese ändern, ungeachtet etwaiger Sicherheitsrichtlinien, die für das

entsprechende Objekt festgelegt wurden. Nur Mitglieder der Rolle 'Systemadministratoren' können die Mitgliedschaft dieser Rolle ändern.

Die Erstkonfiguration für diese Rolle enthält die Gruppe 'Alle'. Sie müssen die ursprünglichen Zugriffsberechtigungseinstellungen für diese Rolle ändern und die Gruppe 'Alle' aus ihrer Mitgliedschaft entfernen. Wenn Sie die Erstkonfiguration nicht ändern, haben alle Benutzer unbeschränkten Zugriff auf den Content Store.

Tenantadministratoren
Mitglieder dieser Rolle können Administrationsaufgaben von Tenants ausführen. Diese Rolle wird in einer IBM Cognos-Umgebung mit mehreren Tenants verwendet. In der Erstkonfiguration besitzt diese Rolle keine Mitglieder und keine Funktionen. Nur Systemadministratoren können dieser Rolle Mitglieder hinzufügen und ihr Zugriffsberechtigungen und Funktionen zuordnen.

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 142.
- Informationen zum Ändern der Zugehörigkeit zu Standardrollen finden Sie im Artikel „Schützen von Systemadministratoren und Standardrollen” auf Seite 123.
- 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 181.

Tabelle 1. 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.

Tabelle 1. Vordefinierte Cognos -Standardrollen (Forts.)	
Standardrolle	**Beschreibung**
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.
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.

Erstellen und Verwalten von Gruppen und Rollen

Sie können neue Gruppen und Rollen im **Cognos**-Namespace erstellen. Diese Rollen sind nicht von den Authentifizierungsprovidern abhängig und können nur in IBM Cognos Analytics verwaltet werden.

Sie können Benutzer, Gruppen und Rollen von mehreren externen Namespaces und vom Namespace **Cognos-Benutzer**, falls vorhanden, als Mitglieder zu den Cognos-Gruppen und -Rollen hinzufügen.

Vorbereitende Schritte

Wenn Sie planen, Einträge von mehreren Namespaces als Mitglieder zu den Cognos-Gruppen und -Rollen hinzuzufügen, melden Sie sich bei jedem dieser Namespaces an, bevor Sie den Vorgang beginnen.

Informationen zu diesem Vorgang

Wenn Sie eine Cognos-Gruppe oder -Rolle löschen, sind die darauf basierenden Zugriffsberechtigungen von Benutzern nicht mehr aktiv. Sie können Zugriffsberechtigungen wiederherstellen, indem Sie eine Gruppe oder Rolle mit demselben Namen erstellen.

Sie müssen über die Administrationsberechtigung **Benutzer, Gruppen und Rollen** verfügen, um Konten verwalten zu können. Weitere Informationen finden Sie unter „Funktionen” auf Seite 124.

Hinweis für Cognos Analytics on Demand-Benutzer:

- Die standardmäßigen integrierten Gruppen und Rollen im Cognos-Namespace sind nicht vorhanden.
- Sie können die Funktionalitäten eines Benutzers, einer Gruppe oder einer Rolle nicht ändern. Funktionalitäten werden durch die on Demand-Abonnementenebene des Benutzers bestimmt.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Personen** > **Konten**.
2. Klicken Sie auf den **Cognos**-Namespace, um diesen zu öffnen.
3. Klicken Sie auf das Symbol zum Erstellen neuer Gruppen oder auf das Symbol zum Erstellen neuer Rollen, geben Sie einen eindeutigen Namen im entsprechenden Bereich ein und drücken Sie die Eingabetaste. Die Gruppe oder Rolle wird zur Liste mit Einträgen im Cognos-Namespace hinzugefügt.

   Tipp: Sie können Gruppen und Rollen auch in Ordnern erstellen. Klicken Sie auf das für neuen Ordner, um einen neuen Ordner zu erstellen.
4. Fügen Sie wie folgt einzelne Mitglieder zu der neuen Gruppe oder Rolle hinzu:
   a) Suchen Sie die neue Gruppe oder Rolle im Cognos-Namespace. So finden Sie ihn schnell:
      - Geben Sie Text in das Feld **Suchen** ein.

        Anmerkung: Sie können auf das Symbol 'Suchmethode' klicken, um nach Einträgen zu suchen, die mit dem eingegebenen Text vollständig oder teilweise übereinstimmen oder genauso beginnen.
      - Klicken Sie auf das Symbol 'Typ , um die Sicht der Einträge einzugrenzen.

   b) Klicken Sie im Menü 'Mehr' der Gruppe oder Rolle auf **Mitglieder anzeigen** und klicken Sie auf **Auswählen**.
   c) Klicken Sie im Fenster **Mitglieder hinzufügen** auf den erforderlichen Namespace und suchen Sie nach dem Benutzer, der Gruppe oder der Rolle, den/die Sie hinzufügen möchten. Sie können Mitglieder von einem beliebigen Namespace oder mehreren Namespaces hinzufügen, bei dem/denen Sie angemeldet sind. Verwenden Sie bei Bedarf die Such- und Filterfunktionen, um den Benutzer, die Gruppe oder die Rolle zu finden, den/die Sie hinzufügen möchten.
   d) Wählen Sie die erforderlichen Benutzer, Gruppen oder Rollen aus. Sie können mehrere Einträge auswählen. Klicken Sie auf **OK**. Die ausgewählten Einträge werden auf der Registerkarte **Mitglieder** angezeigt.
5. Führen Sie die folgenden Schritte aus, um viele Mitglieder gleichzeitig auf die Registerkarte 'Mitglieder' zu importieren:
   a) Klicken Sie auf **Importieren**.
   b) Geben Sie im Fenster **Massenimport von Benutzern** einen oder mehrere Mitgliedsnamen ein, die jeweils durch Semikolon (;) getrennt sind.

      Verwenden Sie das Format *Namespace*/[*Konto* | *Gruppe* | *Rolle*]

Tipp: Zur Angabe des *Kontos* geben Sie den in der Spalte **Name** angezeigten Vornamen des Benutzers ein, nachdem Sie **Personen** > **Konten** > ***Name des Namespace*** ausgewählt haben.

c) Klicken Sie auf **Importieren**.

d) Klicken Sie auf **Fertig**.

6. Um ein Mitglied zu entfernen, zeigen Sie mit dem Cursor auf seinen Namen und klicken Sie das auf das Symbol 'Entfernen' .

   Die Gruppe oder Rolle schließt jetzt Mitglieder ein. Sie kann auch zu einer anderen Gruppe oder Rolle hinzugefügt werden.

Nächste Schritte

Das Menü 'Mehr' der Gruppe oder Rolle enthält Optionen zum Verwalten dieser Einträge. Unter **Eigenschaften** können Sie auf der Registerkarte **Berechtigungen** Zugriffsberechtigungen für die Gruppen und Rollen festlegen. Mit der Option **Mitglieder anzeigen** können Sie Mitglieder zu einer Gruppe oder Rolle hinzufügen oder von dieser entfernen. Mit der Option **Hinzufügen zu** können Sie den Eintrag zu einer anderen Gruppe oder Rolle oder auch zu einem Ordner hinzufügen. Mit der Option **Kopieren oder verschieben** können Sie den Eintrag an eine andere Position im Namenspace kopieren oder verschieben. Verwenden Sie zum Löschen der Gruppe oder Rolle die Option **Löschen**.

Erstellen und Verwalten von Benutzern

Sie können Benutzer im Namespace **Cognos-Benutzer** erstellen, wenn die Option **Easy Install** bei der Installation von IBM Cognos Analytics verwendet wurde.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Personen** > **Konten**.
2. Klicken Sie auf den Namespace **Cognos-Benutzer**, um diesen zu öffnen.
3. Klicken Sie auf das Symbol zum Erstellen neuer Benutzer und geben Sie im Dialogfeld **Neuer Benutzer** die erforderlichen Informationen einschließlich Benutzer-ID und Kennwort ein. Klicken Sie auf **OK**.

   Der Benutzername wird zur Liste mit Einträgen im Namespace **Cognos-Benutzer** hinzugefügt. Sie können den Benutzer jetzt zu einem Ordner, einer Gruppe oder einer Rolle hinzufügen. Der Benutzer kann sich mit der Benutzer-ID und dem Kennwort bei IBM Cognos Analytics anmelden, die Sie ihm zugewiesen haben.

Nächste Schritte

Das Menü 'Mehr' eines Benutzers stellt Optionen zum Verwalten des Benutzereintrags bereit. Unter **Eigenschaften** können Sie auf der Registerkarte **Allgemein** im Eigenschaftenbereich **Erweitert** das Benutzerkennwort ändern. Unter **Eigenschaften** können Sie außerdem auf der Registerkarte **Berechtigungen** Zugriffsberechtigungen für den Benutzer festlegen. Mit der Option **Hinzufügen zu** können Sie den Benutzer zu einer Gruppe, einer Rolle oder einem Ordner hinzufügen. Verwenden Sie zum Löschen des Benutzers die Option **Löschen**.

Anpassen von Rollen

Wenn Sie die Rollen verwenden, die im Cognos-Namespace vordefiniert sind, können Sie Motive, Startseiten und Berichtsparameter anpassen, die für die einzelnen Cognos-Rollen spezifisch sind.

Anmerkung: Nur Cognos-Rollen können angepasst werden. Sie können eine Rolle nur dann anpassen, wenn sie zum Cognos-Namespace gehört - entweder als vordefinierte Cognos-Rolle oder als Rolle, die Sie selbst erstellt haben. Weitere Informationen zu Cognos-Rollen finden Sie in der Veröffentlichung *IBM Cognos AnalyticsVerwaltung und Sicherheit*.

Sie können angeben, dass eine benutzerdefinierte Startseite, ein bestimmter Bericht oder ein bestimmtes Dashboard angezeigt wird, wenn ein Benutzer mit einer bestimmten Cognos-Rolle IBM Cognos Analytics öffnet. Sie können Standardbenutzerschnittstellenfeatures für Rollen entfernen. Darüber hinaus können Sie Parameter, die in allen Berichten verwendet werden können, an jede Benutzerrolle anpassen.

Vor dem Festlegen von benutzerdefinierten Motiven und Startseiten (außer Dashboards oder Berichten) müssen Sie die benutzerdefinierten Motive bzw. Startseiten erstellen und hochladen. Weitere Informationen finden Sie unter Kapitel 9, „Anpassen von Cognos Analytics für alle Rollen", auf Seite 201.

Klicken Sie zum Anpassen einzelner Rollen unter **Verwalten** > **Personen** > **Konten** auf einen Namespace, um die Liste von Rollen für den Namespace anzuzeigen. Wenn Sie auf das Menü 'Mehr'  einer Rolle klicken und **Eigenschaften** auswählen, hat das Slideout-Fenster für diese Rolle eine Registerkarte **Anpassung**.

Anmerkung: Wenn Sie Anpassungen für alle Rollen festlegen möchten, verwenden Sie das Slideout-Fenster **Verwalten** > **Anpassung**. Weitere Informationen finden Sie unter „Anwenden von Motiven, Erweiterungen und Ansichten" auf Seite 227.

Festlegen einer Standardstartseite

Klicken Sie neben der Standardstartseite auf >. Nun können Sie nach einem Dashboard oder Bericht suchen, das bzw. der als Standardstartseite verwendet werden soll, oder Sie können eine Ansicht in der Liste der Ansichten auswählen, die als Standardstartseite für alle Benutzer in dieser Rolle verwendet werden soll.

Entfernen oder Einschließen von Features

Sie können Benutzerschnittstellenfeatures auswählen, die für Benutzer in einer bestimmten Rolle entfernt oder eingeschlossen werden sollen. Klicken Sie neben **Features** auf >. Eine Liste mit Ansichten wird angezeigt. Diese Liste enthält sowohl die integrierten Ansichten als auch alle benutzerdefinierten Ansichten, die hochgeladen wurden. Klicken Sie auf eine Ansicht, um eine allgemeine Gruppierung der Features für die Ansicht anzuzeigen. Klicken Sie neben einer Gruppierung auf >, um die Features einer unteren Ebene einzublenden. Sie können beliebige Features in dieser Liste abwählen oder auswählen oder für Ihre Auswahl zu den darunter liegenden Ebenen navigieren. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Mit **Auf Standardwerte zurücksetzen** können Sie die Änderungen zurücksetzen.

Zur Anpassung des Navigationsmenüs in der Berichterstellung erweitern Sie **Berichterstellung** > **Sammlungen** > **Bericht**.

Festlegen eines Standardmotivs

Klicken Sie neben einem Standardmotiv auf >. Sie können ein Motiv in der Liste der Motive auswählen, das als Standardmotiv für alle Benutzer in dieser Rolle verwendet werden soll.

Erstellen eines benutzerdefinierten Ordners

Klicken Sie neben **Benutzerdefinierter Ordner** auf >, um einen benutzerdefinierten Inhaltsordner für Benutzer mit dieser Rolle anzugeben. Wenn sich ein Benutzer mit dieser Rolle anmeldet, wird der benutzerdefinierte Ordner in der Navigationsleiste unter **Teaminhalt** angezeigt.

Festlegen der Standardposition für hochgeladene Dateien

11.1.5

Klicken Sie auf > neben **Standardposition für Upload**, um einen Ordner in **Teaminhalt** als Standardposition für hochgeladene Dateien für Benutzer mit dieser Rolle anzugeben.

Standardparameter für Rollen festlegen

Klicken Sie neben **Parameter** auf **Einstellungen**. Es wird eine Liste von Parametern, die Sie angepasst haben, angezeigt. Wählen Sie die Parameter aus, die Sie für die Rolle konfigurieren möchten. Wählen Sie dann die Standardwerte aus, die für alle Benutzer in dieser Rolle angezeigt werden sollen. Klicken Sie auf **Anwenden** und dann auf **OK**, wenn Sie fertig sind.

Weitere Informationen finden Sie unter "Benutzerdefinierte Parameter verwenden" in der Veröffentlichung *IBM Cognos Analytics Reporting - Benutzerhandbuch*.

Lösen von Konflikten bei Benutzern mit mehreren Rollen

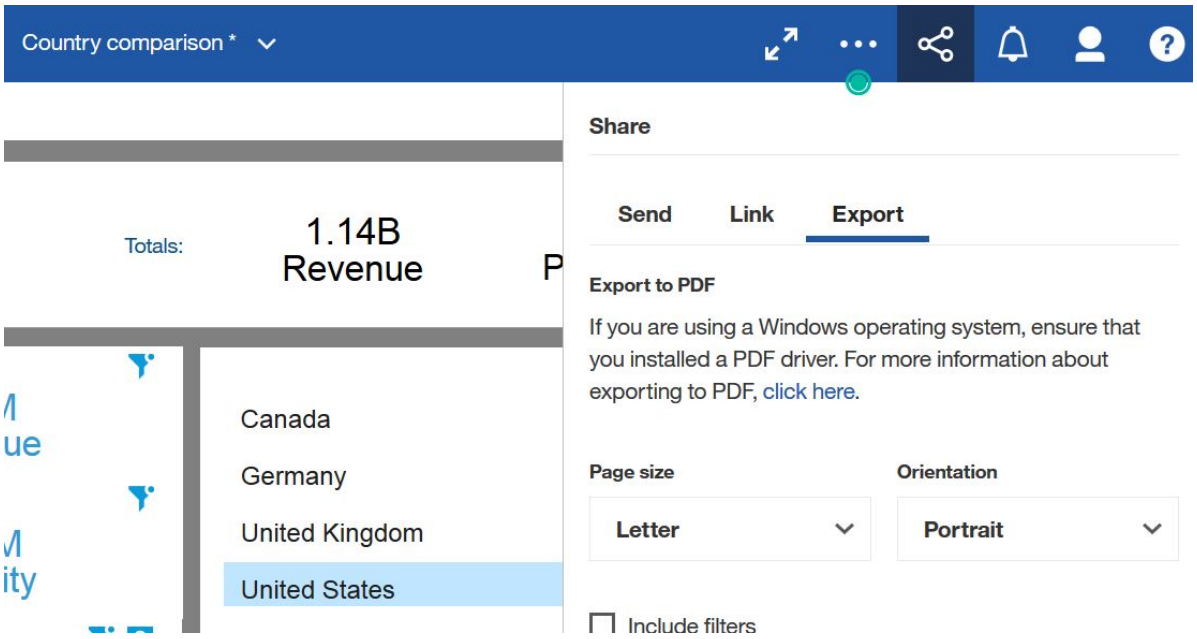
Einem Benutzer können mehrere Rollen zugewiesen sein, die unterschiedliche Standardmotive oder Standardstartseiten umfassen. Zur Lösung dieses Problems klicken Sie beim Festlegen von Anpassungen für eine Rolle auf **Erweitert** und legen Sie eine Priorität von 0 bis 10 für die Rolle fest. Im Falle eines Konflikts werden die Anpassungen für die Rolle mit der höchsten Priorität verwendet. Der Rolle **Systemadministrator** ist eine fest codierte Priorität von 1000 zugeordnet.

Beispiel 1: Entfernen des Features 'In PDF Exportieren' aus der Rolle 'Analysebenutzer'

In diesem Beispiel entfernt der Administrator die Option **In PDF exportieren** in der Anwendungsleiste von Analysis-Benutzern, die Dashboardinhalte gemeinsam nutzen wollen.

Vorgehensweise

1. Prüfen Sie das Standardverhalten.
   a) Melden Sie sich als Analysis-Benutzer an und öffnen Sie ein Dashboard.
   b) Klicken Sie auf die Schaltfläche 'Teilen' in der Anwendungsleiste.
      Das Fenster **Teilen** wird geöffnet.
   c) Klicken Sie auf die Registerkarte **Exportieren**.
      Die Optionen für die Funktion **In PDF exportieren** werden angezeigt, wie im folgenden Diagramm dargestellt.



2. Entfernen Sie das Feature 'In PDF exportieren' für Analysis-Benutzer.
   a) Melden Sie sich als Administrator an.

b) Wechseln Sie zu **Verwalten** > **Personen** > **Konten** und klicken Sie auf den Namespace **Cognos**.

c) Klicken Sie auf die Schaltfläche 'Mehr' neben der Rolle **Analysis-Benutzer**.

d) Klicken Sie auf **Eigenschaften**.

e) Klicken Sie auf die Registerkarte **Anpassung**.

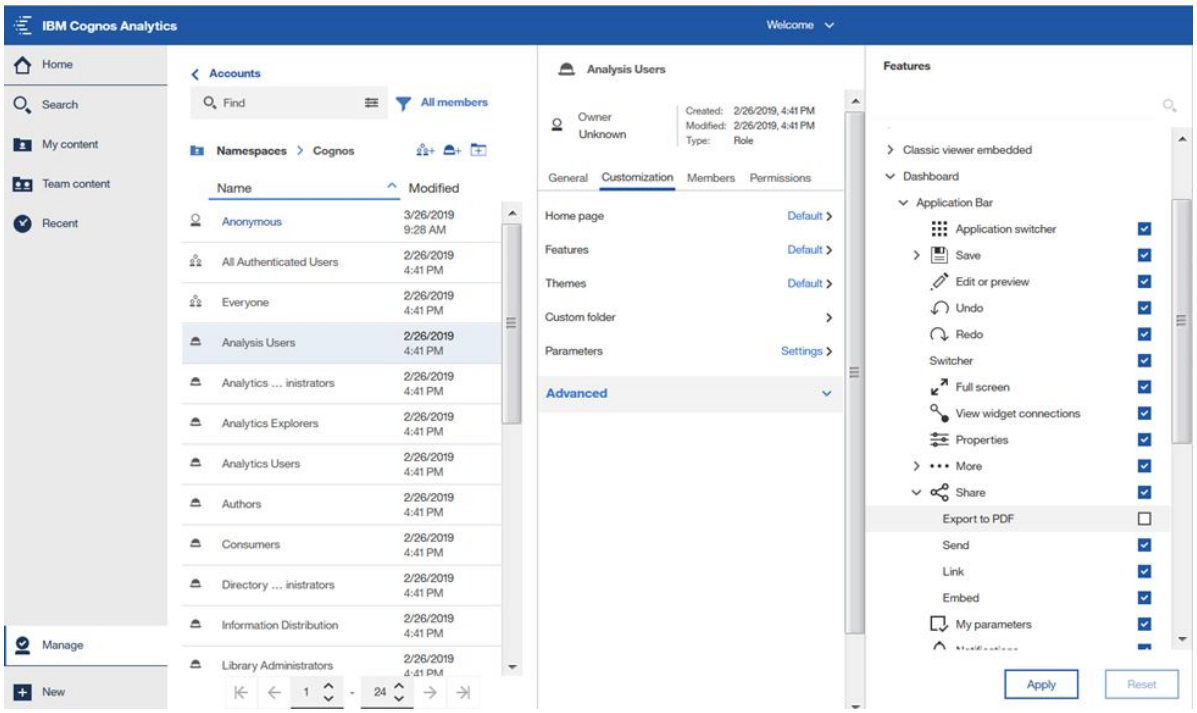
f) Klicken Sie auf die Winkelschaltfläche hinter **Features**.

g) Klicken Sie auf die Winkelschaltfläche vor **Dashboard**, um die Liste zu erweitern.

h) Klicken Sie auf die Winkelschaltfläche vor **Anwendungsleiste**, um die Liste zu erweitern.

i) Klicken Sie auf die Winkelschaltfläche vor **Teilen**, um die Liste zu erweitern.

j) Wählen Sie das Kontrollkästchen **In PDF exportieren** ab.
Das Cognos Analytics-Fenster sieht dann wie folgt aus:

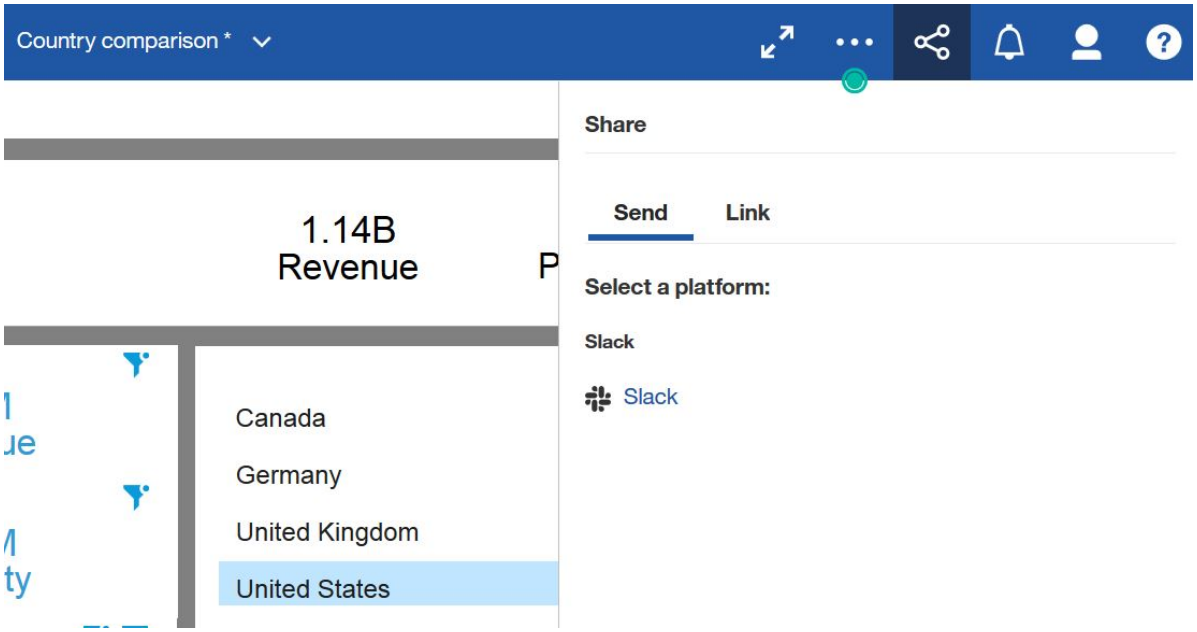


k) Klicken Sie auf **Anwenden**.

3. Vergewissern Sie sich, dass das Feature entfernt wurde.

a) Melden Sie sich als Analysis-Benutzer an und öffnen Sie dasselbe Dashboard.

b) Klicken Sie auf die Schaltfläche 'Teilen' in der Anwendungsleiste.
Das Fenster **Teilen** wird ohne die Registerkarte **Exportieren** geöffnet, wie im folgenden Diagramm dargestellt.



Ergebnisse

Das Feature, das Sie ausgewählt haben, wurde für die Rolle, die Sie angegeben haben, entfernt.

Anmerkung: Betroffene Benutzer müssen sich ab- und wieder anmelden, bevor die Änderung in ihrer Ansicht des Produkts wiedergegeben wird.

Beispiel 2: Einschränken der Anzeige der On-Demand-Symbolleiste für Benutzer

Administratoren können die bedarfsgesteuerte Symbolleiste für ausgewählte Benutzer, Gruppen oder Rollen inaktivieren.

Informationen zu diesem Vorgang

Informationen zum Ausblenden der bedarfsgesteuerten Symbolleiste für einen bestimmten Bericht, unabhängig davon, welcher Benutzer diesen anzeigt, finden Sie im Abschnitt "Inaktivieren der bedarfsgesteuerten Symbolleiste" in der Veröffentlichung *IBM Cognos Analytics Reporting - Benutzerhandbuch*.

Wichtig: Wenn die bedarfsgesteuerte Symbolleiste inaktiviert wird, sind bestimmte Aspekte bestimmter Berichte in HTML-Ansichten nicht mehr verfügbar. Wenn beispielsweise für einen Bericht ursprünglich sowohl die Drillthrough-Funktion als auch die Drilldown-Funktion aktiviert ist, dann ist *nur noch* die Drillthrough-Funktion für die den Bericht anzeigenden Benutzer verfügbar, deren bedarfsgesteuerte Symbolleiste durch eine der folgenden Prozeduren inaktiviert worden ist:

- die folgende Verwaltungsprozedur.
- die Prozedur zum Inaktivieren der Symbolleiste für einen bestimmten Bericht.

Vorgehensweise

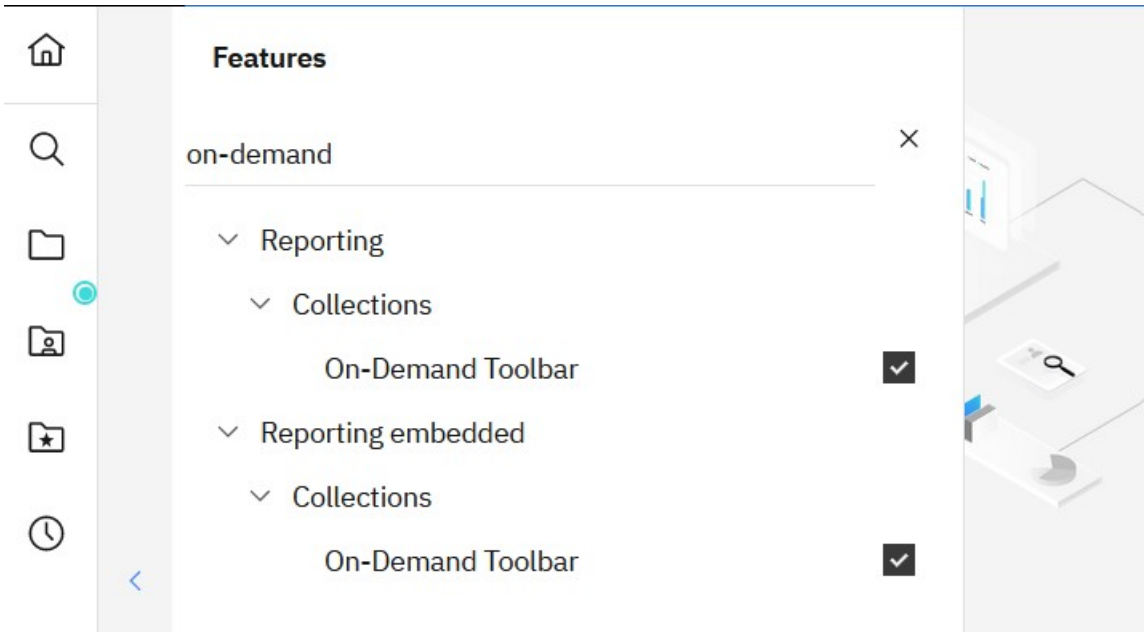
1. Melden Sie sich als Administrator an.
2. Wechseln Sie zu **Verwalten** > **Personen** > **Konten** und klicken Sie auf den Namespace **Cognos**.
3. Klicken Sie auf die Schaltfläche für 'Mehr' ... neben der Rolle **Autoren**.
4. Klicken Sie auf **Eigenschaften**.
5. Klicken Sie auf die Registerkarte **Anpassung**.
6. Klicken Sie auf die Winkelschaltfläche > hinter **Features**.

Das Fenster **Features** wird angezeigt. Es ist jedoch nicht ersichtlich, wo in der Verzeichnisstruktur des Fensters 'Features' die bedarfsgerechte Symbolleiste zu finden ist.

Tipp: Mithilfe des Suchfelds können Sie das Feature ausfindig machen, das Sie aktivieren bzw. inaktivieren wollen.

7. Geben Sie in das Suchfeld den Suchbegriff `bedarfsgesteuert` ein.

   Die Suchergebnisse zeigen, dass Sie die Darstellung der bedarfsgesteuerten Symbolleiste in Berichten und/oder Dashboards steuern können.



8. Wählen Sie das Kontrollkästchen neben **Berichterstellung** > **Sammlungen** > **Bedarfsgesteuerte Symbolleiste** ab.
9. Klicken Sie auf **Anwenden**.

Ergebnisse

Die bedarfsgesteuerte Symbolleiste wird für Reporting-Benutzer, die zur Rolle 'Autoren' gehören, nicht angezeigt.

Anmerkung: Betroffene Benutzer müssen sich ab- und wieder anmelden, bevor die Änderung in ihrer Ansicht des Produkts wiedergegeben wird.

Beispiel 3: Inaktivieren einer Modellierungsfunktion für eine Rolle

Sie können festlegen, dass bestimmte Modellierungsfunktionen für ausgewählte Rollen nicht verfügbar sind.

Informationen zu allen Cognos Analytics-Modellierungsfunktionen finden Sie unter "Datenmodellierung in Cognos Analytics" im Handbuch *IBM Cognos Analytics -Datenmodellierung*.

Im folgenden Beispiel möchten Sie nicht, dass Modellierer neu hochgeladene Dateien verwenden, die sich auf ihren lokalen Computern befinden. Sie können verhindern, dass sie lokale Dateien in Cognos Analytics hochladen. Infolgedessen werden bei der Modellierung von hochgeladenen Dateien nur Dateien verwendet, die zuvor in Cognos Analytics hochgeladen wurden.

Vorgehensweise

1. Melden Sie sich als Administrator an.
2. Wechseln Sie zu **Verwalten** > **Personen** > **Konten** und klicken Sie auf den Namespace **Cognos**.

3. Klicken Sie auf die Schaltfläche 'Mehr'  neben der Rolle **Modellierer**.
4. Klicken Sie auf **Eigenschaften**.
5. Klicken Sie auf die Registerkarte **Anpassung**.
6. Klicken Sie auf die Winkelschaltfläche hinter **Features**.

   Das Fenster **Features** wird angezeigt.
7. Klicken Sie auf die Winkelschaltflächen für **Datenmodul** > **Navigationsleiste** > **Neu**.
8. Wählen Sie das Kontrollkästchen neben **Dateien hochladen** ab.
9. Klicken Sie auf **Anwenden**.

Ergebnisse

Die Option **Dateien hochladen** ist im Menü **Neu** für Benutzer, die zu der Rolle 'Modellierer' gehören, nicht mehr verfügbar.

Anmerkung: Betroffene Benutzer müssen sich ab- und wieder anmelden, bevor die Änderung in ihrer Ansicht des Produkts wiedergegeben wird.

Beispiel 4: Inaktivieren der Option 'Alle auf einmal ausführen'

Sie können verhindern, dass Benutzer einen Job erstellen, bei dem alle Berichte auf einmal ausgeführt werden.

Informationen zu Jobs finden Sie im Abschnitt zum "Erstellen eines Jobs zur Planung mehrerer Einträge" im Handbuch *IBM Cognos Analytics - Erste Schritte*.

Beispiel

In diesem Beispiel möchten Sie verhindern, dass Berichte in einem Job gleichzeitig ausgeführt werden, um die Leistung Ihres Servers zu verbessern. Sie entscheiden sich, die Option **Alle auf einmal ausführen** in Jobs zu inaktivieren, die von Personen mit der Rolle **Analytics-Explorer** erstellt wurden.

Vorgehensweise

1. Melden Sie sich als Administrator an.
2. Wechseln Sie zu **Verwalten** > **Personen** > **Konten** und klicken Sie auf den Namespace **Cognos**.
3. Klicken Sie auf die Schaltfläche 'Mehr'  neben der Rolle **Modellierer**.
4. Klicken Sie auf **Eigenschaften**.
5. Klicken Sie auf die Registerkarte **Anpassung**.
6. Klicken Sie auf die Winkelschaltfläche hinter **Features**.

   Das Fenster **Features** wird angezeigt.
7. Klicken Sie auf die Winkelschaltflächen für **Jobs** > **Objektgruppen**.
8. Wählen Sie das Kontrollkästchen neben **Alle auf einmal ausführen** ab.
9. Klicken Sie auf **Anwenden**.

Ergebnisse

Die Option **Alle auf einmal ausführen** ist nicht mehr in der Anzeige **Ausführungsoptionen** für Jobs verfügbar, die von Benutzern mit der Rolle **Analytics-Explorer** erstellt wurden.

Anmerkung: Betroffene Benutzer müssen sich ab- und wieder anmelden, bevor die Änderung in ihrer Ansicht des Produkts wiedergegeben wird.

Authentifizierungsprovider

Die Benutzerauthentifizierung in IBM Cognos Analytics wird mit Authentifizierungsprovidern verwaltet. Authentifizierungsprovider definieren Benutzer, Gruppen und Rollen für die Authentifizierung. Zu den in den Providern gespeicherten Informationen gehören unter anderem Benutzernamen, IDs, Kennwörter, regionale Einstellungen und persönliche Präferenzen.

In der Cognos Analytics-Benutzerschnittstelle werden Authentifizierungsprovider durch Namespaces dargestellt.

Cognos Analytics unterstützt die folgenden Typen von Authentifizierungsprovidern:

- Active Directory
- OpenID Connect
- Benutzerdefinierter Java-Provider
- OpenID Connect-Authentifizierungsproxy
- IBM Cognos Series 7
- LDAP
- SAP
- SiteMinder

Authentifizierungsprovider werden in IBM Cognos Configuration unter der Kategorie **Security** > **Authentication** konfiguriert. Nachdem der Provider-Namespace dort hinzugefügt und der **IBM Cognos**-Service erneut gestartet wurde, wird der Namespace-Name unter **Verwalten** > **Personen** > **Konten** angezeigt und Benutzer können sich mit diesem Namespace bei Cognos Analytics anmelden. Weitere Information zum Konfigurieren von Authentifizierungsprovidern finden Sie in der Veröffentlichung *IBM Cognos Analytics - Installation und Konfiguration*.

Sie können keine Benutzer, Gruppen oder Rollen in Namespaces von Authentifizierungsprovidern aus Cognos Analytics erstellen. Sie können jedoch Benutzer, Gruppen und Rollen von diesen Namespaces zu Gruppen und Rollen im **Cognos**-Namespace hinzufügen.

Mehrere Namespaces

Wenn mehrere Namespaces für Cognos Analytics konfiguriert sind, müssen Sie am Anfang einer Sitzung einen Namespace auswählen. Sie können sich jedoch auch noch zu einem späteren Zeitpunkt in der Sitzung bei anderen Namespaces anmelden. Beim Festlegen von Zugriffsberechtigungen möchten Sie beispielsweise eventuell Einträge aus verschiedenen Namespaces referenzieren. Um sich bei einem anderen Namespace anzumelden, müssen Sie sich nicht bei dem aktuell verwendeten Namespace abmelden. Sie können bei mehreren Namespaces gleichzeitig angemeldet sein.

Ihre primäre Anmeldung sind der Namespace und die Berechtigungsnachweise, die Sie am Anfang der Sitzung verwendet haben. Die Namespaces, bei denen sich sich zu einem späteren Zeitpunkt in der Sitzung anmelden, sowie die entsprechenden Berechtigungsnachweise sind Ihre sekundären Anmeldungen.

Wenn Sie einen der Namespaces löschen, können Sie sich mit einem anderen Namespace anmelden. Wenn Sie alle Namespaces mit Ausnahme desCognos-Namespace löschen, werden Sie nicht zur Anmeldung aufgefordert. Wenn der anonyme Zugriff aktiviert ist, werden Sie automatisch als anonymer Benutzer angemeldet. Ist der anonyme Zugriff nicht aktiviert, haben Sie keinen Zugriff auf die Anmeldeseite. Aktivieren Sie in diesem Fall den anonymen Zugriff über Cognos Configuration.

Verwalten von OpenID Connect-Namespaces

Verwenden Sie den Namespacetyp **OpenID Connect**, um die OpenID Connect-Authentifizierung für IBM Cognos Analytics zu implementieren.

Cognos Analytics unterstützt die folgenden OpenID Connect-Identitätsprovider:

- ADFS (Active Directory Federation Services)

- Azure AD (Active Directory)
- Generic
- Google
- IBM Cloud Identity
- IBMid (IBM Identitätsprovider)
- MS Identity
- OKTA
- Ping
- SalesForce
- SiteMinder

IBMid ist der IBM Identitätsservice, eine cloudbasierte ID-Zugriffs- und Managementlösung, die Identitäts- und Single Sign-on-Services für IBM Anwendungen bereitstellt.

Nach der Konfiguration des OpenID Connect-Namespace in IBM Cognos Configuration haben alle OpenID Connect-Benutzer Zugriff auf Cognos Analytics. Bei der Anmeldung werden die Namen der Benutzer automatisch im Namespace angezeigt.

Anmerkung: Zur erfolgreichen Einrichtung eines OpenID Connect-Namespace müssen Sie sicherstellen, dass der Content Manager-Computer auf den OIDC-Identitätsprovider (IDP) zugreifen kann. In einigen Fällen kann Content Manager keine Verbindung herstellen, wenn ein Proxy zwischen Content Manager und dem IDP vorhanden ist.

Als Systemadministrator müssen Sie möglicherweise basierend auf der Anzahl der Anzahl der Lizenzen oder anderen Faktoren die Anzahl der Benutzer beschränken, die auf das Produkt zugreifen können. Führen Sie dazu die folgenden optionalen Schritte durch:

- Fügen Sie eine begrenzte Anzahl von Benutzern zum **OpenID Connect**-Namespace hinzu.

  Siehe Schritt „3” auf Seite 15 unten.
- Fügen Sie Gruppen zum **OpenID Connect**-Namespace hinzu.

  Siehe Schritt „4” auf Seite 16 unten.
- Fügen Sie die **OpenID Connect**-Benutzer zu Gruppen oder Rollen im **Cognos**-Namespace hinzu.

  Durch die Verwendung der **Cognos**-Gruppen und Rollen können Sie schnell die erforderlichen Zugriffsberechtigungen für verschiedene Benutzer zuweisen.
- Legen Sie in IBM Cognos Configuration unter **Sicherheit** > **Authentifizierung** die Eigenschaft **Zugriff auf Mitglieder des integrierten Namespace begrenzen** auf 'wahr' fest.

  Nur Mitglieder des integrierten **Cognos**-Namespace haben jetzt Zugriff auf Cognos Analytics.

Vorgehensweise

1. Melden Sie sich bei IBM Cognos Analytics als Systemadministrator an.
2. Melden Sie sich beim **OpenID Connect**-Namespace an.
3. Gehen Sie wie folgt vor, um Benutzerkonten zum **OpenID Connect**-Namespace hinzuzufügen:
   a) Navigieren Sie zu **Verwalten** > **Personen** > **Konten** und öffnen Sie den Namespace **OpenID Connect**.
   b) Führen Sie die folgenden Schritte aus, um ein einzelnes Benutzerkonto hinzuzufügen:
      - Klicken Sie auf das Symbol 'Neuer Benutzer'  .

        Die Anzeige **Benutzer hinzufügen** wird angezeigt.
      - Geben Sie einen eindeutigen Namen im Feld **Eindeutige ID** ein.

        Geben Sie zum Beispiel die E-Mail-Adresse des Benutzers ein.

- Geben Sie im Feld **Bevorzugter Name** den Namen ein, der in der Namespace-Liste angezeigt werden soll.
- Klicken Sie auf **Hinzufügen**.

Der Wert für **Bevorzugter Name** wird in der Namespace-Liste angezeigt.

c) Um mehrere Benutzerkonten auf einmal hinzuzufügen, können Sie eine CSV-Datei importieren, die speziell mit Kontoinformationen formatiert ist:

- Stellen Sie sicher, dass Sie die CSV-Datei erstellt haben, die Ihre Benutzerinformationen enthält.

  Weitere Informationen finden Sie unter „Erstellen einer CSV-Datei mit Benutzerkontoinformationen" auf Seite 17.

- Klicken Sie auf das Symbol 'Importieren'  und wählen Sie **Benutzer importieren** aus.
- Doppelklicken Sie auf die CSV-Datei, die die Benutzerinformationen enthält.

  Die Datei wird hochgeladen und die `defaultName`-Werte aus der CSV-Datei werden im OpenId Connect-Namespace aufgelistet.

  Dieselbe CSV-Datei kann mehrfach importiert werden. Wenn ein `defaultName`-Wert bereits im Namespace vorhanden ist, wird das Benutzerkonto aktualisiert. Sie können den Importvorgang auch wiederholen, falls zuvor importierte Einträge falsch zu sein scheinen.

  Wenn Sie mehrere Dateien haben, wiederholen Sie diesen Schritt für die anderen Dateien.

4. Gehen Sie wie folgt vor, um Gruppen zum **OpenID Connect**-Namespace hinzuzufügen:

a) Navigieren Sie zu **Verwalten** > **Personen** > **Konten** und öffnen Sie den Namespace **OpenID Connect**.

b) Führen Sie die folgenden Schritte aus, um einzelne Gruppen hinzuzufügen:

- Klicken Sie auf das Symbol 'Neue Gruppe'  .
- Geben Sie den Namen der neuen Gruppe ein.

Der Gruppenname wird im Namespace aufgelistet.

c) Um mehrere Gruppen auf einmal hinzuzufügen, können Sie eine CSV-Datei importieren, die speziell mit Gruppeninformationen formatiert ist:

- Stellen Sie sicher, dass Sie die CSV-Datei erstellt haben, die Ihre Gruppeninformationen enthält.

  Weitere Informationen finden Sie unter „Erstellen einer CSV-Datei mit Gruppeninformationen" auf Seite 18.

- Klicken Sie auf das Symbol 'Importieren'  und wählen Sie **Gruppen importieren** aus.
- Doppelklicken Sie auf die CSV-Datei, die die Gruppeninformationen enthält.

  Die Datei wird hochgeladen und die `defaultName`-Werte aus der CSV-Datei werden im OpenId Connect-Namespace aufgelistet. Dieselbe CSV-Datei kann mehrfach importiert werden. Wenn eine Gruppe bereits im Namespace vorhanden ist, wird die Gruppe aktualisiert. Sie können den Importvorgang auch wiederholen, falls zuvor importierte Einträge falsch zu sein scheinen.

  Wenn Sie mehrere Dateien haben, wiederholen Sie diesen Schritt für die anderen Dateien.

5. Fügen Sie die **OpenID Connect**-Benutzer zu Gruppen oder Rollen im **Cognos**-Namespace hinzu.

a) Öffnen Sie den **Cognos**-Namespace und suchen Sie nach der Gruppe oder Rolle, der Sie Benutzer aus dem **OpenID Connect**-Namespace hinzufügen möchten.

b) Wählen Sie im Kontextmenü der Gruppe oder Rolle  die Option **Mitglieder anzeigen** aus.

c) Klicken Sie auf  **Auswählen**.

d) Wählen Sie das Fenster **Mitglieder hinzufügen**, wählen Sie Ihren **OpenID Connect**-Namespace und dann die entsprechenden Benutzer aus. Sie können mehrere Benutzer gleichzeitig auswählen.

e) Klicken Sie auf **Hinzufügen**. Die ausgewählten Mitglieder werden auf der Registerkarte **Mitglieder** angezeigt.

f) Wiederholen Sie die Schritte, um die **OpenID Connect**-Benutzer zu anderen **Cognos**-Gruppen oder -Rollen hinzuzufügen.

g) Um Benutzer aus einer CSV-Datei zu importieren, klicken Sie auf **Importieren** und wählen Sie die entsprechende Datei aus. Weitere Informationen finden Sie unter „Erstellen einer CSV-Datei mit Benutzerkontoinformationen" auf Seite 17.

Dieselbe CSV-Datei kann mehrfach importiert werden. Wenn ein Benutzerkonto bereits im Namespace vorhanden ist, wird das Konto aktiviert. Sie können den Importvorgang auch wiederholen, falls zuvor importierte Einträge falsch zu sein scheinen.

Wenn Sie mehrere Dateien haben, wiederholen Sie diesen Schritt für die anderen Dateien.

6. Zum Löschen eines Eintrags klicken Sie im Kontextmenü  neben der betreffenden Gruppe, Rolle oder dem betreffenden Ordner auf **Löschen**.

Ergebnisse

Benutzer, die den **OpenID Connect**-Namespace für die Anmeldung bei Cognos Analytics verwenden, werden an eine externe Anmeldeseite weitergeleitet, auf der sie ihre Berechtigungsnachweise eingeben können. Wenn die Berechtigungsnachweise akzeptiert werden, können die Benutzer auf Cognos Analytics zugreifen.

Erstellen einer CSV-Datei mit Benutzerkontoinformationen

Die CSV-Datei, die die Liste der Benutzer enthält, die in den OpenID Connect-Namespace importiert werden sollen, muss ordnungsgemäß formatiert sein, damit der Import erfolgreich durchgeführt werden kann.

Die CSV-Datei muss folgende Formate verwenden:

- UTF-8-Zeichencodierung
- Windows CRLF für Zeilenumbrüche

Die erste Zeile in dieser Datei ist der Header. Diese Zeile muss die Spalte `email` enthalten und kann die folgenden optionalen Spalten aufweisen: `defaultName`, `businessPhone`, `faxPhone`, `givenName`, `homePhone`, `mobilePhone`, `pagerPhone`, `postalAddress`, `surname`, `userName`.

Tipp: Alle Spaltennamen sind Eigenschaften der Kontoklasse ('account') in IBM Cognos Analytics. Bei den Namen muss die Groß-/Kleinschreibung beachtet werden und sie müssen genau wie in diesem Dokument angegeben eingegeben werden.

Alle anderen Zeilen in der Datei enthalten Werte, die den in der ersten Zeile angegebenen Werten entsprechen.

Nachfolgend finden Sie ein Beispiel einer CSV-Datei mit zwei Benutzern:

- Zeile 1: `email,defaultName,givenName,surname`
- Zeile 2: `Andy.Bergin@ca.ibm.com,Andy Bergin,Andy,Bergin`
- Zeile 3: `Kirsten.Vaughan@ca.ibm.com,Kirsten Vaughan,Kirsten,Vaughan`

Sie können alle Ihre Benutzer in eine CSV-Datei einfügen oder mehrere Dateien mit weniger Namen in jeder Datei erstellen.

Nachdem die Datei importiert wurde, wird der Wert für `defaultName` für den Benutzer folgendermaßen festgelegt:

- Wenn `defaultName` in der CSV-Datei angegeben ist, wird der Name verwendet.
- Wenn `defaultName` nicht in der CSV-Datei angegeben ist, jedoch `givenName` und `surname` angegeben sind, wird der Standardname als `givenName surname` festgelegt.

- Wenn weder `defaultName` noch `givenName` oder `surname` angegeben ist, wird der Wert für `email` als Standardname verwendet.

Mehrere Benutzer können den gleichen Vor- und Nachnamen haben. Um potenzielle Konflikte zu vermeiden, legen Sie entweder einen anderen Wert für `defaultName` für die Benutzer fest oder geben Sie nicht `surname` und `givenName` für sie an. Sie können auch den Wert für `surname` ändern, indem Sie dem Nachnamen ein eindeutiges Zeichen oder eine eindeutige Zahl hinzufügen, wie `Simpson1` oder `Simpson2`.

Anmerkung: Eigenschaften werden automatisch vom Namespaceprovider aktualisiert, wenn sich der Benutzer anmeldet. Wenn der Namespace Eigenschaften wie 'timeZone' und 'localePreference' unterstützt, werden sie daher im Konto-Proxy gespeichert, wenn sich der Benutzer anmeldet.

Erstellen einer CSV-Datei mit Gruppeninformationen

Eine CSV-Gruppendatei enthält die Liste der Gruppen, die in den OpenID Connect-Namespace importiert werden sollen. Diese Datei muss ordnungsgemäß formatiert sein, damit der Import erfolgreich ausgeführt werden kann.

Die CSV-Datei muss folgende Formate verwenden:

- UTF-8-Zeichencodierung
- Windows CRLF für Zeilenumbrüche

Die erste Zeile in der CSV-Gruppendatei ist der Header. Diese Zeile muss sowohl die Spalte `type` als auch die Spalte `defaultName` enthalten. Die Headerzeile kann auch die folgende optionale Spalte enthalten: `tenantID`.

Tipp: Alle Spaltennamen sind Eigenschaften der Gruppenklasse in IBM Cognos Analytics. Bei den Namen muss die Groß-/Kleinschreibung beachtet werden und sie müssen genau wie in diesem Dokument angegeben eingegeben werden.

Alle anderen Zeilen in der Datei enthalten Werte, die den in der ersten Zeile angegebenen Werten entsprechen.

Nachfolgend finden Sie ein Beispiel einer CSV-Datei mit zwei Gruppen:

- Zeile 1: `type,defaultName`
- Zeile 2: `group,Reviewers`
- Zeile 3: `group,Data-Scientists`

Sie können alle Ihre Gruppen in eine CSV-Datei einfügen oder mehrere Dateien mit weniger Gruppen in jeder Datei erstellen.

Suchen von Benutzern, Gruppen und Rollen

Als Administrator müssen Sie häufig die Benutzer, Gruppen und Rollen lokalisieren, die Sie verwalten.

In der Ansicht **Namespaces** unter **Verwalten** > **Personen** > **Konten** finden Sie alle Namespaces, die für die Verwendung mit IBM Cognos Analytics konfiguriert sind, den **Cognos**-Namespace und ggf. den **Cognos-Benutzer**-Namespace. Sie können nur in den Namespaces, bei denen Sie angemeldet sind, und in den Namespaces **Cognos** und **Cognos-Benutzer** navigieren.

Suchen von Einträgen

Ein Namespace enthält möglicherweise tausende Benutzer und zahlreiche Gruppen, Rollen und Ordner. Sie können diese Einträge nur finden, indem Sie die Suchfunktion unter **Konten** verwenden. Sie können immer nur in einem Namespace nach Einträgen suchen. Sie müssen also zunächst den Namespace auswählen und dann Text in das Feld **Suchen** eingeben.

Sie können auf das Symbol 'Suchmethode' klicken, um nach Einträgen zu suchen, die mit dem eingegebenen Text vollständig oder teilweise übereinstimmen oder genauso beginnen. Die Suche wird

ebenfalls verwendet, wenn Sie Gruppen- und Rollenmitglieder hinzufügen, Zugriffsberechtigungen angeben usw.

Filtern von Einträgen

Sie können Benutzer, Gruppen und Rollen filtern, um die angezeigten Einträge einzugrenzen. Geben Sie bei Verwendung im Rahmen der Suche für schnellere Antworten die Filterkriterien an. Klicken Sie auf das Filtersymbol  und wählen Sie die Filteroptionen aus oder ab.

Sortieren von Einträgen

Klicken Sie auf das Symbol 'Sortieren'  . Anschließend können Sie angeben, dass Suchergebnisse nach Name, nach Änderungsdatum oder nach Typ sortiert werden sollen. Sie können auch auswählen, ob die Ergebnisse in aufsteigender oder absteigender Reihenfolge angezeigt werden sollen.

Tipp: Wenn Suchergebnisse angezeigt werden, können Sie die Optionen für Suchmethode, Filterung und Sortierung ändern. Die Ergebnisse werden nach jeder Änderung dynamisch aktualisiert.

Blättern

Wenn Ihre Namespaces viele Einträge enthalten und Sie aktiviert haben, dass Kontoeinträge seitenweise geladen werden, können Sie schneller zwischen Seiten navigieren, um die gewünschten Einträge zu finden.

Erstellen von Kontakten, Verteilerlisten und Ordnern

Erstellen Sie Kontakte und Verteilerlisten für Personen, die Empfänger sein können, wenn Berichte per E-Mail zugestellt werden.

Verwenden Sie Verteilerlisten, wenn Sie einen Bericht gleichzeitig an mehrere Empfänger senden möchten. Verteilerlisten enthalten eine Kombination aus Benutzern, Gruppen, Rollen, Kontakten oder anderen Verteilerlisten.

Wenn ein Empfänger nicht Teil des IBM Cognos-Sicherheitssystems ist, können Sie einen Kontakt für diese Person erstellen. Die Kontakte, die Sie erstellen, können auch als Kontakte für Berichte zugeordnet werden. Sie können Ordner erstellen, um Ihre Einträge auf logische Weise zu organisieren.

Beachten Sie: Wenn Sie den E-Mail-Empfänger aus einer Liste auswählen, z. B. eine Gruppe, Rolle oder Verteilerliste, müssen Sie über Lesezugriff auf die Liste und das E-Mail-Konto des Empfängers verfügen. Andernfalls schlägt die Berichtszustellung fehl.

Erstellen von Kontakten

Wenn ein Empfänger nicht Teil des IBM® Cognos®-Sicherheitssystems ist, können Sie einen Kontakt für diese Person erstellen.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Personen** > **Kontakte**.
2. Klicken Sie auf das Symbol 'Neu'  und klicken Sie dann auf **Kontakt**  .
3. Geben Sie den Namen und die E-Mail-Adresse der Person ein.
4. Klicken Sie auf **Erstellen**.

   Der Kontaktname wird im Fenster **Kontakte** angezeigt.

Nächste Schritte

Wie bei einem Benutzernamen im Namespace **Cognos-Benutzer** können Sie auf das Symbol 'Mehr' eines Kontakts klicken, auf **Eigenschaften** klicken und bekommen dann diese Optionen angezeigt:

- Auf der Registerkarte **Allgemein** unter **Erweitert** können Sie den Kontakt inaktivieren oder ausblenden.
- Auf der Registerkarte **Vorgaben** können Sie das Standardformat des Kontakts, die Zeitzone und die Sprache des Cognos Analytics-Inhalts angeben.
- Auf der Registerkarte **Berechtigungen** können Sie Zugriffsberechtigungen für den Kontakt festlegen. Weitere Informationen finden Sie unter „Zugriff auf Funktionen festlegen” auf Seite 179.

Sie können den Kontakt auch zu einer Verteilerliste hinzufügen.

Erstellen von Verteilerlisten

Verwenden Sie Verteilerlisten, wenn Sie einen Bericht gleichzeitig an mehrere Empfänger senden möchten.

Verteilerlisten können eine Kombination aus Benutzern, Gruppen, Rollen, Kontakten oder anderen Verteilerlisten enthalten.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Personen** > **Kontakte**.
2. Klicken Sie auf das Symbol 'Neu' und klicken Sie dann auf **Verteilerliste**.
3. Geben Sie einen Namen für die Verteilerliste ein.
4. Klicken Sie auf **Erstellen**.

   Der Name der Verteilerliste wird im Fenster **Kontakte** angezeigt.
5. Führen Sie die folgenden Schritte aus, um Benutzer, Gruppen, Rollen, Kontakte oder andere Verteilerlisten zu der Verteilerliste hinzuzufügen:
   a) Klicken Sie auf den Namen der Verteilerliste.
   b) Klicken Sie auf die Registerkarte **Mitglieder**.
   c) Klicken Sie auf das Symbol 'Hinzufügen'.
   d) Suchen Sie nach dem Eintrag im Namespace **Cognos** oder **Cognos-Benutzer**. So finden Sie ihn schnell:
      - Geben Sie Text in das Feld **Suchen** ein.

        Anmerkung: Sie können auf das Symbol 'Suchmethode' klicken, um nach Einträgen zu suchen, die mit dem eingegebenen Text vollständig oder teilweise übereinstimmen oder genauso beginnen.
      - Klicken Sie auf das Filtersymbol, um die angezeigten Einträge einzugrenzen.
      - Klicken Sie auf das Symbol 'Sortieren'. Anschließend können Sie angeben, dass Suchergebnisse nach Name, nach Änderungsdatum oder nach Typ sortiert werden sollen. Sie können auch auswählen, ob die Ergebnisse in aufsteigender oder absteigender Reihenfolge angezeigt werden sollen.

      Tipp: Wenn Suchergebnisse angezeigt werden, können Sie die Optionen für Suchmethode, Filterung und Sortierung ändern. Die Ergebnisse werden nach jeder Änderung dynamisch aktualisiert.
   e) Wählen Sie die Einträge aus. Sie können mehrere Einträge auswählen.

      Tipp: Sie können Mitglieder von einem beliebigen Namespace oder mehreren Namespaces hinzufügen, bei dem/denen Sie angemeldet sind.
   f) Klicken Sie auf **Hinzufügen**.

Die ausgewählten Einträge werden auf der Registerkarte **Mitglieder** angezeigt.

g) Um ein Mitglied zu entfernen, zeigen Sie mit dem Cursor auf seinen Namen und klicken Sie das auf das Symbol 'Entfernen'  .

Nächste Schritte

Wenn Sie auf das Menü 'Mehr'  eines Kontakts geklickt haben, und dann auf **Eigenschaften** klicken, haben Sie die folgenden Optionen:

- Auf der Registerkarte **Allgemein** unter **Erweitert** können Sie die Verteilerliste ein- oder ausblenden.
- Auf der Registerkarte **Mitglieder** können Sie die Liste von Mitgliedern bearbeiten.
- Auf der Registerkarte **Berechtigungen** können Sie Zugriffsberechtigungen für die Verteilerliste festlegen. Weitere Informationen finden Sie unter „Zugriff auf Funktionen festlegen” auf Seite 179.

Kapitel 2. Verwalten von Inhalten

Am häufigsten wird eine Sicherung und Wiederherstellung von Inhalt durchgeführt, weil Inhalt innerhalb des Anwendungsentwicklungsprozesses von einer Testumgebung in eine Produktionsumgebung verschoben werden soll oder weil ein Upgrade auf eine neue Produktversion vorbereitet wird.

Zum Verwalten von Inhalten ist die Administrationsberechtigung **System konfigurieren und verwalten** erforderlich.

Bereitstellungsplanung

Der Prozess des Sicherns und Wiederherstellens von Inhalt wird als Bereitstellung bezeichnet. In der Quellenumgebung und in der Zielumgebung müssen dieselben Namespaces für Richtlinien, Benutzer, Rollen und Gruppen verwendet werden, damit Zugriffsberechtigungseinstellungen beim Bereitstellen von Inhalt einwandfrei funktionieren. Der Cognos-Namespace wird beim Erstellen einer Sicherung eingeschlossen. Stellen Sie sicher, dass die übrigen erforderlichen Namespaces vor dem Wiederherstellen des Inhalts in der Zielumgebung konfiguriert sind.

Falls die Bereitstellung im Rahmen eines Upgrades erfolgt, können Sie vor dem Erstellen einer Sicherung eine Konsistenzüberprüfung durchführen, um Inkonsistenzen innerhalb des Content Stores oder zwischen dem Content Store und externen Namespaces zu finden und zu korrigieren. Eine Konsistenzüberprüfung können Sie über die Option **Administrationskonsole** > **Konfiguration** > **Inhaltsadministration** > **Neue Konsistenzüberprüfung** ausführen.

Sichern von Inhalt

Zum Schutz sensibler Informationen werden alle Sicherungen verschlüsselt. Wenn Sie den Inhalt wiederherstellen möchten, müssen Sie das Kennwort angeben, das beim Erstellen der Sicherung festgelegt wurde.

Die Sicherung wird als Archivdatei (.zip) an der in Cognos Configuration angegebenen **Bereitstellungsarchivposition** gespeichert. Als Standardposition wird das Verzeichnis *Installationsposition*\deployment verwendet. Wenn der Content Store in einer anderen Instanz von IBM Cognos Analytics bereitgestellt werden soll, beispielsweise auf dem für die Produktionsumgebung verwendeten Computer, kopieren Sie die Archivdatei in die Speicherposition der Bereitstellungsdateien auf dem Zielcomputer, damit die Datei für die Wiederherstellung verfügbar ist.

Eine Sicherung umfasst den folgenden Inhalt.

- Öffentliche Ordner
- Packages
- Berichte
- Datenquellen
- Verteilerlisten und Kontakte
- Druckerkonfiguration
- Zugriffsberechtigungseinstellungen
- Den Cognos-Namespace
- Bereitstellungsspezifikationen

Persönliche Einträge zu den einzelnen Benutzern, zum Beispiel Berichte und Ordner aus dem Bereich **Eigene Inhalte** eines Benutzers, sind nicht in der Sicherung enthalten.

Wiederherstellen von Inhalt

Für die Wiederherstellung von Inhalt muss sich die Sicherungsdatei, die Sie verwenden möchten, an der in Cognos Configuration angegebenen **Bereitstellungsarchivposition** befinden. Als Standardposition

wird das Verzeichnis *Installationsposition*\deployment verwendet. Sie müssen das beim Erstellen der Sicherung festgelegte Kennwort angeben.

Beim Wiederherstellen von Inhalt werden die Inhalte des Ziel-Content Stores entfernt und durch die Inhalte des Quellen-Content Stores ersetzt.

Kapitel 3. Verwalten des Datenzugriffs

IBM Cognos Analytics unterstützt Datenserver, Datenmodule, Packages, Datasets und hochgeladene Dateien als Datenquellen.

Datenserver

Ein Datenserver definiert die physische Verbindung zu einer Datenbank oder einem Cube.

Eine Datenserverbindung gibt die Parameter an, die zum Herstellen einer Verbindung mit der Datenbank oder dem Cube erforderlich sind, beispielsweise die Position der Datenbank und das Zeitlimit. Authentifizierungsinformationen können auch in die Verbindung eingeschlossen werden.

IBM Cognos Analytics unterstützt mehrere relationale und OLAP-Datenserver. Die Liste unterstützter Datenservertypen kann sich zwischen den Releases ändern. Informationen zu den gegenwärtig unterstützten Typen finden Sie auf der Website Unterstützte Softwareumgebungen (www.ibm.com/support/docview.wss?uid=ibm10735235).

Wenn Sie Datenbankauthentifizierungsinformationen, wie die Cognos Analytics-Berechtigungsnachweise oder eine Anmeldung für die Verbindung, einschließen, müssen Benutzer nicht bei jeder Verwendung der Verbindung Datenbankauthentifizierungsinformationen eingeben. Die beim Erstellen einer Datenserververbindung erzeugte Anmeldung ist standardmäßig für die Gruppe **Alle** verfügbar. Sie können die Berechtigungen für die Anmeldung über die Eigenschaften der Datenserververbindung ändern.

Datenserver versus Datenquelle

In der traditionellen **IBM Cognos Administration**-Benutzerschnittstelle ist das Äquivalent von **Datenserver** die **Datenquelle**, für die die JDBC-Verbindung angegeben ist.

Datenquellen werden erst unter **Verwalten** > **Datenserververbindungen** angezeigt, wenn Sie die webbasierte Modellierung für die Datenquellenverbindungen aktivieren. Wechseln Sie dazu zu **Verwalten** > **Administrationskonsole** > **Konfiguration** > **Datenquellenverbindungen** und wählen Sie das Kontrollkästchen **Webbasierte Modellierung zulassen** für die Verbindungen aus. Nur Datenquellen mit JDBC-Verbindungen haben dieses Kontrollkästchen.

Herstellen einer Datenserververbindung

Eine Datenserververbindung gibt die Parameter an, die zum Herstellen einer Verbindung mit der entsprechenden Datenbank oder dem entsprechenden Cube erforderlich sind.

Jeder Datenserver kann über eine oder mehrere Verbindungen verfügen. Die Verbindungsnamen müssen eindeutig sein.

Vorbereitende Schritte

Für die meisten Datenserververbindungen ist ein von einem Datenbankanbieter bereitgestellter JDBC-Treiber erforderlich. Verwenden Sie eine Version des JDBC-Treibers, die mit Java™ Runtime Environment Version 8 kompatibel ist. Kopieren Sie den Treiber in das Cognos Analytics-Verzeichnis *installations-position*\drivers und starten Sie den Abfrageservice erneut. Ein Neustart des vollständigen **IBM Cognos**-Service ist nicht erforderlich.

Für die Erstellung von Datenserververbindungen benötigen Sie die Administrationsberechtigung **Datenquellenverbindungen**. Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics Verwaltung und Sicherheit*.

Wenn Sie eine Datenserververbindung zum The Weather Company-Datenserver erstellen, finden Sie im *Verwaltung - Benutzerhandbuch* Informationen zu Verbindungsparametern, die Sie angeben können.

Informationen zu diesem Vorgang

In der Benutzerschnittstelle **Verwalten** > **Datenserververbindungen** stehen die zur Definition der folgenden Verbindungsfeatures benötigten Steuerelemente nicht zur Verfügung:

- Verbindungsbefehlsblöcke
- Db2 LUW, Db2 for z/OS, Db2 Warehouse, IBM Big SQL - vertrauenswürdige Verbindungen
- Db2 for z/OS - Identitätsweitergabe
- Oracle - einfache Verbindungen (Befehlsblöcke erforderlich)

Wenn Sie Verbindungen definieren möchten, die diese Features umfassen, verwenden Sie die **Administrationskonsole**. Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics Verwaltung und Sicherheit*.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Datenserververbindungen**.
2. Klicken Sie im Fensterbereich **Datenserververbindungen** auf das Symbol **Datenserver hinzufügen**  .
3. Wählen Sie den Datenservertyp in der Liste der unterstützten Typen aus.

   Wählen Sie zum Beispiel **IBM Db2** aus, um eine Verbindung zu einer IBM Db2-Datenbank zu erstellen, oder wählen Sie **IBM Planning Analytics** aus, um eine Verbindung zu einer IBM Cognos TM1-Datenbank zu erstellen.
4. Geben Sie im Feld **Neue Datenserververbindung** einen eindeutigen Namen für die Verbindung ein.
5. Klicken Sie neben **Verbindungsdetails** auf **Bearbeiten** und geben Sie die Verbindungsdetails für den Typ der Verbindung ein, die Sie erstellen.

   Für die meisten Verbindungen müssen Sie die JDBC-URL angeben. Unter den Verbindungsdetails können Sie die Syntax und eine Beispiel-URL anzeigen. Möglicherweise müssen Sie sich an den Datenbankadministrator wenden, um weitere Details zu erhalten, oder die Informationen in der Dokumentation des Datenbankanbieter lesen.

   Geben Sie im Feld **Verbindungseigenschaften** den Namen der unterstützten Eigenschaft ein. Informationen zu den unterstützten JDBC-Eigenschaften finden Sie in „Cognos-spezifische Verbindungsparameter” auf Seite 47.

   Geben Sie für Verbindungen zu **IBM Planning Analytics** den Host und die HTTP-Portnummer der TM1-Datenbank ein. Wenn Sie eine SSL-Verbindung verwenden möchten, wählen Sie das Feld **SSL verwenden** aus.
6. Geben Sie unter **Authentifizierungsmethode** an, wie auf den Datenserver zugegriffen werden soll.

   Sie können eine der nachfolgend aufgeführten Optionen auswählen.

   'Anonyme Verbindung herstellen' oder 'Integrierte Sicherheit'

   Wählen Sie die Option **Anonyme Verbindung herstellen**, wenn der anonyme Zugriff auf den Datenserver zulässig ist.

   Wählen Sie die Option **Integrierte Sicherheit** aus, wenn die TM1-Datenbank für den integrierten Sicherheitsmodus 4 oder 5 konfiguriert ist. Diese Option ist nur für Verbindungen zu **IBM Planning Analytics** anwendbar.

   Zur Eingabe der Benutzer-ID und des Kennworts auffordern

   Wählen Sie diese Option aus, wenn der Benutzer bei jeder Anmeldung zur Eingabe der Datenbank-Berechtigungsnachweise aufgefordert werden soll.

Externen Namespace verwenden

Wählen Sie diese Option aus, um die Verbindung gegen einen Namespace zu schützen, der für Cognos Analytics konfiguriert ist. Wählen Sie einen der verfügbaren Namespaces über das Dropdown-Menü aus.

Cognos Analytics meldet sich bei dem Datenserver mit den Berechtigungsnachweisen an, die zur Authentifizierung bei dem ausgewählten Namespace verwendet werden. Der Namespace muss aktiv sein, Benutzer müssen vor dem Zugriff auf die Datenserververbindung angemeldet sein und die für den Namespace verwendeten Berechtigungsnachweise müssen für die Datenserverauthentifizierung relevant sein.

In der Regel wird diese Authentifizierungsmethode in den folgenden Situationen verwendet:

- Sie wollen, dass Cognos Analytics während der Authentifizierung die Benutzer-ID und das Kennwort, an die Datenbank übergibt, die an das Portal gesendet werden.
- Sie wollen, dass Cognos Analytics die Kerberos-Authentifizierung verwendet.
- Sie wollen, dass Cognos Analytics die JSON-Web-Token-Authentifizierung (JWT-Authentifizierung) verwendet.

Der Abfrageserver ermittelt die Berechtigungsinformationen, die durch den externen Namespace bereitgestellt werden, und wählt die Verbindungsmethode aus, die versucht werden soll.

Die folgende Anmeldung verwenden

Wählen Sie diese Option, um eine Anmeldung für die Verbindung zuzuweisen.

Wählen Sie die Anmeldung in der Dropdown-Liste aus oder erstellen Sie eine neue Anmeldung, indem Sie auf das Symbol 'Hinzufügen' klicken. Geben Sie im Fenster **Neue Datenserververbindung** auf der Registerkarte **Berechtigungsnachweise** eine Benutzer-ID und ein Kennwort ein.

Um die Anmeldung auf bestimmte Benutzer, Rollen oder Gruppen zu beschränken, klicken Sie auf der Registerkarte **Berechtigungen** auf das Symbol 'Hinzufügen' und geben die Zugriffsberechtigungen für die Anmeldung an.

Wenn Sie eine Datenquellenverbindung für The Weather Company erstellen, müssen Sie mindestens eine Anmeldung konfigurieren. Das Kennwort muss Ihr The Weather Company-API-Schlüssel sein.

7. Klicken Sie auf **Testen**, um die Datenserververbindung zu überprüfen, und anschließend auf **Speichern**, um die neue Datenserververbindung zu speichern.

Ergebnisse

Der neue Verbindungsname wird im Fenster **Datenserververbindungen** angezeigt. Sie können die Datenserververbindung bearbeiten, beispielsweise durch Hinzufügen oder Ändern der entsprechenden Anmeldung, indem Sie auf ihren Namen klicken.

Anmerkung: Möglicherweise wird die folgende Nachricht angezeigt:

MSR-GEN-0026 Das Schema "*Schemaname*" ist leer oder es besteht mit der aktuellen Anmeldung kein Zugriff darauf

Wie angegeben, kann diese Nachricht bedeuten, dass das Schema leer ist (keine Objekte enthält) oder dass der Benutzer keinen Zugriff auf das Schema hat. Die Nachricht kann jedoch auch bedeuten, dass das Schema zwei keine TABLE-Objekte wie TABLE, VIEW oder SYNONYM für ein TABLE/VIEW-Objekt, jedoch andere Objekttypen enthält. In diesem Szenario ist die generierte Nachricht falsch.

Nächste Schritte

Wenn Sie einen Datenserver als Quelle für Berichte, Dashboards, Explorationen und andere Cognos Analytics-Inhalte verwenden wollen, erstellen Sie Datenmodule, die auf der Verbindung basieren.

Für Verbindungen zu relationalen Datenservern müssen Sie die Schemametadaten vorab laden, um das Schema zum Erstellen von Datenmodulen in der Modellierungskomponente verfügbar zu machen. Weitere Informationen finden Sie unter „Laden von Metadaten” auf Seite 51.

Für Verbindungen zu **IBM Planning Analytics** können Sie Datenmodule direkt über die Verbindungsbenutzerschnittstelle erstellen. Weitere Informationen finden Sie unter „Erstellen von Datenmodulen aus Planning Analytics-Cubes” auf Seite 65.

Für Verbindungen zu The Weather Company gelten einige Anforderungen für die Erstellung eines Datenmoduls für den The Weather Company-Server. Weitere Informationen finden Sie im Beispiel 'The Weather Company' in der Veröffentlichung *Beispiele*.

Datenservertypen - Verbindungsdetails

Einige Datenservertypen erfordern eindeutige Parameter, wenn Sie ihre Verbindungen konfigurieren.

In diesem Abschnitt werden die Verbindungsdetails für einige dieser Datenservertypen beschrieben.

IBM Planning Analytics-Datenserververbindungen

Wenn Sie planen, eine Verbindung zu einem IBM Planning Analytics-Datenserver herzustellen, können Sie die Datenverwaltung durch Cognos Analytics optimieren, indem Sie die Tasks in diesem Abschnitt ausführen.

Verbindung zu Planning Analytics-Datenservern herstellen

11.1.7 Aus einer IBM Cognos Analytics on Demand-Umgebung können Sie eine Verbindung zu einem TM1-Datenserver herstellen, der sich in einer Planning Analytics on Cloud-Umgebung befindet. Wählen Sie dazu Datenserververbindung erstellenaus und wählen Sie **IBM Planning Analytics** als Datenservertyp aus.

Wichtig: In diesem Abschnitt wird beschrieben, wie die Authentifizierungsmethode in Cognos Analytics so festgelegt wird, dass sie mit der Authentifizierungsmethode übereinstimmt, die auf dem TM1-Datenserver verwendet wird. Der TM1-Datenbankadministrator muss jedoch auch den TM1 Server mit der dedizierten Cognos Analytics-Instanz, die dem Benutzer 'Planning Analytics Tenant' zugeordnet ist, sichern. Wenden Sie sich an den TM1-Datenbankadministrator, um die URL des TM1-Datenbankservers zu bestimmen.

Benutzer und Gruppen werden separat verwaltet und in Cognos Analytics on Demand und Planning Analytics on Cloud konfiguriert. Daher können Sicherheitsgruppen in Cognos Analytics on Demand nicht in Planning Analytics on Cloud verwendet werden.

Die Benutzer-ID von Cognos Analytics on Demand muss in der Subscription für Planning Analytics on Cloud enthalten sein.

Weitere Informationen finden Sie unter "Planning Analytics security overview" im Handbuch *IBM Planning Analytics TM1 Operations Guide*.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Datenserververbindungen**.
2. Klicken Sie im Teilfenster **Datenserververbindungen** auf das Symbol **Datenserver hinzufügen** + .
3. Wählen Sie **IBM Planning Analytics** in der Liste der unterstützten Typen aus.
4. Geben Sie im Feld **Neue Datenserververbindung** einen eindeutigen Namen für die Verbindung ein.
5. Wählen Sie unter **Authentifizierungsmethode**die Option **Integrierte Sicherheit**aus, in der die TM1-Datenbank für den integrierten Sicherheitsmodus 4 oder 5 konfiguriert ist.
6. Klicken Sie neben **Connections-Details**auf **Bearbeiten** und geben Sie die Verbindungsdetails ein:
   a. Geben Sie in das Feld **TM1-Datenbankhost** die URL des TM1-Datenbankservers ein, z. B.:

```
https://prodsupport.planning-analytics.ibmcloud.com/api/v0/tm1/GO_New_Stores
```

b. Geben Sie in das Feld **HTTP-Portnummer** den Wert `-2` ein.

c. Lassen Sie das Kontrollkästchen **SSL verwenden** nicht ausgewählt.

7. Klicken Sie auf **Test** ▷ , um sicherzustellen, dass die Verbindung gültig ist.
8. Klicken Sie auf **Speichern**.

Sicherstellen, dass Stammmitglieder in einer Planning Analytics-Datenquelle mit denen im TM1-Client übereinstimmen

11.1.3 Wenn Sie eine TM1-Datenquelle in Cognos Analytics importieren und den Datenquellentyp als **IBM Planning Analytics** auswählen, kann die Liste der Stammmitglieder in der Metadatenverzeichnisstruktur anders aussehen als die Liste, die im TM1-Client angezeigt wird.

Lösung

Sie können die REST-API `tm1.RootMembers()` aktivieren. Diese REST-API gibt Stammmitglieder von der Planning Analytics-Datenquelle zurück, die mit den vom TM1-Client zurückgegebenen Stammmitgliedern übereinstimmen.

Wichtig: Sie müssen Version 2.0.6 oder höher des Planning Analytics-Servers verwenden.

Führen Sie folgende Schritte aus:

1. Stoppen Sie den IBM Cognos Analytics-Service.
2. Wechseln Sie in das Verzeichnis *Installationsposition*`\configuration`.
3. Wenn die Datei `xqe.config.custom.xml` noch nicht vorhanden ist, kopieren Sie die Datei `xqe.config.xml` und benennen Sie sie in `xqe.config.custom.xml` um.
4. Bearbeiten Sie die Datei `xqe.config.custom.xml`:
   a. Fügen Sie unmittelbar nach der Zeile <queryExecution> die folgende Zeile hinzu:

```
<paUseRootMembers enabled="true"/>
```

   b. Speichern Sie die Datei `xqe.config.custom.xml`.
5. Starten Sie den IBM Cognos Analytics-Service.

Füllmitglieder in einem Planning Analytics-Paket inaktivieren

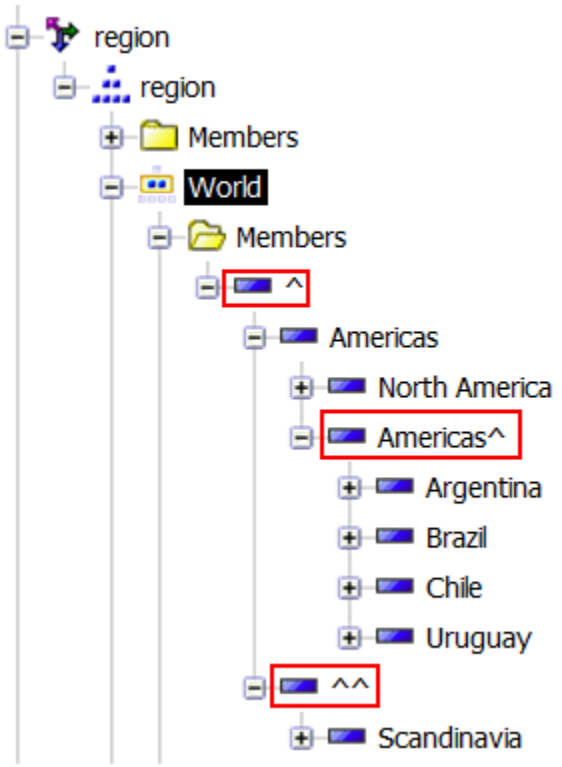
11.1.2 Sie können die automatische Generierung von Füllmitgliedern inaktivieren, sodass ein in Cognos Analytics importiertes Planning Analytics-Paket dieselben Merkmale hat wie im TM1-Client.

In Cognos Analytics werden standardmäßig Füllelemente generiert, um Lücken zu schließen, da der Zugriff vom Stamm der Hierarchie bis zu den Mitgliedern beschränkt ist, deren Daten für den Benutzer sichtbar sind. In IBM Cognos TM1 werden jedoch keine Füllmitglieder generiert.

Beispiel 1: Füllmitglieder aktiviert

Wenn Füllmitglieder aktiviert sind, entspricht die Titelzeile eines Füllmitglieds in der Datenverzeichnisstruktur der Titelzeile des übergeordneten Mitglieds mit angehängtem Winkelzeichen (^). Wenn dem Benutzer kein Zugriff auf ein Stammmitglied erteilt wird, besteht die Titelzeile des Stammmitglieds nur aus einem Winkelzeichen (^).

Eine Metadatenverzeichnisstruktur mit aktivierten Füllmitgliedern wird in der folgenden Abbildung dargestellt:



Ein Diagramm für denselben Cube wird wie folgt angezeigt:

Budget	1 Quarter	2 Quarter	3 Quarter	4 Quarter
*Americas^*				
North America	*825517.05*	*846801.29*	*830379.17*	*868830.05*
Total(children(Am))	**825517.05**	**846801.29**	**830379.17**	**868830.05**

Beispiel 2: Füllmitglieder inaktiviert

Anmerkung: Da der Zugriff auf das Stammmitglied für den Cube in Beispiel 1 eingeschränkt ist, kann der Benutzer, wenn Füllmitglieder inaktiviert sind, keine Mitglieder in der Datenverzeichnisstruktur sehen.

Ein Diagramm von demselben Cube wird wie folgt angezeigt:

Budget	1 Quarter	2 Quarter	3 Quarter	4 Quarter
North America	*825517.05*	*846801.29*	*830379.17*	*868830.05*
Total(children(Am))	**825517.05**	**846801.29**	**830379.17**	**868830.05**

Prozedur

Führen Sie die folgenden Schritte aus, um sicherzustellen, dass eine Datenquelle dieselben Merkmale im TM1-Client und Planning Analytics hat:

1. Stoppen Sie den IBM Cognos Analytics-Service.
2. Wechseln Sie in das Verzeichnis *Installationsposition*\configuration.

3. Wenn die Datei `xqe.config.custom.xml` noch nicht vorhanden ist, kopieren Sie die Datei `xqe.config.xml` und benennen Sie sie in `xqe.config.custom.xml` um.
4. Bearbeiten Sie die Datei `xqe.config.custom.xml`:
   a. Fügen Sie unmittelbar nach der Zeile <queryExecution> die folgende Zeile hinzu:

```
<!-- Attributwert 'paUseFillerMember enabled' auf 'false' setzen, um Füllmitglied zu inak
tivieren -->
<paUseFillerMember enabled="false"/>
```

   b. Speichern Sie die Datei `xqe.config.custom.xml`.
5. Starten Sie den IBM Cognos Analytics-Service.

Probleme, die aus doppelten (mehrdeutigen) Namen in Planning Analytics-Cubes abgeleitet wurden

Wenn ein Planning Analytics-Server über Elemente eines anderen Typs verfügt, z. B. ein Member, ein Level oder eine Untergruppe, die einen Namen gemeinsam nutzen, kann der Cognos AnalyticsAbfrageservice diese Elemente nicht ordnungsgemäß verarbeiten. Die Abfragen werden mehrdeutig.

Die folgenden Abfragen können mehrdeutig werden.

- Die Abfrage enthält einen Namen, der von einem Subset, einem Member oder einer Ebene gemeinsam genutzt wird.

  Die Wahrscheinlichkeit, dass die Antwort auf diese Abfrage das angeforderte Objekt enthält, ist wahrscheinlich nicht enthalten. Wenn die Abfrageantwort nicht die erwartete Antwort ist, erkennt der Abfrageservice das Problem und erstellt einen internen Fehler, der mit der folgenden Nachricht beginnt: `XQE-GEN-0010 Gefunden einen internen Fehler: '! mapSuccess-reportName=`
- Die Abfrage verweist auf einen Namen, der von einem Member und einer Ebene in einem Cube gemeinsam genutzt wird.

  Die Abfrageantwort entspricht dem Member und nicht der Ebene. Ein Bericht oder ein Dashboard-Autor, der für die mehrdeutig benannte Ebene fragt, sieht jedoch stattdessen ein einzelnes Member, das denselben Namen hat wie die angeforderte Ebene.

Die Lösung für diese Art von Problemen besteht darin, allen Mitgliedern, Ebenen und Untergruppen innerhalb der Würfeldimension eindeutige Namen zu geben.

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-XX`angegeben 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.
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.

Parameter	Beschreibung
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.

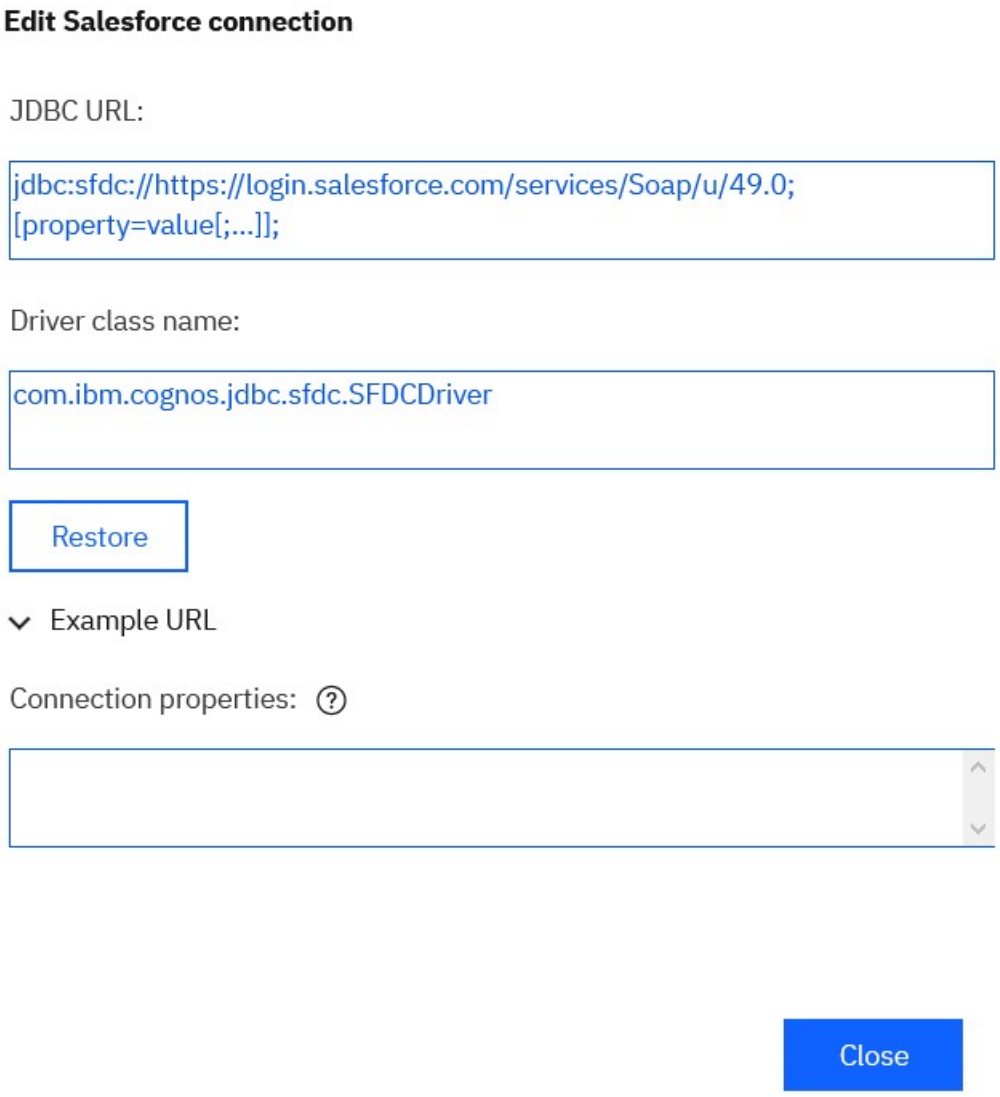
Im folgenden Beispiel werden nur die Objekte importiert, die für den The Weather Company -API-Schlüssel verfügbar sind, der der Anmeldung zugeordnet ist. Eine Abfrage kann bis zu 250 MB Speicher verwenden.

```
jdbc:twc://?FILTER_METADATA=true,CACHE_SIZE=250
```

Verbindungseditor für Salesforce

11.1.7 Der Verbindungseditor für Salesforce ist sowohl über **Verwalten** > **Datenserververbindungen** als auch über die Administrationskonsole verfügbar.

Das folgende Diagramm zeigt das Fenster zum Bearbeiten der Verbindung für Salesforce:



Wenn Sie eine neue Verbindung erstellen, enthält die Standard-URL den Standardinstanznamen `login.salesforce.com` und die API-Version `49.0`.

Beispiel:

```
jdbc:sfdc://https://login.salesforce.com/services/Soap/u/49.0;
```

Optionale Name/Wert-Paare können in der URL oder als Teil der Verbindungseigenschaften angegeben werden.

Beispiel:

```
jdbc:sfdc://https://login.salesforce.com/services/Soap/u/49.0;QUERYBATCHSIZE=1000;
```

Namen sind von der Groß-/Kleinschreibung unabhängig. Tritt ein doppelter Name auf, wird derjenige Name verwendet, der als Letzter mittels Parsing aus den URL- oder Verbindungseigenschaften ermittelt wurde. Nicht erkannte Namen oder ungültige Werte führen zu einer Fehlernachricht.

Verbindungseigenschaften für Salesforce

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie an die Verbindungszeichenfolge anhängen können.

Verbindungseigenschaft	Beschreibung
CONNECTION_TIMEOUT	Wenn eine Verbindung in der angegebenen Zeit nicht hergestellt werden kann, erfolgt automatisch eine Zeitlimitüberschreitung. Der Standardwert ist 60 Sekunden. Der Wert muss ein Ganzzahlwert im Bereich 0 (null) bis 2147483647 sein. Falsche Werte führen zu einem Fehler.
MAX_RETRIES	Wenn bei dem Versuch, eine Verbindung herzustellen, ein Netzfehler zurückgegeben wird, dann wird der Verbindungsversuch so oft wiederholt, bis der angegebene Maximalwert erreicht ist. Der Standardwert ist 1 (eins). Der Wert muss ein Ganzzahlwert im Bereich 0 (null) bis 2147483647 sein. Falsche Werte führen zu einem Fehler.
WAIT_BETWEEN_RETRIES	Wenn der Versuch, eine Verbindung herzustellen, wiederholt wird, dann wartet das System zwischen den einzelnen Wiederholungsversuchen die angegebene Anzahl von Sekunden ab. Der Standardwert ist 0 (null). Der Wert muss ein Ganzzahlwert im Bereich 0 (null) bis 2147483647 sein. Falsche Werte führen zu einem Fehler.
PROXY_ENABLED	Gibt an, ob ein Proxy-Server zwischen Cognos Analytics und Salesforce verwendet wird. Der Standardwert ist 'false'. Der Wert muss entweder 'false' oder 'true' sein. Falsche Werte führen zu einem Fehler.
PROXY_HOST	Der Hostname des Proxy-Servers, der verwendet wird, wenn PROXY_ENABLED auf 'true' gesetzt ist. Ein gültiger Hostname, auf den zugegriffen werden kann und der den Proxy-Server hostet. Falsche Werte führen zu einem Fehler.
PROXY_PORT	Die Portnummer des Proxy-Servers, der verwendet wird, wenn PROXY_ENABLED auf 'true' gesetzt ist. Der Standardwert ist 80. Eine gültige Portnummer. Falsche Werte führen zu einem Fehler.
PROXY_USERNAME	Gibt einen Benutzernamen für den Proxy-Server an, der verwendet wird, wenn PROXY_ENABLED auf 'true' gesetzt ist. Falsche Werte führen zu einem Fehler.

Verbindungseigenschaft	Beschreibung
PROXY_PASSWORD	Gibt einen Kennwort für den Proxy-Server an, der verwendet wird, wenn PROXY_ENABLED auf 'true' gesetzt ist. Falsche Werte führen zu einem Fehler.
QUERY_BATCH_SIZE	Gibt die Stapelgröße an, die von der Salesforce-Abfrage-API verwendet wird. Der Standardwert ist 500. Der Wert muss ein Ganzzahlwert im Bereich 200 bis 2000 sein.
CONCURRENT_CALLS_LIMIT	Gibt die maximal zulässige Anzahl an gleichzeitigen Anforderungen an. Der Standardwert ist 25. Der Wert muss ein Ganzzahlwert im Bereich 1 (eins) bis 2147483647 sein.
USER_CONCURRENT_CALLS_LIMIT	Gibt die maximal zulässige Anzahl an gleichzeitigen Anforderungen für einen Benutzer an. Der Standardwert ist 10. Der Wert muss ein Ganzzahlwert im Bereich 200 bis 2000 sein.

Anmerkung: In Vorgängerversionen von Cognos Analytics wird noch ein Verbindungseditor bereitgestellt, der nur über die Administrationskonsole verfügbar ist. Diese Verbindungen können nur für Framework Manager-Packages verwendet werden. Verbindungen, die diesen Editor verwenden, funktionieren zwar weiterhin, doch wird dieser Verbindungseditor in einem zukünftigen Release von Cognos Analytics nicht weiter unterstützt. Anwendungen sollten für die Verwendung des neuen Verbindungseditors entsprechend migriert werden.

In die von diesen Verbindungen beschriebenen Metadaten werden nicht-gruppierbare Spalten üblicherweise eingeschlossen, während diese Spalten vom neuen Editor standardmäßig ausgeschlossen werden.

Progress DataDirect Autonomous REST-Verbindungen

11.1.7 The Progress DataDirect Autonome REST-Verbindung fragt JSON-Antworten von API-Endpunkten ab, auf die über das HTTP-Protokoll zugegriffen wird. Die Verbindung generiert eine Konfigurationsdatei, die den JSON-Inhalt des Endpunkts in Datenbanktabellen (Schemas) in Cognos Analytics umsetzt. Sie können Dashboards und Berichte erstellen, die diese REST-API-Endpunktdaten als ihre Datenquelle verwenden.

Zum Erstellen oder Bearbeiten einer Verbindung zu einem Progress-DataDirect-Datenserver wechseln Sie zu **Verwalten** > **Datenserververbindungen**. Ihre Verbindung kann auf eine einzelne URL oder auf mehrere Endpunkt-URLs zugreifen.

Ausführliche Informationen zum Konfigurieren einer Verbindung und der unterstützten Optionen: Siehe *Progress ® DataDirect ® Autonomous REST Connector for JDBC™ User's Guide for Partners*.

Die Verbindungszeichenfolge, die Sie eingeben, muss entweder ein Name/Wert-Paar `'Sample=REST_API_endpoint'` oder `'Config=configuration_file'` enthalten, in dem die abzufragenden Endpunkte angegeben sind. Möglicherweise müssen Sie in Ihrer Verbindung auch einen API-Schlüssel angeben. Wenn Sie dies tun, stellen Sie sicher, dass die Berechtigungen für die Datenserververbindung nur für die Personen gelten, für die der Zugriff mit diesem API-Schlüssel erforderlich ist.

- Die Methode `Sample` ermöglicht das einfache Abrufen von Daten von einer einzelnen Endpunkt-URL. Wenn Sie jedoch mit großen Datenmengen in einem komplexen Schema arbeiten, kann diese Methode

die Leistung verlangsamen. Der Grund hierfür ist, dass der Treiber die Endpunkt-zu-Schema-Zuordnung auf sich selbst aufbauen muss.

.Weitere Informationen finden Sie unter" Beispiel" auf Seite 99 des Autonomen REST-Connectors von *Progress ® DataDirect ® for JDBC™ . Benutzerhandbuch für Partner*.

- Mit der Methode `Config` können Sie den Endpunkt für die Schemazuordnung zur Konfigurationszeit definieren. Sie bietet die folgenden Vorteile:
  - Die Arbeit, die der Treiber zur Laufzeit ausgeführt hat, wird erheblich reduziert und die Ergebnisse werden schneller zurückgegeben.
  - Sie kann mehrere REST-API-Endpunktanforderungen in einer einzigen Verbindung ausgeben.
  - Sie entspricht den REST-API-Ergebnissen für die Schemazuordnung. Auf diese Weise können angepasste Tabellennamen, Spaltennamen und Datentypzuordnungen verwendet werden.

  Weitere Informationen finden Sie im Abschnitt "Konfiguration" auf Seite 73 des Autonomen REST-Connectors von *Progress ® DataDirect ® für JDBC™ . Benutzerhandbuch für Partner*.

Vorbereitende Schritte: Lesen Sie das Thema" Treiber einrichten" auf Seite 10 des *Progress ® DataDirect ® Autonomous REST Connector for JDBC™ User's Guide for Partners*.

Beispielparameter

Geben Sie den Parameter `Sample` in der JDBC-URL einer REST-API-Verbindung an. Die REST-Antwort ist ein tabellarisches Schema, das Sie in Cognos Analytics als Datenmodul importieren können.

Das Feld **JDBC-URL** wird angezeigt, wenn Sie eine Datenserververbindung erstellen und als Verbindungstyp **Progress Data Direct Autonomous REST connection** (Progress Data Direct Autonomous REST Connection) auswählen.

Für weitere Details: verwendenLesen Sie das Thema" Beispieleigenschaftenmethode" verwenden auf Seite 19 des Handbuchs *Progress ® DataDirect ® Autonomous REST Connector for JDBC™ User's Guide for Partners*

Syntax

```
jdbc:ibmcognos: autorest:Beispiel= 'endpoint_URL'
```

Die Endpunkt-URL

Bei der Endpunkt-URL handelt es sich um eine REST-API-Position, die Daten zurückgibt, die Sie in Cognos Analytics verwenden können. Sie kann viele optionale Verbindungseigenschaften enthalten, um verschiedene Typen von API-Antworten und -Authentifizierung zu berücksichtigen. Seine Eigenschaften unterstützen beispielsweise viele OAuth 2.0-Authentifizierungsdatenflüsse, die je nach den Sicherheitsanforderungen jedes Web-Service variieren.

Beispiel-URLs

Die folgende Verbindung führt ein HTTP-GET für die URL `http://worldtimeapi.org/api/timezone/America/Toronto`aus. Die vom Endpunkt zurückgegebene JSON-Antwort wird als Tabelle mit Spalten dargestellt, die den Feldern in der Antwort entsprechen.

```
jdbc:ibmcognos:autorest:Sample=http://worldtimeapi.org/api/timezone/America/Toronto
```

Wenn eine URL Zeichen enthält, die vom Treiber verwendet werden, müssen Sie die URL in einfache Anführungszeichen setzen. Die folgende URL enthält eine Abfragezeichenfolge, in der das Name/Wert-Paar ein Gleichheitszeichen (=) enthält.

```
jdbc:ibmcognos:autorest:Sample='http://myWebSite/resources?type=dog'
```

Anmerkung: Weitere Beispiele finden Sie unter „Beispiele mit der Methode Sample-Parameter” auf Seite 41.

Konfigurationsparameter

Geben Sie den Parameter `Config` in der JDBC-URL einer REST-API-Verbindung an. Im Gegensatz zur `Sample` -Methode erstellt die `Config` -Methode eine Verbindung, die auf eine lokale Konfigurationsdatei verweist. Sie können diese `.json` -Konfigurationsdatei so anpassen, dass die Schemaübersetzung vorkonfiguriert ist. Auf diese Weise können Sie eine hohe Leistung erzielen, wenn Sie große Datenmengen abrufen.

Das Feld **JDBC-URL** wird angezeigt, wenn Sie eine Datenserververbindung erstellen und als Verbindungstyp **Progress Data Direct Autonomous REST connection** (Progress Data Direct Autonomous REST Connection) auswählen.

Für weitere Details: Lesen Sie das Thema" Methode" der Eingabe-REST-Datei verwenden auf Seite 20 des *Progress ® DataDirect ® Autonomous REST Connector for JDBC™ User's Guide for Partners*

Syntax

```
jdbc:ibmcognos: autorest:Konfiguration= "path_to_local_configuration_file"; ServerName=End
point_URL
```

Dabei gilt:

- *path_to_local_configuration_file* ist der Pfad, der in doppelte Anführungszeichen eingeschlossen ist, an eine zentrale Position, an die Sie die Konfigurationsdatei hochgeladen haben.

  Weitere Informationen finden Sie unter „JSON-Dateien an einer zentralen Position speichern” auf Seite 41.
- *Endpoint_URL* ist eine REST-API-Position, die Daten zurückgibt, die Sie in Cognos Analytics verwenden können. Sie kann viele optionale Verbindungseigenschaften enthalten, um verschiedene Typen von API-Antworten und -Authentifizierung zu berücksichtigen. Seine Eigenschaften unterstützen beispielsweise viele OAuth 2.0-Authentifizierungsdatenflüsse, die je nach den Sicherheitsanforderungen jedes Web-Service variieren.

Für weitere Details: Weitere Informationen finden Sie im Artikel "Syntax" für REST-Eingabedateien auf der Seite 117 des *Progress ® DataDirect ® Autonomous REST Connector for JDBC™ User's Guide for Partners*.

API-Schlüssel

Wenn der Data Direct-Datenserver, zu dem Sie eine Verbindung herstellen, die OAuth 2.0-Authentifizierung verwendet, müssen Sie Werte für den Schlüssel und den geheimen Schlüssel in der Verbindungszeichenfolge angeben.

Möglicherweise ist für einen Endpunkt ein API-Schlüssel erforderlich, bevor er Anforderungen akzeptieren kann. Es kann sein, dass eine Site einen Prozess verwendet, um ein Token zu generieren, das Teil des HTTP-Anforderungsheaders sein muss. Der Treiber stellt Name/Wert-Paare bereit, die zum Festlegen von Headervariablen verwendet werden können. Der Schlüssel kann auf verschiedene Art und Weise angegeben werden:

- in den URL- oder Verbindungseigenschaften
- im optionalen Schlüsselfeld
- über eine Cognos Analytics-Sitzungsvariable

Beispiel: Wenn eine Site einen API-Schlüssel generiert, der als Trägertoken übergeben werden muss, und Sie den Schlüssel ausgeblendet lassen wollen, dann verwenden Sie das optionale Schlüsselfeld. Wenn es sich bei dem Schlüssel um ein Trägertoken handelt, geben Sie den Wert `Bearer` für Träger ein, gefolgt von einem Leerschritt, auf das wiederum der API-Schlüssel der Site folgt.

Für weitere Details: Siehe die Themen "ClientId" und "ClientSecret" auf den Seiten 71 und 72 der Veröffentlichung *Progress® DataDirect® Autonomous REST Connector for JDBC™ User's Guide for Partners*.

Tipps zum Erstellen von REST-API-Verbindungen

Dieser Abschnitt enthält Tipps, mit denen Sie Zeit sparen können, wenn Sie eine autonome DataDirect-REST-Verbindung erstellen.

API forschen, zu der eine Verbindung hergestellt werden soll

Bevor Sie eine Verbindung zu einem bestimmten API-Endpunkt definieren, überprüfen Sie die Dokumentation der API, um Antworten auf diese Fragen zu finden:

- ☐ Was ist das Format der URL und der Abfragezeichenfolge?
- ☐ Was ist das Format der zurückgegebenen JSON-Antworten?
- ☐ Welche Einschränkungen kann ein Endpunkt in Bezug auf Anforderungen in einem Zeitraum festlegen?
- ☐ Welche Methoden werden verwendet, um Anforderungen zu authentifizieren, z. B. über einen API-Schlüssel?
- ☐ Gibt die Verbindung Endpunkte an, die für analytische Anwendungen entworfen wurden?
- ☐ Was ist die Antwortzeit des Endpunkts?
- ☐ Wie werden die Antworten vom Treiber zugeordnet?

Diese Tools testen

Sie können das Verhalten der Endpunkte mithilfe der folgenden Tools recherchieren:

- ☐ Curl
- ☐ Postman
- ☐ Web-Browser

Ist der Endpunkt angemessen?

Ein Kandidatenendpunkt kann *nicht* für eine Verbindung von Cognos Analytics geeignet sein, wenn die Verbindung eines der folgenden Verhaltensweisen aufweist:

- ☐ Es wird kein HTTP für das Protokoll verwendet.
- ☐ Es werden keine JSON-Antworten zurückgegeben.
- ☐ Es wird eine proprietäre Abfragespezifikationssprache verwendet, die in der Hauptteil-/Abfragezeichenfolge ausgedrückt wird.
- ☐ Die JSON-Darstellung kann nicht in ein Schema umgesetzt werden, das vom Treiber verwendet wird.
- ☐ Die Endpunkte wurden möglicherweise nicht speziell für analytische Anwendungen entwickelt.

Beispiel: Ein Geschäftsbenutzer will ein Dashboard erstellen, in dem Informationen für mehrere Standorte über mehrere Geschäftstage zusammengefasst werden. Wenn nun die URL so konzipiert ist, dass Informationen lediglich für einen einzigen Standort und einen einzigen Tag zurückgeben werden, muss sie möglicherweise erweitert werden.

Boolesche Werte dem Typ 'VarChar' oder 'Integer' zuordnen

Cognos Analytics unterstützt keine zurückgegebenen booleschen Werte, z. B. 'true' oder 'false'. Wenn Ihre JSON-Ausgabe boolesche Werte enthält, können Sie demzufolge die Methode `Sample` nicht verwenden. Verwenden Sie stattdessen die Methode `Config` , um boolesche Werte entweder Text (z. B. `VarChar`) oder Ganzzahlen (`Integer`) zuzuordnen.

Informationen zu den Datentypen, die von Cognos Analytics unterstützt werden, finden Sie unter "Unterstützte SQL-Datentypen" im Cognos Analytics-*Datenmodellierungshandbuch*..

Verschachtelte Datenobjekte im Namen der Tabelle der höchsten Ebene angeben

Einige API-Aufrufe geben Datenobjekte zurück, die unter einer Tabelle der höchsten Ebene verschachtelt sind. Sie können eine Namenskonvention für die Tabelle der höchsten Ebene annehmen, die folgendes angibt:

- Die Daten sind verschachtelt
- Den Namen des verschachtelten Objekts, dessen Daten in Cognos Analytics verwendet werden sollen

Eine Tabelle der höchsten Ebene kann beispielsweise Attribute auf Aufrufebene enthalten, z. B. `success`, `return code`, `error message` und auch ein Array (oder Objekt) mit dem Namen `data`. In diesem Beispiel enthält `data` die Daten, an denen Sie interessiert sind. Sie geben der Tabelle der höchsten Ebene den Namen `ObjectResults` und dem verschachtelten Array den Namen `Object`. Auf diese Weise können Sie bei der Erstellung eines Datenmoduls die `ObjectResults` -Tabellen ignorieren und nur die verschiedenen `Object` -Tabellen in Ihr Modul einbringen.

Für weitere Details: Lesen Sie das Thema "Spalten mit verschachtelten Objekten" auf Seite 143 des Handbuchs *Progress® DataDirect® Autonomous REST Connector for JDBC™ User's Guide for Partners*

Kommentare hinzufügen

Sie können Kommentare zu den Konfigurationsdateien für die Progress DataDirect-REST-API hinzufügen. Geben Sie dazu `//` am Anfang jeder Kommentarzeile ein. Verwenden Sie Kommentare, um den Inhalt Ihrer Konfigurationsdatei sowie alle Nuancen der APIs, die Sie aufrufen, zu dokumentieren.

Sie möchten zum Beispiel zwei Untergruppen von Daten aus derselben API abrufen. Wenn Sie jedoch versuchen, alle Daten in einem Aufruf abzurufen, überschreitet die API das Zeitlimit, da zu viele Daten vorhanden sind. Um dieses Problem zu lösen, entscheiden Sie, zwei separate Aufrufe an die API zu machen, von denen jeder eine andere Untergruppe abrufen kann. Sie fügen einen Kommentar hinzu, der erklärt, warum Ihr Schema zwei Aufrufe anstelle von einem durchführt.

Überschreibungen von Spaltennamen verwenden

Sie können die Spaltennamen Ihrer JSON-Ausgabe in etwas ändern, das für Endbenutzer und Analysten mehr Aussagekraft hat. Wenn Sie einen Spaltennamen überschreiben möchten, bearbeiten Sie Ihre Konfigurationsdatei und fügen Sie die neuen Namen in eckigen Klammern ein. Das heißt, ändern Sie "*alter-spaltenname*" in "*alter-spaltenname<neuer-spaltenname>*".

Beispiel: Sie verwenden in der Regel Unterstreichungszeichen in Ihren Schemas. Die API, die Sie aufrufen, gibt jedoch verknüpfte Namen zurück. Sie entscheiden sich, sie so umzubenennen, dass Unterstreichungszeichen verwendet werden. Sie bearbeiten die Konfigurationsdatei und ändern den folgenden Text:

```
"fieldNumberOne":"VarChar(64)"
```

in

```
"fieldNumberOne<field_number_1>":"VarChar(64)"
```

Zugehörige Datenmodule nach einer Verbindungsaktualisierung erneut verbinden

Wenn Sie eine neue Version Ihrer autonomen Data Direct-REST-Verbindung speichern, aktualisieren Sie ein Schema. Wie bei jeder Schemaänderung müssen Sie jedes Datenmodul, das diese Datenserververbindung verwendet, erneut verbinden.

Weitere Informationen finden Sie im Abschnitt zum "erneuten Verbinden von Quellen" im Cognos Analytics-*Datenmodellierungshandbuch*.

JSON-Dateien an einer zentralen Position speichern

Stellen Sie sicher, dass Sie Ihre JSON-Dateien an einer zentralen Position speichern, die für alle Personen in Ihrer Cognos-Umgebung verfügbar ist. Im Folgenden sind einige Beispiele für Speicherpositionen aufgeführt, je nachdem, welche Cognos Analytics-Angebote Sie verwenden:

Wenn Sie Cognos Analytics on Cloud Hosted verwenden:
Ihr Administrator kann Ihnen Zugriff auf ein SFTP-Dropbox (SSH File Transfer Protocol) im Stammdateisystem geben.

Wenn Sie Cognos Analytics for Cloud Pak for Data oder Cognos Analytics on Demand verwenden, gehen Sie wie folgt vor:
Sie können Ihre Konfigurationsdatei in einer öffentlichen URL oder einer Cloud Object Store-Position hosten. Weitere Informationen finden Sie unter Kapitel 10, „Verwalten des Cloud-Speichers", auf Seite 243.

Gehen Sie wie folgt vor, wenn Sie Cognos Analytics on Premises oder Cognos Analytics on Cloud Hosted verwenden:
Ihre Konfigurationsdatei kann gespeichert werden

- in einer Cloud Object Store-Position (COS)
- in einer Dateisystemposition auf jedem Cognos Analytics-Anwendungsschichtserver
- auf einer Netzlaufwerkposition, auf die für jeden Cognos Analytics-Anwendungs-Tier-Server zugegriffen werden kann

Beispiele mit der Methode Sample-Parameter

Im Folgenden sind zwei Beispiele aufgeführt, die den Parameter `Sample` verwenden, um eine REST-API-Verbindung zu erstellen. Im ersten Beispiel wird ein fiktiver API-Providerverwendet. Der zweite verwendet einen realen API-Provider.

Beispiel, das einen fiktiven API-Provider verwendet

In diesem Beispiel erstellen Sie eine REST-API-Datenserververbindung zu einem API-Provider, indem Sie den Parameter `Sample` verwenden. Ihre Verbindung ruft ein `Panel` -Datenobjekt ab. Das Objekt `Panel` enthält `Listen` -Tabellen, die `Karten` -Tabellen enthalten. Sie werden Ihre neue Verbindung verwenden, um ein Datenmodul in Cognos Analytics zu erstellen, das auf das **Panel** -Schema verweist.

1. Sie gehen auf die Website des API-Anbieters und erkundigen sich nach dessen API-Anforderungen. Sie notieren sich die erforderlichen Eingaben für die API, einschließlich der URL-Syntax und der Authentifizierungsparameter.

   Sie stellen fest, dass:

   - Dass die API die OAUTH1-Authentifizierung verwendet.

     Für weitere Details: Sehen Sie sich das Thema "Authentifizierung" auf Seite 42 des *Progress ® DataDirect ® Autonomous REST Connector for JDBC™ User's Guide for Partners*an.
   - Sie möchten auf die `Panel` -API zugreifen.
   - Sie verwenden die Methode SAMPLE, um die API abzufragen.
2. Sie registrieren sich mit dem API-Service des Unternehmens und erhalten eindeutige Informationen, die Sie in Ihrem `Panel` -API-Aufruf verwenden.
   - Sie erhalten eine Panel-ID, die die Schema-Instanz identifiziert, die an Sie zurückgegeben wird.
   - Sie erhalten Ihren eigenen Sicherheitsschlüssel und Ihr eigenes Sicherheitstoken.
3. In Cognos Analytics erstellen Sie eine Datenserververbindung zu der API.
   a. Führen Sie die Schritte im Abschnitt Datenserververbindung erstellenaus, indem Sie die folgenden Werte angeben:
      - Klicken Sie im Teilfenster **Typ auswählen** auf **Progress Data Direct Autonomous REST Connection**(Progress Data Direct Autonomous REST Connection).

- Geben Sie in das Feld **JDBC URL** Folgendes ein:

```
jdbc:ibmcognos: autorest:sample= 'HTTP: //company_api_url/panel_id? fields = all &
key=your_security_key& token=your_security_token'
```

Dabei gilt::

  - Die Beispielmethode verwendet einzelne Anführungszeichen um ihren gesamten Wert.
  - Der *panel_id* wird an Sie gesendet, wenn Sie sich mit seinem API-Service registriert haben.
  - `fields=all` gibt an, dass alle Felder in den Daten zurückgegeben werden sollen.
  - `key=` und `token=` sind Präfixe für den Sicherheitsschlüssel und die Sicherheitstokenwerte, die Sie bei der Registrierung beim API-Service zugeordnet wurden.
  - Das Feld **Treiberklassenname** wird mit diesem Text automatisch ausgefüllt: `com.ibm.cognos.jdbc.autorest.AutoRESTDrive`

- Wählen Sie unter **Authentifizierungsmethode**die Option **Verbindung anonym herstellen**aus.

b. Sie speichern die neue Verbindung.

4. Überprüfen Sie, ob die Metadaten geladen wurden.
   a. Klicken Sie auf die Registerkarte **Schemas**.

      Das Schema **AUTOREST** wird in der Liste angezeigt, womit bestätigt wird, dass alle Tabellen aus dem API-Service in Cognos Analytics geladen wurden.

   b. Klicken Sie auf das Symbol 'Mehr' neben dem Schema **AUTOREST**.

      Die Namen der Tabellen werden angezeigt. Sie können diese Tabellen verwenden, um ein Datenmodul zu erstellen.

   c. Wenn Sie die Daten aktualisieren müssen, klicken Sie auf **Metadaten laden**.
5. Sie erstellen ein Datenmodul, basierend auf dem Anschluss, den Sie erstellt haben.
   a. Auf der Begrüßungsseite von Cognos Analytics klicken Sie auf **Neu** > **Datenmodul**.
   b. Im Dialogfenster **Quellen auswählen** wählen Sie das Symbol Datenserver und Schemas aus.
   c. Sie wählen den Anschluss aus, den Sie gerade erstellt haben.

      Sie werden aufgefordert, eine Verbindung auszuwählen.

   d. Wählen Sie **Anzeigeninformationen** aus und klicken Sie anschließend auf **OK**.
   e. Wählen Sie das Schema **Autorest** aus, das von Ihrer Verbindung zurückgegeben wurde.

      Automatisch generierte Tabellennamen werden angezeigt.

      Tipp: Die letzte Tabelle in der Liste hat den Namen **Konfiguration**. Wenn Sie eine Verbindung erstellen möchten, die den Parameter `Config` verwendet, können Sie Daten aus einer ähnlichen **Configuration** -Tabelle in eine angepasste Konfigurationsdatei kopieren. Weitere Informationen finden Sie unter „Beispiel mit dem Parameter 'Config'" auf Seite 43.

   f. Wählen Sie alle Tabellen in der Liste aus, und klicken Sie anschließend auf **OK**.

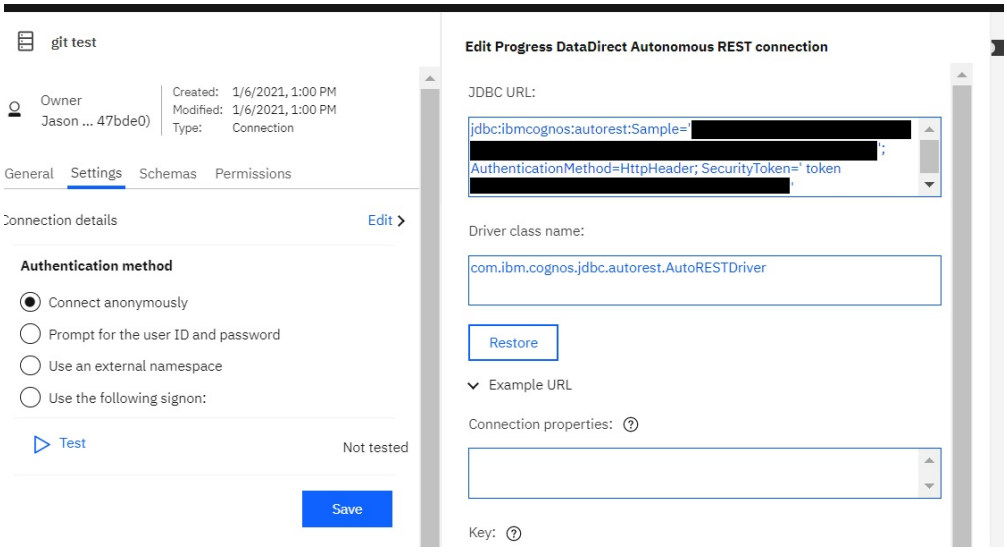
      Die Tabellen, die Sie importiert haben, werden in einer **Raster** -Ansicht angezeigt. Beachten Sie, dass eine der Tabellen die Anzeige "Info" enthält. Dieser Name wurde automatisch aus dem JDBC-URL-Wert generiert, den Sie bei der Erstellung der API-Verbindung eingegeben haben.

   g. Sie untersuchen das Datenmodul und ändern es, falls erforderlich.
   h. Klicken Sie auf **Speichern** , um das Datenmodul zu speichern.

Das Datenmodul wird an der von Ihnen ausgewählten Position erstellt.

Beispiel für die Verwendung eines realen API-Providers

Dieses Beispiel zeigt die Anzeige **Edit Progress DataDirect Autonomous REST connection** , die für eine reale Arbeitsverbindung mit GitHub konfiguriert ist. Im Feld **JDBC-URL** werden die HTTP-Position und die Token-ID aus Datenschutzgründen gelöscht. Dies wird in der folgenden Abbildung gezeigt:



Anmerkung:

- Das Feld **Authentifizierungsmethode** in der linken Anzeige wird auf **Verbindung anonym verbinden**ge-setzt. Dies liegt daran, dass die Authentifizierungsinformationen für dieses Beispiel im Feld **JDBC-URL** angegeben sind.
- Im Wert für **JDBC-URL** werden sowohl der SAMPLE -Wert als auch der `SecurityToken` -Wert durch einfache Anführungszeichen (') eingeschlossen.

Beispiel mit dem Parameter 'Config'

In diesem Beispiel erstellen Sie mit dem Parameter `Config` eine REST-API-Verbindung zu einem fiktiven API-Provider. Diese Verbindungsmethode referenziert eine Konfigurationsdatei, die mehrere Endpunkte aufruft und die Ergebnisse in ein benutzerdefiniertes Datenbankschema abbildet. Sie bearbeiten dann die Konfigurationsdatei, um den zukünftigen Datenabruf über die Verbindung zu optimieren.

Tipp: In Schritt „4” auf Seite 44 dieses Beispiels wird die Änderung der Konfigurationsdatei beschrieben, die in der Verbindung verwendet wird. Sie können das Cognos Analytics-Modellierungstool auch verwenden, um Änderungen an Objekten vorzunehmen, z. B. um Namen von Beschriftungen zu ändern.

Vorgehensweise

1. Sie verwenden eine Konfigurationsdatei, zum Beispiel `my_config.json`, um die Daten anzugeben, die vom REST-API-Service zurückgegeben werden sollen.
2. Sie speichern die Datei `my_config.json` in einer zentralen Position, die für alle Benutzer in Ihrer Cognos Analytics-Umgebung verfügbar ist.

   Weitere Informationen finden Sie unter „JSON-Dateien an einer zentralen Position speichern” auf Seite 41.
3. Sie erstellen eine Verbindung mit dem Parameter `Config` :
   a) Führen Sie die Schritte in „Herstellen einer Datenserververbindung” auf Seite 25 aus und geben Sie diese Werte an:
      - Klicken Sie im Teilfenster **Typ auswählen** auf **Progress Data Direct Autonomous REST Connection**(Progress Data Direct Autonomous REST Connection).

- Geben Sie in das Feld **JDBC-URL** Folgendes ein:

  ```
  jdbc:ibmcognos: autorest:config = "path_to_my_config.json"; ServerName=url_endpoint
  ```

  Dabei gilt::

  – *path_to_my_config.json* ist der Pfad zu Ihrer Konfigurationsdatei, die in einer zentralen Position gespeichert ist.

  – Der Pfad zu Ihrer Konfigurationsdatei wird in doppelte Anführungszeichen eingeschlossen.

  – Sie bestimmen den *url_endpoint* , indem Sie die Website des API-Providers besuchen.

  – Der *panel_id*, der Sicherheitsschlüssel und das Sicherheitstoken werden nicht explizit in den API-Aufruf eingeschlossen. Stattdessen werden sie in der Konfigurationsdatei definiert, die verschlüsselt ist.

  – Das Feld **Treiberklassenname** wird mit diesem Text automatisch ausgefüllt: `com.ibm.cognos.jdbc.autorest.AutoRESTDriver`

- Wählen Sie unter **Authentifizierungsmethode**die Option **Verbindung anonym herstellen**aus.

b) Sie speichern die neue Verbindung.

4. Sie untersuchen `my_config.json` in einem Texteditor und ändern die Datei, falls erforderlich:
   - Sie können den Schemanamen und den Panel-Namen umbenennen, um sie intuitiver zu gestalten.
   - Sie werden feststellen, dass bei Verwendung dieser Konfigurationsdatei mehrere API-Aufrufe erfolgen.
   - Wenn Sie einige Mitglieder oder Zeilen in einer Tabelle ignorieren möchten, können Sie diese mit doppelten Schrägstrichen (//) auskommentieren.
   - Für jedes Haupttabellenobjekt ersetzen Sie *tatsächliche* Werte durch einen entsprechenden *Datentyp*.
   - Sie können verschachtelte Tabellen in der Konfigurationsdatei beachten. Beispielsweise kann jede verschachtelte Tabelle als Feldgruppe, die durch ein Paar eckiger Klammern (`[]`) gekennzeichnet ist, unter der zugehörigen übergeordneten Tabelle angezeigt werden.
   - Möglicherweise möchten Sie einen ursprünglichen Tabellennamen umbenennen. Beispiel: Sie möchten `labels` in `cardLabels`umbenennen. Wenn Sie die Syntax der Konfigurationsdatei verwenden, ersetzen Sie den Code `labels` durch `labels<cardLabels>`.

   Für Details zum Ändern einer Konfigurationsdatei: Lesen Sie das Thema "Relationale Ansicht ändern" auf Seite 21 des *Progress ® DataDirect ® Autonomous REST Connector for JDBC™ User's Guide for Partners*.
5. Sie erstellen ein Datenmodul auf der Basis der Verbindung.

   Tipp: Siehe Schritt „5” auf Seite 42 in "Beispiel, das einen fiktiven API-Provider" verwendet.
6. Wählen Sie im Datenmodul die Ansicht **Beziehungen** aus.

   Die Tabellenbeziehungen werden grafisch dargestellt. Diese Beziehungen wurden in Cognos Analytics von den entsprechenden Informationen in der Konfigurationsdatei generiert.

Nächste Schritte

Sie können dieses Datenmodul als Datenquelle verwenden, wenn Sie zum Beispiel einen oder ein erstellen.

Microsoft Azure Analysis Services

Die Verbindung des Microsoft Azure Analysis Services-Datenservers wird nur lokal in IBM Cognos Analytics unter Microsoft Windows unterstützt. Befolgen Sie die folgenden Leitlinien bei der Erstellung der Datenserververbindung.

- Geben Sie die Option **Zur Eingabe der Benutzer-ID und des Kennworts auffordern** oder die Option **Die folgende Anmeldung verwenden** für die Authentifizierungsmethode an.

- Geben Sie den Servernamen, der im Microsoft Azure-Portal angezeigt wird, im Feld **Servername** an. Verwenden Sie nicht den Management-Servernamen.
- Geben Sie das Feld **Sprache** im folgenden Format an: `ll` oder `ll-cc`. Dabei ist `ll` der ISO-Sprachencode und `cc` ist die ISO-Region bzw. der Landescode. .

Weitere Informationen zu Microsoft-Anforderungen finden Sie in der Clientbibliothek für Verbindungen zu Azure Analysis Services (https://docs.microsoft.com/en-us/azure/analysis-services/analysis-services-data-providers).

Anmerkung:

- Die Treiberversion muss Microsoft Analysis Services OLE DB Provider (MSOLAP) 15.1 oder höher sein.
- Die Kompatibilitätsstufe muss 1400 oder höher sein.

Microsoft Analysis Services und Microsoft Azure Analysis Services - Sprachencode

Verwenden Sie das folgende Format im Feld **Sprache** für die Verbindung eines Microsoft Analysis Services- oder Microsoft Azure Analysis Services-Datenservers:

`ll` oder `ll-cc`. Dabei ist `ll` der ISO-Sprachencode und `cc` ist die ISO-Region bzw. der Landescode. . Die Region bzw. der Landescode ist optional.

Snowflake-Verbindungen

Sie können eine Verbindung zu Snowflake mit dem Snowflake-JDBC-Treiber so konfigurieren, dass er ein JSON Web Token (JWT) beim Authentifizieren in der Datenbank übergibt.

Führen Sie die folgenden Tasks aus, um eine Snowflake-Verbindung zu aktivieren:

1. Wählen Sie einen Identitätsprovider-Namespace aus, der Ansprüche in dem JWT zurückgeben kann, das Snowflake benötigt.
2. Konfigurieren Sie Cognos Analytics für die Verwendung des OpenID Connect-Authentifizierungsproviders.

   Weitere Informationen finden Sie im Abschnitt zum "OpenID Connect-Authentifizierungsprovider" im Handbuch *IBM Cognos Analytics - Installation und Konfiguration*.
3. Geben Sie die Verbindungseinstellungen an:
   a. Wählen Sie den OpenID Connect-Namespace aus, den Sie als Identitätsprovider konfiguriert haben.

      Tipp: Auf diese Weise kann das JWT-Token übergeben werden.
   b. Wählen Sie **Einen externen Namespace verwenden** als Authentifizierungsmethode aus.
   c. Schließen Sie das Snowflake-Name/Wert-Paar `authenticator=oauth` in die Verbindungs-URL ein.

   Weitere Informationen finden Sie unter „Herstellen einer Datenserververbindung” auf Seite 25.

Informationen zu der Snowflake-JWT-Authentifizierung finden Sie in der Snowflake-Dokumentation.

memSQL

Eine Verbindung zu MemSQL unterstützt die Verwendung des JDBC-Treibers MariaDB Connector/J. In vorherigen Cognos Analytics-Releases erforderten Verbindungen den JDBC-Treiber MySQL Connector/J.

Aufgrund von Änderungen, die in Version 8 von MySQL Connector/J eingeführt wurden. schlagen Verbindungen fehl. MemSQL empfiehlt, dass Anwendungen den JDBC-Treiber MariaDB Connector/J verwenden. Zur Konvertierung vorhandener Verbindungen für die Verwendung von MariaDB Connector/J ändern Sie die URL in das Format, das von MariaDB unterstützt wird, und ändern den Treiberklassennamen so, dass er auf den Treiberklassennamen von MariaDB verweist.

Datenkataloge

11.1.6 IBM Cognos Analytics kann mit einem Katalog wie z. B. dem Watson Knowledge Catalog (WKC) verbunden werden.

Watson Knowledge Catalog ist eine Erweiterung von IBM Cloud Pak for Data, die Self-Service-Zugriff für Fachkräfte bietet, die diese Datenassets zum Gewinnen von Erkenntnissen verwenden müssen.

Weitere Informationen finden Sie in den folgenden Abschnitten:

- Was ist IBM Watson Knowledge Catalog? (https://www.ibm.com/cloud/Watson-knowledge-catalog)
- Watson Knowledge Catalog - Übersicht (https://www.ibm.com/support/knowledgecenter/SSBRA9_addon/wsj/catalog/overview-wkc.HTML)

Ein Katalog in WKC kann auf eine oder mehrere verbundene Assets verweisen, die ihrerseits auf Datenquellen verweisen. Cognos Analytics kann die Verbindungsdetails importieren und erneut verwenden. Derzeit werden nur Details für verbundene Assets, die den von Cognos Analytics unterstützten Datenbanken entsprechen, importiert.

Hinweise zu WKC-Verbindungen in Cognos Analytics

- Cognos Analytics zeigt WKC-Schemas und -Tabellen auf die gleiche Weise an, wie es Daten für andere Typen von Datenserververbindungen anzeigt.
- Cognos Analytics-Administratoren verwalten nicht die Verbindungsdetails eines verbundenen WKC-Assets. Die Verbindungsdetails werden vom Datenbankadministrator in WKC verwaltet.
- Sie können Cognos Analytics-Verbindungen zu mehreren Katalogen erstellen.

Vorbereitende Schritte

Um eine Verbindung zu einem Watson Knowledge Catalog herzustellen, müssen Sie zuerst Ihrem Cognos-Server das WKC-Zertifikat hinzufügen. Gehen Sie dazu folgendermaßen vor:

- Folgen Sie den Schritten unter "CA-Zertifikate in IBM Cognos-Komponenten importieren" in der Veröffentlichung *IBM Cognos Analytics - Installation und Konfiguration - Handbuch*.

  Wichtig: Selbst signierte Zertifikate werden für die CA/WKC-Integration in 11.1.7 und höher nicht unterstützt. Das CPD/WKC-Zertifikat, das in Cognos Analytics importiert wird, muss von einer anerkannten Rootberechtigung signiert werden. Um zu bestätigen, dass Ihr Zertifikat von einer vertrauenswürdigen Root-Berechtigung signiert wurde, geben Sie die WKC-URL in einen Browser ein und überprüfen Sie, ob ein Vorhängeschloss links neben der URL vorhanden ist.

  Wenn Sie ein selbst signiertes Zertifikat importieren und versuchen, eine externe Katalogverbindung zu WKC zu erstellen, wird möglicherweise die folgende Nachricht angezeigt:

  MSR-WKC-2404 Verbindungszeichenfolge, Benutzername oder Kennwort nicht gültig

  Wenn Ihr Zertifikat selbst signiert ist, ersetzen Sie es durch ein vertrauenswürdiges TLS-Zertifikat, indem Sie die Schritte im Abschnitt Angepasstes TLS-Zertifikat für HTTPS-Verbindungen verwenden (https: //www.ibm.com/support/producthub/icpdata/docs/content/SSQNUZ_latest/cpd/install/https-config-openshift.html) befolgen.
- Starten Sie Ihre IBM Cognos-Services erneut.

Herstellen einer Verbindung zu einem Watson Knowledge Catalog

1. Klicken Sie auf **Verwalten** > **Datenserververbindungen**.
2. Klicken Sie im Fensterbereich **Datenserververbindungen** auf das Symbol **Datenserver hinzufügen** .

3. Wählen Sie als Typ **Externer Katalog** aus.
4. Geben Sie in der Anzeige **Externe Katalogverbindung bearbeiten** den folgenden Text in das Feld **Server-URL** ein:

   `jdbc:wkc:`*`url_for_wkc_server`*

   Dabei steht *url_for_wkc_server* für die URL der Hauptlandeseite von IBM Cloud Pak for Data für die CPD-Instanz mit installiertem WKC.

   Wenn Ihre CPD-URL beispielsweise `https://wkc-cpd.test.cloud.ibm.com`lautet, lautet der Wert für **Server-URL** wie folgt:

   ```
   jdbc:wkc:https://wkc-cpd.test.cloud.ibm.com
   ```

   Tipp: Lassen Sie das Feld **Verbindungseigenschaften** leer.
5. Wählen Sie im Abschnitt **Authentifizierungsmethode** die Option **Die folgende Anmeldung verwenden** aus.

   Tipp: Dies ist die einzig gültige Authentifizierungsmethode für einen Verbindungstyp 'Externer Katalog'.
6. Klicken Sie auf das Pluszeichen  .
7. Geben Sie auf der Registerkarte **Berechtigungsnachweise** eine gültige Watson Knowledge Catalog-Benutzer-ID und ein gültiges Kennwort ein.

   Tipp: Geben Sie einen Benutzernamen und ein Kennwort an, mit denen eine Verbindung zu WKC hergestellt werden soll. Die Benutzerberechtigungsnachweise sind die Berechtigungsnachweise, die in der CPD-Instanz definiert sind. Sie können die Benutzer-ID CPD admin oder eine andere CPD-Benutzer-ID mit Zugriff auf WKC verwenden.
8. Klicken Sie auf **Testen**, um sicherzustellen, dass die Verbindung funktioniert.
9. Klicken Sie auf **Speichern**, um die Verbindung in Cognos Analytics zu speichern.

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 2. 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.maxRowsRetrieved

Die Eigenschaft **`ibmcognos.maxRowsRetrieved`** in einer Datenserververbindung kann verwendet werden, um die maximale Anzahl von Zeilen festzulegen, die in einer SQL-Abfrage zurückgegeben werden.

Diese Eigenschaft ist nur für den dynamischen Abfragemodus (DQM) anwendbar und kann verwendet werden, um zu verhindern, dass Benutzer Abfragen ausführen, die eine große Anzahl von Zeilen vom Datenbankserver abrufen.

Verwenden Sie die folgende Syntax, um diese Eigenschaft anzugeben, wobei *N* für die maximale Anzahl von Zeilen steht, die zurückgegeben werden sollen:

```
ibmcognos.maxRowsRetrieved=N
```

Der Wert für *N* muss eine ganze Zahl größer als 0 und kleiner oder gleich 2147483647 sein.

Es wird eine Ausnahme ausgelöst, wenn ein ungültiger Wert erkannt wird. Standardmäßig wird die Anzahl der zurückgegebenen Zeilen nicht begrenzt.

Wenn Sie diese Eigenschaft nicht festlegen oder auf 0 setzen, gibt es keine Begrenzung.

Anmerkung: Wenn die abgefragte Datenbank Workload-Management-Features bietet, verwenden Sie diese Funktionen anstelle dieser Eigenschaft.

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.

Laden von Metadaten

Nachdem eine Datenserver-Verbindung hergestellt wurde, müssen Sie die Metadaten aus den Datenbankschemata oder Katalogen laden. Nur Schemata, bei denen Metadaten geladen wurden, können zum Erstellen von Datenmodulen verwendet werden. Die geladenen Metadaten werden in dem Inhaltsspeicher gespeichert.

Wenn Sie Metadaten laden, untersucht IBM Cognos Analytics die Datenserver auf Informationen, wie zum Beispiel Primär- oder Fremdschlüssel, die ungefähre Anzahl von Zeilen in jeder Tabelle oder unterschiedliche Werte in bestimmten Spalten. Auf der Grundlage dieser Informationen werden Daten für die Verwendung in Datenmodulen aufbereitet. Zum Beispiel werden Beziehungen zwischen Tabellen automatisch abgeleitet und den Eigenschaften **Aggregation** und **Nutzung** intelligente Standardeinstellungen zugeordnet. Dieser Prozess wird auch als intelligente Datenaufbereitung bezeichnet.

Informationen zu diesem Vorgang

Das Laden von Metadaten dauert bei einigen Datenserver-Schemas nicht lange, bei Schemas mit Tausenden von Tabellen kann es jedoch eine Weile dauern. Wenn das Schema Tabellen enthält, die keinen analytischen Wert besitzen, schließen Sie diese aus, sodass keine Zeit mit dem Abruf der zugehörigen Metadaten vergeudet wird.

Bei der Angabe der Ladeoptionen können Sie eine Stichprobe von statistischen Daten einbeziehen, die vom zugrunde liegenden Datenserver abgerufen wird. Diese Daten werden von der Cognos AnalyticsKI verwendet, um eine bessere Automatisierung zu ermöglichen und bessere Visualisierungsvorschläge zu machen.

Tipp: Der Begriff des Schemas in der Cognos Analytics-Benutzerschnittstelle stellt auch den Begriff des Katalogs dar. Beide Begriffe bezeichnen eine logische Klassifizierung von Datenbankobjekten.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Datenserververbindungen**.

   Im Slideout-Fenster wird eine Liste mit Datenserververbindungen angezeigt.
2. Klicken Sie im Fenster **Datenserververbindungen** auf einen Datenservernamen.

   Tipp: Stellen Sie sicher, dass die Verbindung eine relationale Datenbank darstellt.

   Das Fenster mit den Eigenschaften des Datenservers wird angezeigt. Das Fenster enthält drei Registerkarten: **Allgemein**, **Verbindungen**und **Berechtigungen**.
3. Klicken Sie auf die Registerkarte **Verbindungen** und klicken Sie dann auf den Namen der Datenserververbindung.

Das Fenster "Verbindungseigenschaften" wird angezeigt. Es enthält vier Registerkarten: **Allgemein**, **Einstellungen**, **Schemas**und **Berechtigungen**.

4. Klicken Sie auf die Registerkarte **Schemas**.

   Die Liste von Datenbankschemas wird angezeigt. Das Häkchen in der Spalte **Status** gibt an, dass das Schema zuvor geladen wurde. Die Spalte **Informationen laden** gibt an, wie viele Tabellen geladen werden. Wenn das Schema nicht geladen wird, sind diese Informationen nicht verfügbar.

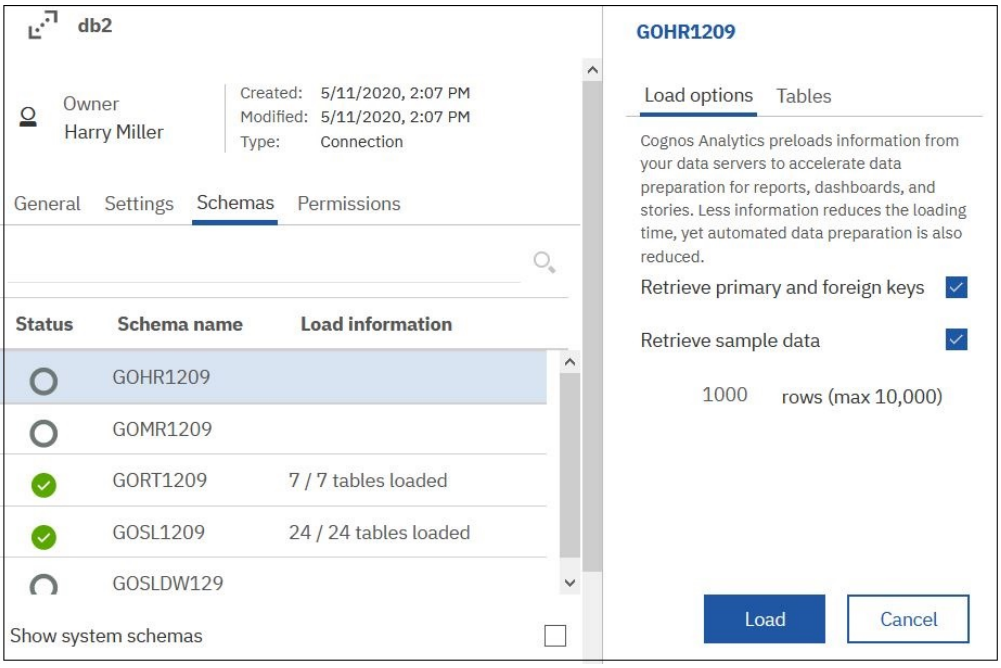
   Die Liste enthält die System- und Verwaltungsschemas für verschiedene Typen von Datenservern standardmäßig nicht. Diese Typen von Schemas werden standardmäßig nicht geladen. Das Schema PUBLIC in ORACLE wird zum Beispiel nicht angezeigt. Wählen Sie das Kontrollkästchen **Systemschemas anzeigen** aus, um die System-und Verwaltungsschemas für eine Datenserververbindung anzuzeigen.

   Tipp: Die Gruppe von System- und Verwaltungsschemas, die für bestimmte (nicht alle) Anbieter angezeigt wird, wird in der Datei *installationsposition*`\configuration\moser\import.xml` definiert.

5. Klicken Sie im Kontextmenü des Schemas ••• auf eine der folgenden Optionen:

   - **Ladeoptionen**

     Verwenden Sie diese Optionen, um anzugeben, welche Ladeoptionen ausgewählt werden sollen und welche Schematabellen geladen werden sollen.



   – Wählen Sie auf der Registerkarte **Ladeoptionen** die folgenden Kontrollkästchen aus oder löschen Sie die Auswahl. (Diese Kontrollkästchen sind standardmäßig ausgewählt):

     Primär- und Fremdschlüssel abrufen
     Aktivieren Sie dieses Kontrollkästchen, um die automatische Erkennung von Beziehungen zwischen Tabellen zu erleichtern.

     Das Deaktivieren dieses Kontrollkästchens reduziert die Zeit und den Speicherverbrauch des Systems beim Laden der Daten Es werden jedoch möglicherweise weniger Joins erstellt.

     Stichprobendaten abrufen
     Aktivieren Sie dieses Kontrollkästchen, um eine statistische Stichprobe von Daten aus jeder ausgewählten Tabelle abzurufen..

     Standardmäßig werden 1000 Zeilen der Daten pro Tabelle abgerufen. Sie können diesen Wert ändern und bis zu 10000 Zeilen angeben. Zu viele Zeilen können sich negativ auf die Systemleistung auswirken; zu wenige Zeilen erfassen möglicherweise nicht genügend Informationen.

Das Deaktivieren dieses Kontrollkästchens reduziert die Zeit und den Speicherverbrauch des Systems beim Laden der Daten und kann in manchen Situationen die richtige Wahl sein.

Weitere Informationen finden Sie unter „Datenstichprobe” auf Seite 53.

– Wählen Sie auf der Registerkarte **Tabellen** die Tabellen aus, die geladen werden sollen, oder deaktivieren Sie diese

Sie können die Tabellen ausschließen, die nicht in Ihren Dashboards oder Explorationen verwendet werden, was die Zeit und den Speicherverbrauch bei der Ausführung von Abfragen reduziert. Sie können auch Tabellen ausschließen, die Fehler verursachen, oder solche, auf die Sie nicht zugreifen können.

- **Metadaten laden**.

  Durch diese Option werden alle Tabellen im Schema unter Verwendung der Standardladeoptionen geladen.

- **Metadaten löschen**

  Diese Option ist nur verfügbar, wenn die Schema-Metadaten zuvor geladen wurden. Verwenden Sie diese Option, um die zuvor geladenen Metadaten aus dem Content Store zu entfernen. Diese Option sollte jedoch mit Vorsicht verwendet werden, da sie Berichte, Dashboards oder Explorationen unterbrechen kann, die auf Datenmodulen basieren, die das Schema verwenden, und Sicherheitsfilter aus den Datenmodulen löschen kann.

Ergebnisse

Nach Abschluss des Ladens gibt die Spalte **Status** an, dass das Schema geladen wurde. Die Spalte **Informationen laden** gibt an, wie viele Tabellen geladen werden.

Nächste Schritte

Wenn das Schema zum ersten Mal geladen wurde, kann es nun zum Erstellen von Datenmodulen verwendet werden. Wenn es sich um ein anschließendes Neuladen der Schema-Metadaten handelt, werden die Daten in den zugehörigen Datenmodulen aktualisiert.

Datenstichprobe

Datenstichproben sind ein Weg für die IBM Cognos Analytics künstliche Intelligenz (AI) von , um Informationen zu den Daten im zugrunde liegenden Datenserver zu erhalten. Diese Daten werden von der KI verwendet, um eine bessere Automatisierung zu ermöglichen und bessere Visualisierungsvorschläge zu machen.

Ohne die Beispieldaten funktionieren einige Cognos AnalyticsFunktionen nicht. Das Beziehungsdiagramm in **Explore** wird beispielsweise nur angezeigt, wenn die Beispieldaten verfügbar sind. Andernfalls wird er nicht angezeigt.

Beim Laden der Schemametadaten oder Bereicherung eines Paketskann eine Stichprobe von statistischen Daten vom zugrunde liegenden Datenserver abgerufen werden. Um diese Funktion zu aktivieren, wählen Sie das Kontrollkästchen **Beispieldaten abrufen** im zugehörigen Dialogfenster aus.

Standardmäßig werden 1000 Zeilen einer statistischen Stichprobe der Daten pro Tabelle (Abfragethema für Pakete) aus dem zugrunde liegenden Datenserver abgerufen. Diese Beispieldaten werden von der Cognos AnalyticsKI verwendet, um Eigenschaften oder "erweiterte Metadaten" zu übertragen, die die KI in ihren Automationsoptionen und Visualisierungsvorschlägen unterstützen.

Ein Beispiel für eine Eigenschaft, die aus den Beispieldaten abgeleitet werden kann, ist die ungefähre Anzahl eindeutiger Werte in jedem Feld. Diese Informationen helfen der AI, Empfehlungen zum Visualisierungstyp zu erstellen. Beispiel: Ein Balkendiagramm wird nur empfohlen, wenn nicht zu viele eindeutige Werte als Balken angezeigt werden. Ein Blasendiagramm ist für Datenfelder, die Hunderte von eindeutigen Werten aufweisen, besser geeignet.

Der Typ und die Menge der Daten, die mit der Datenstichprobe abgerufen werden, sind nicht immer identisch und werden durch die folgenden Faktoren beeinflusst:

- Die Berechtigungen des Benutzers zum Abfragen bestimmter Tabellen oder Spalten in der Tabelle.
- Datensicherheit, die die Zeilen, die der Benutzer sehen kann, Integritätsbedingungen unterliegt.
- Datenmaskierung, die die Daten ändern kann, die der Benutzer sehen kann.
- Ausdrücke können aufgrund von Makros dynamisch sein.
- Datenserververbindungen können aufgrund von Makros oder Sicherheit auf den Verbindungen dynamisch sein.

Datenstichprobe inaktivieren

Wenn Sie die Datenstichprobe für alle Tabellen im Datenserver inaktivieren möchten, inaktivieren Sie das Kontrollkästchen **Beispieldaten abrufen** in der Benutzerschnittstelle für die Metadatenladevorgänge oder die Benutzerschnittstelle für die Paketanreicherung.

Wenn die Datenstichprobe inaktiviert ist, weiß die Cognos Analytics KI von nicht so viele Merkmale zu den Daten. Sie kennt zwar noch einige Merkmale, indem sie die Metadaten des Datenservers ansieht, aber nicht so viele, wie sie wüssten, ob sie Zugriff auf die Beispieldaten hatte. Bei Verwendung des obigen Beispiels, ohne Stichprobenentnahme, kann ein Balkendiagramm auch für Datenfelder empfohlen werden, die zu viele eindeutige Werte für diesen Visualisierungstyp haben. Zusammenfassend lässt sich sagen, dass die Visualisierungs-Empfehlung ohne die aus den Beispieldaten abgeleiteten Merkmale funktioniert, aber nicht so gut funktioniert.

Im Folgenden finden Sie eine Liste der Features, die negativ beeinflusst werden, wenn die Datenstichprobe inaktiviert ist:

- Vorhersage
- Assistent
- Beziehungsdiagramm
- Entscheidungsbaumvisualisierung
- Spiral-Visualisierung
- Visualisierung der Treiberanalyse
- Sunburst Visualisierung
- Details der natürlichen Sprache
- Einblicke in Visualisierungen
- Korrelierte Einblicke
- Empfohlene Visualisierungen in Explore
- Zugehörige Visualisierungen
- Empfohlene Visualisierungen in Dashboards

Weitere Informationen finden Sie in den Anleitungen*IBM Cognos Analytics Exploration* und *Dashboards and Stories* .

Die Inaktivierung der Datenstichprobe ist in den folgenden Situationen gerechtfertigt:

- Fehler treten auf, wenn die Beispieldaten abgerufen werden.
- Die negativen Auswirkungen auf die Leistung auf das System sind zu stark.

Anstatt die Datenstichprobe vollständig zu inaktivieren, können Sie das Kontrollkästchen **Beispieldaten abrufen** auswählen, aber einige Tabellen aus dem Prozess ausschließen. Sowohl die Benutzeroberfläche zum Laden von Metadaten als auch die Benutzeroberfläche zur Paketanreicherung enthalten Optionen zum Abwählen von Tabellen. Sie können z. B. Tabellen ausschließen, die Fehler generieren. Sie können auch die Anzahl der abgerufenen Beispielzeilen reduzieren.

Referenz und Fehlerbehebung

Beim Herstellen und Verwalten von Datenserververbindungen in IBM Cognos Analytics können Probleme mit JDBC-Treibern, mit der Datenserverversionsunterstützung, mit der Authentifizierung usw. auftreten.

Die Verbindungsinformationen variieren abhängig vom jeweiligen Datenservertyp. Weitere Informationen finden Sie in der Dokumentation des Datenbankanbieters.

Warnungen des Abfrageservice in Bezug auf unbekannte Datentypen

Wenn der Abfrageservice bei der Verarbeitung von Abfragen den Datentyp Unknown (Unbekannt) feststellt, wird unter Umständen eine Warnung zurückgegeben.

Bei Verwendung des Abfrageservice ist es möglich, in Ausdrücken datenbankinterne Funktionen zu referenzieren, deren Signatur (Eingabe- und Ausgabetypen) in IBM Cognos Analytics unbekannt ist. Im Rahmen der Validierung und Planung von Abfragen werden die Datentypinformationen vom Abfrageservice überprüft. Ist ein Datentyp Unbekannt, wird unter Umständen eine Warnung zurückgegeben.

Im Zusammenhang mit dem IBM JCC-Treiber (JDBC) und Db2 gibt es ein bekanntes Problem, bei dem die erwartete Antwort von der JDBC-Methode `DatabaseMetadata.getFunctionColumns` nicht zurückgegeben wird. Folglich ist der Rückgabetyp der Funktion dem Abfrageservice aus dem Modell unbekannt, was zu einer Warnung führt.

Um dieses Problem zu umgehen, können Sie die datenbankinterne Funktion in eine andere Funktion einschließen, die dem Abfrageservice bekannt ist, wie beispielsweise CAST. Beispiel: `CAST( myUDF ( ... ) , integer )`. In diesem Fall verwendet der Abfrageservice die Datentypinformationen, die von dieser Funktion zurückgegeben werden.

Anmerkung: Es ist nicht obligatorisch, eine Funktion in ein Framework Manager-Modell zu importieren, bevor eine Funktion in einem Ausdruck referenziert werden kann. Durch das Importieren einer Funktion werden die Metadaten zur Funktion (einschließlich ihres Datentyps) dem Abfrageservice verfügbar gemacht.

JDBC-Treiber von Cloudera Impala

IBM Cognos Analytics unterstützt Verbindungen zu Cloudera Impala-Datenservern, die JDBC-Treiber der Version 2.5.34 und höher verwenden. JDBC-Treiberversionen vor Version 2.5.34 werden nicht unterstützt.

Beim Herstellen einer Verbindung zu Cloudera Impala überprüft die Abfrageengine die Version des JDBC-Treibers. Bei Versionen vor Version 2.5.34 wird eine Fehlernachricht zurückgegeben.

Ersetzen Sie zur Vermeidung potenzieller Probleme ältere JDBC-Treiberversionen für Impala in der Cognos Analytics-Umgebung durch neuere Versionen. Der Treiber kann von der Cloudera-Website (www.cloudera.com/downloads/connectors/impala/jdbc/2-5-34.html) heruntergeladen werden. Weitere Informationen finden Sie in der Cloudera-Dokumentation.

Blockierte Abfragen in der Pivotal-HDB-Engine

Aufgrund eines Fehlers im Pivotal-Optimierungsprogramm können Abfragen in der Pivotal-HDB-Engine blockiert werden.

Zum Lösen des Problems kann der Pivotal-Administrator die Server-Standardwerte ändern oder den folgenden Befehlsblock für die Verbindung in IBM Cognos Administration hinzufügen.

```
<commandBlock>
  <commands>
   <sqlCommand>
    <sql>select disable_xform('CXformExpandNAryJoinDP')</sql>
   </sqlCommand>
  </commands>
</commandBlock>
```

Wenn in HDB eine Tabelle mit Partitionierung erstellt wurde, gibt der Pivotal-JDBC-Treiber Metadaten für jede Partition der Tabelle zurück. Derzeit besteht in der Pivotal-Software keine Möglichkeit, das Zurückgeben dieser zusätzlichen Metadaten zu verhindern. Ein Modellierungsprogramm in IBM Cognos Analytics muss diese zusätzlichen Metadaten für die einwandfreie Ausführung von Abfragen nicht einbeziehen.

Denodo 5.5- und Denodo 6.0-Datenserver

Die Denodo 5.5- und Denodo 6.0-Datenservertypen werden über den Denodo-JDBC-Treiber unterstützt.

Die unterstützte Mindestversion von Denodo 5.5 ist die Aktualisierung 20160322 mit angewendetem Denodo-Hotfix #26682. Vorgängerversionen von Denodo 5.5 werden nicht unterstützt.

Das erste Release von Denodo 6.0 GA erfordert die Anwendung des Hotfix #26681.

Denodo benötigt einen JDBC-Treiber der Version 6.0 für den Zugriff auf einen Server der Version 6.0 und einen JDBC-Treiber der Version 5.5 für den Zugriff auf einen Server der Version 5.5.

JDBC-Treiber der Denodo-Version 5.5 verhindern die Herstellung von Verbindungen zu einem Server der Version 6.0 nicht. Tritt eine solche Situation auf, löst der Server der Version 6.0 möglicherweise Ausnahmebedingungen aus, wenn Abfragen ausgeführt werden oder wenn versucht wird, Metadaten zu importieren.

In Cognos Analytics nicht mehr unterstützte Datenserver

Die Liste der unterstützten Datenserver wird fortlaufend ausgewertet. Es werden neue Datenserver hinzugefügt, und einige der zuvor unterstützten Datenserver werden entfernt.

Alle Datenserververbindungen, die in früheren Releases von Cognos Analytics definiert wurden, verbleiben im Content Store, bis sie manuell gelöscht oder ggf. in einen unterstützten Typ geändert werden. Diese Verbindungen sind in den Administrationsschnittstellen sichtbar. Wenn solche Verbindungen in IBM Cognos Administration geöffnet werden, werden sie im Verbindungseditor vom Typ **Anderer Typ** angezeigt. Dieser Verbindungseditor stellt eine eingeschränkte Schnittstelle zum Anzeigen oder Bearbeiten der Verbindungen sowie für den Zugriff auf die zugehörigen Anmeldungen bereit.

Jede Datenserververbindung im Content Store wird durch eine Zeichenfolge mit verschiedenen benutzerdefinierten Namen und Werten dargestellt. Diese Zeichenfolge ist in den Verbindungseditoren in Cognos Analytics sichtbar. Beim Testen einer Verbindung wird beispielsweise die folgende Zeichenfolge angezeigt:

```
^User ID:^?Password:;LOCAL;PG;DSN=MyDataSourceName;
UID=%s;PWD=%s;MyODBCDSN@ASYNC=0@0/0@COLSEQ=
```

Der Verbindungstyp wird in der Zeichenfolge nach dem Wert LOCAL angezeigt. Im oben genannten Beispiel ist der Verbindungstyp PG.

Wenn Ihre aktuelle Version von Cognos Analytics Verbindungen zu Datenservern verwendet, die nicht mehr unterstützt werden, können Sie in einigen Fällen die Verbindungen in die unterstützten Typen ändern.

Cognos Analytics 11.1.3

Der Pivotal HDB-Datenserver wird in Cognos Analytics nicht mehr unterstützt.

Der zugehörige Datenservertyp in der Verwaltungsschnittstelle, **Pivotal Greenplum und HDB**, wird in **Pivotal Greenplum** geändert.

Cognos Analytics 11.0.8

Die folgenden Datenserver werden ab Release 11.0.8 nicht mehr unterstützt:

- Hitachi Advanced Data Binder Platform (JDBC)
- IBM Domino (JDBC)
- MongoDB Connector for BI Version 1

  Aktualisieren Sie etwaige Verbindungen für Version 1 auf die Verwendung von MongoDB Connector for BI Version 2.2.1. Aktualisieren Sie außerdem vorhandene Cognos-Modelle, während eine Verbindung mit Version 2.2.1 besteht. Auf diese Weise wird sichergestellt, dass die Modellmetadaten Unterschiede in Datentypen und Skalierung widerspiegeln, die in MongoDB Connector for BI 2.2.1 eingeführt wurden.

Cognos Analytics 11.0.6

Die folgenden Datenserver werden ab Release 11.0.6 nicht mehr unterstützt:

- Actian Matrix (ODBC und JDBC)

  Generische ODBC-Verbindungstypen können verwendet werden, um auf einen ODBC-Datenquellennamen zu verweisen, der einen ODBC-Treiber unter Microsoft Windows-Betriebssystemen für den Zugriff auf einen Actian Matrix-Server verwendet. Sie können keine vorhandene JDBC-Verbindung verwenden.

- Actian Vector (ODBC)

  Generische ODBC-Verbindungstypen können verwendet werden, um auf einen ODBC-Datenquellennamen zu verweisen, der einen ODBC-Treiber unter Microsoft Windows-Betriebssystemen für den Zugriff auf einen Actian Vector-Server verwendet.

- IBM® IMS™ (JDBC)

Cognos Analytics 11.0.3

Die folgenden Datenserver werden ab Release 11.0.3 nicht mehr unterstützt:

- IBM Cognos Finance - Verbindungstyp CL
- Microsoft SQL Server Analysis Services 2005 und 2008 (ODBO) - Verbindungstypen YK und M8

  Anwendungen unter Windows-Betriebssystemen sollten den ODBO-Client verwenden, der mit der unterstützten Version von Microsoft Analysis Services freigegeben wurde. Anwendungen auf anderen Plattformen (nicht Windows) können eine XMLA-Verbindung (Verbindungstyp X8) verwenden. Die ODBO-Clients, die mit SQL Server Analysis Services 2005, 2008 und 2008 R2 freigegeben wurden, werden nicht mehr unterstützt. Die Verbindungen für die Versionen 2012 (Verbindungstyp M12) und 2014 (Verbindungstyp M14) werden beide unterstützt. Neue Verbindungen, die auf 2012- oder 2014-Clients verweisen, dürfen nur für die Versionen 2012 und 2014 der entsprechenden SQL Server Analysis Services-Server verwendet werden.

  Ab Cognos Analytics 11.0.0 unterstützen nur Server mit dem dynamischen Abfragemodus SQL Server Analysis Services. Der kompatible Abfragemodus bietet keine Unterstützung für SQL Server Analysis Services.

- Microsoft SQL Server 2005 und 2008 Native Clients und OLE DB (Verbindungstyp OL und Provider=SQLNCLI oder SQLNCLI10)

  Ältere Versionen der Microsoft SQL Server-Clientbibliotheken werden nicht mehr unterstützt (https://msdn.microsoft.com/en-us/library/cc280510.aspx). Für Anwendungen, die über OLE DB auf SQL Server zugreifen müssen, können Sie Native Client-Verbindungen verwenden, die `Provider=SQLNCLI11` enthalten. Diese Verbindungen sind parallel zur aktuellen SQL Server Native Client Version 11, die mit SQL Server 2016, 2014 und 2012 unterstützt wird. Alternativ können Verbindungen verwendet werden, die den Microsoft-ODBC-Treiber für SQL Server verwenden.

- SAP ECC

Cognos Analytics 11.0.2

Die folgenden Datenserver werden ab Release 11.0.2 nicht mehr unterstützt:

- Composite (ODBC)

  Composite (Verbindungstyp CS): Generische ODBC-Verbindungstypen (OD) können verwendet werden, um auf einen ODBC-Datenquellennamen zu verweisen, der möglicherweise einen ODBC-Treiber unter Windows-Betriebssystemen für den Zugriff auf Siebel-Server verwendet. Der dynamische Abfragemodus unterstützt mehrere Technologien, zum Beispiel Cisco Information Server und Denodo über JDBC, die potenziell zum Bereitstellen von föderiertem Zugriff auf Siebel-Systeme verwendet werden können.

- IBM Cognos Now! - Real-time Monitoring-Cube (Verbindungstyp LA)

  Es steht kein alternativer Verbindungstyp zur Verfügung.

- IBM Cognos Planning - Series 7 (Verbindungstyp CR)

Es steht kein alternativer Verbindungstyp zur Verfügung.

- IBM Cognos Virtual View Manager (ODBC)
- IBM Red Brick® (ODBC)
- Progress OpenEdge (ODBC)
- Siebel
- Sybase Adaptive Server Enterprise (CT-Lib)

Fehler im Zusammenhang mit nicht übereinstimmenden SQL- und Java-Datentypen

Eine Tabellenspalte verwendet möglicherweise einen Anbieterdatentyp, den der JDBC-Treiber nicht direkt unterstützt, sodass er versucht, ihn als anderen Datentyp wie zum Beispiel VARCHAR zurückzugeben.

Eine Tabelle enthält zum Beispiel eine Spalte vom Typ ARRAY und eine Spalte vom Typ STRUCT, die der JDBC-Treiber als Datentyp VARCHAR beschreibt. Effektiv werden für IBM Cognos Analytics diese Spalten und VARCHAR-Datentypen sowie alle Operationen unterstützt, die der Anbieter unterstützt und die einen Datentyp VARCHAR verwenden. Cognos Analytics könnte vielleicht eine SQL-Anweisung generieren, die Operationen wie zum Beispiel COUNT, DISTINCT oder ORDER BY enthält, die auf solche Spalten verweisen. Die Anweisung wird möglicherweise nicht ausgeführt, wenn der Anbieter diese Operationen für den Datentyp der Spalte (z. B. ARRAY) nicht unterstützt.

Diese Typen von Fehlern können auftreten, wenn die beiden folgenden Bedingungen zutreffen:

- Sie importieren Schemametadaten aus einer Datenbank, um zum Beispiel Datenmodule zu erstellen.
- Die Optionen zum Abrufen von Beispieldaten sind aktiviert.

Weitere Informationen finden Sie unter „Laden von Metadaten” auf Seite 51. Ähnliche Fehler können auftreten, wenn Sie Modellabfragesubjekte in Framework Manager erstellen und testen.

Wenden Sie die folgenden Lösungen an, um Fehler im Zusammenhang mit nicht übereinstimmenden Datentypen zu vermeiden:

- Lesen Sie die Dokumentation der Anbieter zu den entsprechenden Datenbanken, um herauszufinden, wie ein JDBC-Treiber die SQL-Datentypen definiert, die von der Datenbank unterstützt werden.
- Definieren Sie datenbankinterne Ansichten oder Ausdrücke, die die nicht übereinstimmenden Datentypen in Typen konvertieren, die von Cognos Analytics erkannt werden.

  Weitere Informationen finden Sie in "Unbekannte Typen" in der Veröffentlichung *IBM Cognos Analytics - Datenmodellierung*.

Aktualisierungen nach Release

Cognos Analytics unterstützt zahlreiche unterschiedliche Datenserver. In den unterschiedlichen Releases werden Datenserver hinzugefügt, geändert oder entfernt.

Eine aktuelle Liste der Datenserver, die für bestimmte Versionen von Cognos Analytics unterstützt werden, finden Sie auf der Seite IBM Cognos Analytics 11.1.x Unterstützte Softwareumgebungen. Klicken Sie im Abschnitt für das entsprechende Release, zum Beispiel 11.1.3, auf einen der folgenden Links, um einen detaillierten Bericht über unterstützte Datenquellen anzuzeigen:

- Klicken Sie unter **Requirements by type** (Anforderungen nach Typ) auf den Link **Software**. Klicken Sie auf der Registerkarte **Supported Software** (Unterstützte Software) auf den Abschnitt **Data Sources** (Datenquellen). Daraufhin werden alle unterstützten Datenquellen in einer Tabelle angezeigt.
- Klicken Sie unter **Requirements by platform** (Anforderungen nach Plattform) auf den Namen des entsprechenden Betriebssystems, zum Beispiel **Linux**. Klicken Sie auf der Registerkarte **Supported Software** (Unterstützte Software) auf den Abschnitt **Data Sources** (Datenquellen). Daraufhin werden alle Datenquellen, die für das ausgewählte Betriebssystem unterstützt werden, in einer Tabelle aufgelistet.

Cognos Analytics 11.1.7 - neue Features

IBM Cognos Analytics unterstützt Microsoft Analysis Services 2019-Verbindungen und die JWT-Authentifizierung mit Db2-Datenservern.

Microsoft Analysis Services 2019 (ODBO und XMLA)

Cognos Analytics unterstützt den Microsoft Analysis Services 2019-Datenserver (ODBO und XMLA).

Vorhandene Verbindungen, die auf diesen Server versetzt werden, verlieren möglicherweise ihre Anmeldungen.

Berichte, die für Vorgängerversionen des Datenservers erstellt wurden, funktionieren weiterhin, nachdem sie auf die Verwendung des neuen Clients und des neuen Servers umgestellt wurden. Die Client- und Serverversionen müssen übereinstimmen.

Ähnlich wie bei anderen MSOLAP-Versionen für Microsoft Analysis Services muss der MSOLAP-Client für Microsoft Analysis Services an derselben Position wie der Berichtsserver installiert werden. Für diese Version von Microsoft Analysis Services ist der MSOLAP-Client der Version 15 erforderlich.

Zum Erstellen einer Verbindung zum neuen Datenserver über die Verwaltungsschnittstelle unter **Verwalten** > **Datenserververbindungen** wählen Sie zunächst den generischen Datenservertyp **Microsoft Analysis Services** und anschließend **2019** aus.

Unterstützung für die JWT-Authentifizierung mit Db2-Datenserververbindungen

Eine Verbindung zu einem Db2-Datenserver, der den IBM JCC-JDBC-Treiber verwendet, kann so konfiguriert werden, dass bei der Authentifizierung ein JSON-Web-Token (JWT) an die Datenbank übergeben wird.

Um diese Funktionalität mit einer Db2-Datenserververbindung verwenden zu können, muss Cognos Analytics zur Verwendung eines OpenID Connect-Authentifizierungsproviders konfiguriert werden. Zur Bereitstellung des Tokens müssen die Verbindungseinstellungen den OpenID Connect-Namespace angeben, der als Identitätsprovider konfiguriert wurde. Der Namespace des Identitätsproviders muss in der Lage sein, Anforderungen (Claims) im JWT zurückzugeben, die für Db2 erforderlich sind.

Wählen Sie bei der Einrichtung der Db2-Datenserververbindung die Authentifizierungsmethode **Externen Namespace verwenden** aus. Weitere Informationen finden Sie im Abschnitt "Datenserververbindung erstellen" in der Veröffentlichung *IBM Cognos Analytics Verwaltung*.

Informationen zur Konfiguration eines OpenID-Authentifizierungsproviders finden Sie unter "OpenID Connect-Authentifizierungsprovider" in *IBM Cognos Analytics Installation und Konfiguration - Handbuch*.

Informationen dazu, welche Db2- und IBM JCC-Versionen die JWT-Authentifizierung unterstützen, finden Sie in der entsprechenden Dokumentation zu Db2 und IBM JCC.

Cognos Analytics 11.1.5 - Neue und geänderte Features

Der **Microsoft Azure Analysis Services**-Datenserver wurde hinzugefügt und ein neuer Name für die Standardtreiberklasse wurde für die **Google BigQuery**-Verbindungen eingeführt.

Microsoft Azure Analysis Services-Datenserver

Die Verbindungen des **Microsoft Azure Analysis Services**-Datenservers werden nur lokal in IBM Cognos Analytics unter Microsoft Windows unterstützt.

Änderungen an den Verbindungen für den Google BigQuery-Datenserver

Neue Verbindungen für den **Google BigQuery**-Datenserver in Cognos Analytics verwenden standardmäßig den Treiberklassennamen `com.simba.googlebigquery.jdbc42.Driver`.

Vor der Einführung des JDBC-Treibers für BigQuery der Version 1.2.2.1004 stellte Google zwei JDBC-Treiber für BigQuery bereit, die jeweils einen anderen Treiberklassennamen verwendeten. Neue Verbindun-

gen für **Google BigQuery** in Cognos Analytics verwendeten standardmäßig den Treiberklassennamen `com.simba.googlebigquery.jdbc41.Driver`.

Ab Version 1.2.2.1004 stellt Google nur noch einen JDBC-Treiber für BigQuery bereit, der den Treiberklassennamen `com.simba.googlebigquery.jdbc42.Driver` referenziert. Neue Verbindungen zu **Google BigQuery** in Cognos Analytics verwenden jetzt diesen Treiberklassennamen standardmäßig.

Wenn Sie bestehende Verbindungen zu **Google BigQuery** haben, die auf den Treiberklassennamen `com.simba.googlebigquery.jdbc41.Driver` verweisen, müssen Sie diese in den Namen `com.simba.googlebigquery.jdbc42.Driver` aktualisieren, um den JDBC-Treiber für BigQuery der Version 1.2.2.1004 oder höher zu verwenden.

Cognos Analytics 11.1.4 - neue und geänderte Features

Der **IBM Weather Company**-Datenserver wurde hinzugefügt und an den Datenservern für **Presto** und **Salesforce** wurden Änderungen vorgenommen.

IBM Weather Company-Datenserver

Verwenden Sie den **IBM Weather Company**-Datenserver, um The Weather Company-Daten für die Verwendung in Cognos Analytics verfügbar zu machen.

Namensänderung des Presto-JDBC-Treibers

Der **Presto**-Treiberklassenname für Version 300 und höher wurde von `com.facebook.presto.jdbc.PrestoDriver` in `io.prestosql.jdbc.PrestoDriver` geändert. Wenn Sie die Verwendung eines älteren Treibers wie Version 215 oder 214 vorziehen, müssen Sie den Treiberklassennamen manuell in `com.facebook.presto.jdbc.PrestoDriver` zurück ändern.

Änderung der Verbindungs-URL für Salesforce

Für die Verbindung zum Salesforce-Datenserver wird jetzt die URL `https://login.salesforce.com` verwendet.

Wenn Ihre Cognos Analytics-Umgebung eine Verbindung zu einem Salesforce-Datenserver umfasst, müssen Sie den URL-Endpunkt manuell in `https://login.salesforce.com` aktualisieren.

Weitere Informationen enthält der folgende Salesforce-Artikel: Salesforce.com API Endpoint retirement.

Cognos Analytics 11.1.3 - neue und geänderte Features

Die Änderungen betreffen Pivotal Greenplum- und SAP BW-Datenserververbindungen sowie Verbindungen, die JDBC-Treiber des Typs 2 verwenden.

Herstellen einer Verbindung zu einem Open-Source-Greenplum-Server mithilfe des PostgreSQL-JDBC-Treibers

Sie können mit dem PostgreSQL-JDBC-Treiber eine Verbindung zu einem Open-Source-Pivotal Greenplum-Server herstellen.

Verwenden Sie zum Erstellen einer Datenserververbindung zu einem Open-Source-Greenplum-Server der Version 5 oder höher den JDBC-Treiber und Verbindungseditor von **PostgreSQL**. Beim Test der Verbindung in den Verwaltungsschnittstellen wird der Untertyp 'Greenplum' angezeigt, wenn die Verbindung erfolgreich ist.

Verwenden Sie zum Erstellen einer Datenserververbindung zu einem proprietären Greenplum-Server den JDBC-Treiber und Verbindungseditor von **Pivotal Greenplum**.

Für SAP BW-Datenserververbindungen ist der SAP BW 7.5-Client erforderlich.

Der SAP-NetWeaver-RFC-Library 7.20-Client, der bei früheren Versionen von Cognos Analytics verwendet wurde, wird nicht mehr unterstützt. SAP NetWeaver RFC Library 7.50 ist nun die unterstützte Bibliothek.

Geänderte Position für Bibliotheken für JDBC-Treiber des Typs 2

Wenn Sie JDBC-Treiber des Typs 2 verwenden, müssen Sie die zugehörigen Nicht-JAVA-Bibliotheken in das Cognos Analytics-Verzeichnis *Installationsposition*\drivers kopieren.

In früheren Releases wurde das Verzeichnis *Installationsposition*\BIN64 zum Speichern der Bibliotheken verwendet.

Diese Änderung ist eine Folge davon, dass java.library.path jetzt das Verzeichnis *Installationsposition*\drivers im Pfad verwendet.

JDBC-Treiber des Typs 2 können weiterhin mit SQL Server- und Oracle-Datenbanken verwendet werden.

Cognos Analytics 11.1.2 - neue Features

IBM Cognos Analytics unterstützt zwei neue Versionen von Microsoft Analysis Services-Datenservern sowie die JWT-Authentifizierung mit dem SAP HANA-Datenserver.

Microsoft Analysis Services (HTTP XMLA)

Cognos Analytics unterstützt den Datenserver Microsoft Analysis Services (HTTP XMLA).

Vorhandene Verbindungen zu Microsoft Analysis Services 2017-Servern funktionieren weiterhin. Berichte, die für Vorgängerversionen des Servers erstellt wurden, funktionieren, nachdem sie auf die Verwendung des neuen Servers umgestellt wurden.

Zum Erstellen einer Verbindung zu dem neuen Datenserver über die Verwaltungsschnittstelle unter **Verwalten** > **Datenserververbindungen** wählen Sie den generischen Datenservertyp **Microsoft Analysis Services** und anschließend **HTTP XMLA** aus. Wenn Sie die Verbindung über die Schnittstelle unter **Verwalten** > **Administrationskonsole** erstellen, ist die Option **Microsoft Analysis Services (HTTP XMLA)** in der Liste der Datenservertypen verfügbar.

Microsoft Analysis Services 2017 (ODBO)

Cognos Analytics unterstützt den Datenserver Microsoft Analysis Services 2017 (ODBO).

Vorhandene Verbindungen, die auf diesen Server versetzt werden, verlieren möglicherweise ihre Anmeldungen.

Berichte, die für Vorgängerversionen des Datenservers erstellt wurden, funktionieren weiterhin, nachdem sie auf die Verwendung des neuen Clients und des neuen Servers umgestellt wurden. Die Client- und Serverversionen müssen übereinstimmen.

Ähnlich wie bei anderen MSOLAP-Versionen für Microsoft Analysis Services muss der MSOLAP-Client für Microsoft Analysis Services an derselben Position wie der Berichtsserver installiert werden. Für diese Version von Microsoft Analysis Services ist der MSOLAP-Client der Version 14 erforderlich.

Zum Erstellen einer Verbindung zu dem neuen Datenserver über die Verwaltungsschnittstelle unter **Verwalten** > **Datenserververbindungen** wählen Sie den generischen Datenservertyp **Microsoft Analysis Services** und anschließend **2017** aus. Wenn Sie die Verbindung über die Schnittstelle unter **Verwalten** > **Administrationskonsole** erstellen, ist die Option **Microsoft Analysis Services 2017 (ODBO)** in der Liste der Datenservertypen verfügbar.

Unterstützung für die JWT-Authentifizierung mit SAP HANA-Datenserververbindungen

Eine Verbindung zu einem SAP HANA-Datenserver, der den SAP HANA-JDBC-Treiber verwendet, kann so konfiguriert werden, dass sie bei der Authentifizierung ein JSON-Web-Token (JWT) an die Datenbank übergibt.

Zur Verwendung dieser Funktionalität mit einer SAP HANA-Datenserververbindung muss Cognos Analytics zur Verwendung eines OpenID Connect-Authentifizierungsproviders konfiguriert werden. Zur Bereitstellung des Tokens müssen die Verbindungseinstellungen den OpenID Connect-Namespace angeben, der als Identitätsprovider konfiguriert wurde. Der Namespace des Identitätsproviders muss in der Lage sein, Anforderungen (Claims) im JWT zurückzugeben, die für SAP HANA erforderlich sind.

Wählen Sie bei der Einrichtung der SAP HANA-Datenserververbindung die Authentifizierungsmethode **Externen Namespace verwenden** aus. Weitere Informationen finden Sie unter Herstellen einer Datenserververbindung..

Informationen zur Konfiguration eines OpenID-Authentifizierungsproviders finden Sie unter "OpenID Connect-Authentifizierungsprovider" in *IBM Cognos Analytics Installation und Konfiguration - Handbuch*.

Cognos Analytics 11.0.9 - neue und geänderte Features

Durch die Änderungen verbessert sich die IBM Cognos Analytics-Serverleistung und die Kompatibilität mit unterstützten Datenbankprodukten wird sichergestellt.

Teradata-JDBC-Verbindungen - verbesserte Abfrageparallelität

Der dynamischer Abfragemodus wurde entsprechend geändert um sicherzustellen, dass nur jeweils eine Abfrage für eine Teradata-JDBC-Verbindung ausgeführt werden kann. Durch diese Änderung wird die Abfrageparallelität verbessert. Dies ist im Abschnitt für Multithreading in der Veröffentlichung Teradata JDBC Driver Reference (https://teradata-docs.s3.amazonaws.com/doc/connectivity/jdbc/reference/current/jdbcug_chapter_2.html#BGBEFIH4) beschrieben.

Datenbankadministratoren, die die Datenbankauslastung überwachen, bemerken möglicherweise einen Zunahme der Anzahl von Datenbankverbindungen im Vergleich zu früheren Releases von Cognos Analytics.

Snowflake-Verbindungen - geänderter Treiberklassenname

In früheren Releases von Cognos Analytics lautete der standardmäßige Treiberklassenname für neue Snowflake-Verbindungen `com.snowflake.client.jdbc.SnowflakeDriver`. Ab Cognos Analytics Version 11.0.9 lautet der standardmäßige Treiberklassenname für neue Snowflake-Verbindungen `net.snowflake.client.jdbc.SnowflakeDriver`.

Bestehende Verbindungen werden weiterhin die Snowflake-Treiberklasse `com.snowflake.client.jdbc.SnowflakeDriver` referenzieren. Wenn Snowflake diesen Klassennamen vom Treiber entfernt, muss für diese Verbindungen die Eigenschaft **Treiberklassenname** in `net.snowflake.client.jdbc.SnowflakeDriver` geändert werden.

Tipp: Wählen Sie zum Bearbeiten einer Datenserververbindung **Verwalten** > **Administrationskonsole** aus. Wählen Sie auf der Registerkarte **Konfiguration** die Option **Datenquellenverbindungen** aus. Suchen Sie die Datenserververbindung und öffnen Sie sie. Sie können bestehende Verbindungen nicht über **Verwalten** > **Datenserververbindungen** bearbeiten.

Amazon Redshift-Verbindungen - geänderter Treiberklassename

In früheren Releases von Cognos Analytics lautete der standardmäßige Treiberklassenname für neue Amazon Redshift-Verbindungen `com.amazon.redshift.jdbc41.Driver`. Hierfür war die Datei `RedshiftJDBC41.*.jar` erforderlich.

Ab Cognos Analytics Version 11.0.9 lautet der standardmäßige Treiberklassenname für neue Amazon Redshift-Verbindungen `com.amazon.redshift.jdbc.Driver`. Dieser Treiberklassenname wird

von Amazon-JDBC-Treiber Version 1.2.1 oder höher verwendet. Die zugehörige Treiberdatei ist `RedshiftJDBC.jar`.

Sie können bestehende Verbindungen aktualisieren, indem Sie die Eigenschaft **Treiberklassenname** in `com.amazon.redshift.jdbc.Driver` ändern.

Tipp: Wählen Sie zum Bearbeiten einer Datenserververbindung **Verwalten** > **Administrationskonsole** aus. Wählen Sie auf der Registerkarte **Konfiguration** die Option **Datenquellenverbindungen** aus. Suchen Sie die Datenserververbindung und öffnen Sie sie. Sie können bestehende Verbindungen nicht über **Verwalten** > **Datenserververbindungen** bearbeiten.

PostgreSQL-Verbindungen können mit Amazon Aurora PostgreSQL verwendet werden

Ab diesem Release können Sie den vorhandenen PostgreSQL-Verbindungseditor und JDBC-Treiber verwenden, um Datenserververbindungen mit Amazon Aurora PostgreSQL zu erstellen und zu verwalten.

Cognos Analytics 11.0.8 - neue Features

In IBM Cognos Analytics wurde Unterstützung für die folgenden Datenserver hinzugefügt: MongoDB Connector for BI 2.2.1, Spark SQL 2.1 Thrift-Server, Azure SQL Data Warehouse, Amazon Redshift und Amazon Athena.

MongoDB Connector for BI 2.2.1

Cognos Analytics unterstützt MongoDB Connector for BI Version 2.2.1 durch den JDBC-Treiber für MySQL, der für MongoDB erforderlich ist. MongoDB Connector for BI 2.2.1 verwendet nicht den JDBC-Treiber für Postgres oder Servertechnologie für den Zugriff auf MongoDB 3.x-Server.

MongoDB Connector for BI Version 1 wird nicht mehr unterstützt. Aktualisieren Sie etwaige Verbindungen von Version 1 in die Verwendung der neuen Version. Aktualisieren Sie außerdem vorhandene Cognos-Modelle, während eine Verbindung mit Version 2.2.1 besteht. Auf diese Weise wird sichergestellt, dass die Modellmetadaten Unterschiede in Datentypen und Skalierung widerspiegeln, die in MongoDB Connector for BI 2.2.1 eingeführt wurden.

Spark SQL 2.1 Thrift-Server

Cognos Analytics unterstützt den Spark SQL 2.1 Thrift-Server durch den JDBC-Treiber SIMBA (Magnitude) für Spark SQL.

Azure SQL Data Warehouse

Verbindungen zu Azure SQL Data Warehouse werden unter Verwendung des Microsoft SQL Server-Verbindungseditors verwaltet.

Amazon Redshift

Standardmäßig müssen die Benutzer von Amazon Redshift eine Version der Datei `RedshiftJDBC41*.jar` in das Cognos Analytics-Verzeichnis *`Installationsposition`*`\drivers` kopieren. Da keine Anforderung zur Verwendung eines 4.0- oder 4.2-Treibers besteht, können Sie den standardmäßigen Treiberklassennamen so bearbeiten, dass er den von Amazon unterstützten Treiberklassennamen entspricht. JDBC-Treiber für Amazon unterstützen ab Version 1.2.1 den generischen Treiber `com.amazon.redshift.jdbc`. Dieser Treiber kann anstelle der vorherigen Treiberklassennamen verwendet werden.

Amazon Athena

Cognos Analytics unterstützt Amazon Athena durch den JDBC-Treiber für Amazon Athena. Für eine Verbindung muss eine gültige Amazon S3-Position unter Verwendung der Amazon Athena-Verbindungseigenschaft s3_staging_dir angegeben werden, von der der Treiber Abfrageergebnisse abruft.

Cognos Analytics 11.0.7 - neue und geänderte Features

MemSQL und Presto werden als unterstützte Datenservertypen hinzugefügt und MariaDB beinhaltet einen eigenen Verbindungseditor.

MemSQL

Ab diesem Release werden MemSQL-Datenservertypen unterstützt. Verwenden Sie zum Verwalten einer Verbindung für diesen Datenserver den Verbindungstyp MySQL und den JDBC-Treiber Connector/J.

Presto

Ab diesem Release werden Presto-Datenservertypen (Version 0.167 und höher) unterstützt. Es können die JDBC-Treiber von Presto und von Teradata Presto verwendet werden. Verbindungen zu diesem Datenserver werden abhängig vom verwendeten JDBC-Treiber durch Verwendung des Presto- oder Teradata Presto-Verbindungseditors verwaltet.

Tipp: Die aktuellen Releases von Presto bieten begrenzte Unterstützung für Zeichentypen mit fester Länge (CHAR). Die Verwendung solcher Typen kann zu falschen Ergebnissen führen. Sie können diese Einschränkung umgehen, indem Sie Ausdrücke erstellen, die Zeichentypen variabler Länge verwenden.

MariaDB

Ab Cognos Analytics 11.0.7, verfügt der MariaDB-Datenserver über einen eigenen Verbindungseditor, der den JDBC-Treiber Connector/J für MariaDB unterstützt.

In früheren Releases wurden Verbindungen zu MariaDB unter Verwendung des Verbindungseditors MySQL und des JDBC-Treibers Connector/J für MySQL definiert.

Der MariaDB-Treiber Connector/J gibt Versionsdetails zurück. Hierdurch können im dynamischen Abfragemodus die SQL-Erweiterungen verwendet werden, die in MariaDB 10.2.4 eingeführt wurden. Wenn Verbindungen unter Verwendung des JDBC-Treibers für MySQL definiert werden, können diese Features nicht verwendet werden, und es erfolgt möglicherweise mehr lokale Verarbeitung im dynamischen Abfragemodus.

Datenmodule

Datenmodule enthalten Daten von Datenservern, hochgeladenen Dateien, Datasets, anderen Datenmodulen und von relationalen Packages, die den dynamischen Abfragemodus verwenden.

Datenmodule werden in der Webmodellierungskomponente in IBM Cognos Analytics erstellt und in **Teaminhalt** oder **Eigener Inhalt** gespeichert. Sie können mehrere Eingabequellen für ein einzelnes Datenmodul verwenden.

Tipp: Wenn Sie ein Datenmodul mit Daten aus einer hochgeladenen Datei erstellen und die Daten anderen Benutzern zur Verfügung stellen möchten, speichern Sie sowohl das Datenmodul als auch die Datei in **Teaminhalt**. Dadurch wird sichergestellt, dass ein anderer Benutzer einen Bericht ausführen kann, der auf die Daten verweist. Diese Einschränkung gilt für Berichtsersteller und Konsumenten. Administratoren können Berichte ausführen, die Daten aus dem Ordner **Eigener Inhalt** eines beliebigen Benutzers verwenden.

Datenmodule können als Quellen für Berichte, Dashboards, Storys, Explorationen, Notebooks, Datasets und andere Datenmodule verwendet werden.

Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics - Datenmodellierung*.

Datenmodule, die aus IBM Planning Analytics-Cubes stammen, werden in der Verwaltungskomponente erstellt. Weitere Informationen finden Sie unter „Erstellen von Datenmodulen aus Planning Analytics-Cubes” auf Seite 65.

Erstellen von Datenmodulen aus Planning Analytics-Cubes

Nach der erfolgreichen Erstellung einer Verbindung zu einem IBM Planning Analytics TM1-Datenbankserver können Sie die Cubes dieses Datenservers durchsuchen und zum Erstellen von Datenmodulen verwenden.

Datenmodule, die Planning Analytics-Cubes enthalten, können zum Erstellen von Berichten, Dashboards, Storys und anderen Cognos Analytics-Inhalten auf dieselbe Weise wie Packages, die Planning Analytics-Cubes enthalten, verwendet werden.

Vorbereitende Schritte

Eine erfolgreiche Verbindung vom Typ **IBM Planning Analytics** zum TM1-Datenbankserver muss bereits erstellt worden sein. Weitere Informationen finden Sie unter „Herstellen einer Datenserververbindung” auf Seite 25.

Informationen zu diesem Vorgang

Die folgenden Einschränkungen gelten, wenn Sie ein Datenmodul aus einem Planning Analytics-Cube erstellen:

- Nur Subsets von Hierarchiemitgliedern werden unterstützt.
- Die folgenden Planning Analytics-Subsets werden nicht unterstützt:
  - Mitgliedssätze mit mehreren Hierarchien.

    Tipp: Sie können eine Planning Analytics-Datenquelle mit mehreren Kennzahlenhierarchien so ändern, dass die Berichtsergebnisse gültig sind. Weitere Informationen finden Sie in „Beispiel: Eine PA-Datenquelle ändern, um nur eine Messhierarchie zu haben” auf Seite 66.
  - Steuersubsets, deren Subsetname mit "}" beginnt.
  - In Planning Analytics-Ansichten erstellte Rollup-Subsets. Diese Subsets sind Tupelmengen, keine Mitgliedssätze.
  - Subsets mit einem ungültigen MDX-Ausdruck oder einem leeren Mitgliedssatz.

Vorgehensweise

1. Suchen Sie unter **Verwalten** > **Datenserververbindungen** nach einer vorhandenen Datenserververbindung für **IBM Planning Analytics**.
2. Klicken Sie auf den Datenserver, um die zugehörigen Eigenschaften zu öffnen.
3. Klicken Sie auf der Registerkarte **Verbindungen** auf die Verbindung, um auf die zugehörigen Eigenschaften zuzugreifen.
4. Klicken Sie auf die Registerkarte **Cubes**.

   Die Liste der Cubes, die diese Verbindung umfasst, wird angezeigt.
5. Klicken Sie im Kontextmenü  eines Cubes auf **Datenmodul erstellen**.
6. Geben Sie den Modulnamen ein und speichern Sie das Modul an einer Position unter **Teaminhalt** oder **Eigener Inhalt**.

   Tipp: In **Teaminhalt** müssen Sie Elemente in Ordnern speichern.

   Eine Nachricht im oberen Bereich der Anwendungsseite bestätigt, dass das Datenmodul erfolgreich erstellt wurde.
7. Wenn die Datenbank mehr Cubes enthält, wiederholen Sie die Schritte 5 und 6, um ein Datenmodul für jeden der übrigen Cubes zu erstellen.

Ergebnisse

Die Datenmodule werden an der Position erstellt, die Sie angegeben haben.

Nächste Schritte

Verwenden Sie Datenmodule, um Berichte, Dashboards, Explorationen und andere Cognos Analytics-Inhalte für Planning Analytics-Cubes zu erstellen.

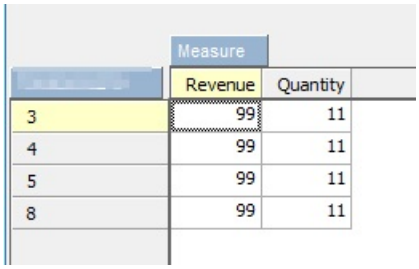
Beispiel: Eine PA-Datenquelle ändern, um nur eine Messhierarchie zu haben

Dieses Beispiel beginnt mit einem Bericht über eine Planning Analytics-Datenquelle mit mehreren Messhierarchien, die ursprünglich ungültige Ergebnisse liefern. Um das Problem zu beheben, entfernen Sie die zusätzlichen Maßshierarchien, sodass nur eine Hierarchie verbleibt.

Problem

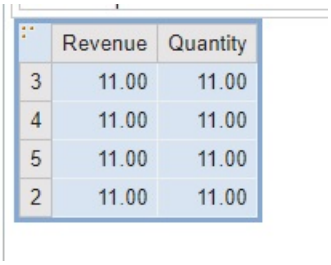
In Cognos Analytics führen Sie einen Bericht für eine Planning Analytics-Datenquelle aus, die mehrere Messhierarchien verwendet. In der Berichtsausgabe werden die Werte in einer Kennzahl jedoch fälschlicherweise in einer anderen Kennzahl wiederholt.

Dies ist das erwartete Ergebnis, das Sie in Planning Analytics erhalten haben:



	Measure	
	Revenue	Quantity
3	99	11
4	99	11
5	99	11
8	99	11

Im Folgenden sehen Sie das eigentliche Ergebnis in Cognos Analytics:



	Revenue	Quantity
3	11.00	11.00
4	11.00	11.00
5	11.00	11.00
2	11.00	11.00

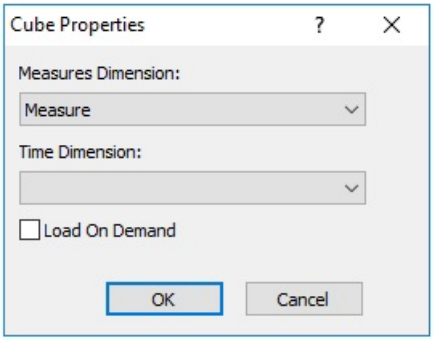
Ursache

Die Kennzahlenwerte werden wiederholt, da Cognos Analytics PA-Datenquellen, die mehr als eine Maßhierarchie verwenden, nicht unterstützt.

Lösung

Um dieses Problem zu beheben, entfernen Sie die zusätzlichen Kennzahlenhierarchien, sodass nur eine Hierarchie übrig bleibt.

1. Suchen Sie in Architect nach der Maßdimension, indem Sie die Eigenschaften des Würfels überprüfen.



2. Überprüfen Sie die vorhandenen Hierarchien dieser Dimension mithilfe des} HierarchiesProperties-Steuerwürfels.
3. Verwenden Sie die Funktion HierarchyDestroy in einem TI-Prozess, um alle zusätzlichen Hierarchien aus der Maßdimension zu entfernen.

   Tipp: Stellen Sie sicher, dass Sie auch die Leaves-Hierarchie entfernen.
4. Führen Sie in Cognos Analytics den Bericht erneut in der geänderten PA-Datenquelle aus.

Die Berichtsausgabe wird jetzt wie erwartet angezeigt.

Packages

Ein Package ist ein Subset eines Modells (welches das ganze Modell beinhalten kann), das der IBM Cognos Analytics-Anwendung zur Verfügung gestellt wird.

Relationale Packages werden in IBM Cognos Framework Manager erstellt und OLAP-Packages werden in IBM Cognos Cube Designer und in IBM Cognos Administration erstellt. Weitere Informationen finden Sie in dem Kapitel zum Publizieren von Packages in der Veröffentlichung *IBM Cognos Framework Manager - Benutzerhandbuch*.

Nicht alle Typen von Packages können in allen Cognos Analytics-Komponenten verwendet werden. Nur die Funktion zur Berichterstellung kann alle Typen von Packages verwenden, die traditionell von früheren Versionen von Cognos Analytics unterstützt wurden.

Für Dashboards und Storys werden die folgenden Packages unterstützt:

- Relationale Packages mit einem dynamischen Abfragemodus.
- Relationale Packages im kompatiblen Abfragemodus, wenn eine JDBC-Verbindung für jede Datenquelle im Package definiert ist.
- Dimensionale OLAP-Packages, die auf PowerCubes, dynamischen Cubes, TM1-Datenquellen, dimensional modellierten relationalen (DMR) Datenquellen und anderen Datenquellen basieren.

Die Modellierungskomponente unterstützt nur relationale Packages, die den dynamischen Abfragemodus verwenden, als Quellen für Datenmodule.

Weitere Informationen finden Sie im Handbuch *IBM Cognos Analytics - Datenmodellierung*.

Anmerkung: Cognos Analytics unterstützt keine Framework Manager-Namespaces, die Container sind, mit denen Inhalte in einem Model organisiert und eindeutig qualifiziert werden. Die Namespaces werden als Ordner angezeigt, wenn Framework Manager-Packages in Datenmodulen, Dashboards und anderen Inhalten angezeigt werden.

Pakete anreichern

Um die Benutzererfahrung in IBM Cognos Analytics -Komponenten, wie z. B. Dashboards und Explorationen, zu optimieren, müssen Framework Manager-Pakete angereichert werden.

Mit dem Anreicherungsprozess werden die Cognos Analytics -Datenmerkmale, wie **Zeit** und **Geografische Position**, den Abfrageelementen in den Paketen zugeordnet. Die Informationen aus dem Anreicherungs-

prozess ergänzen die Informationen, wie z. B. den Datentyp, den Spaltennamen oder den **Verwendung** -Eigenschaftswert, der aus den Paketmetadaten abgeleitet wird.

Ein angereichertes Paket umfasst die Datenmerkmale, die für die Funktionalität der künstlichen Intelligenz (KI) im Produkt erforderlich sind, wie z. B. Visualisierungsempfehlungen oder intelligent festgelegte Standardwerte für Spalteneigenschaften. Wenn Sie zum Beispiel das Beziehungsdiagramm in **Untersuchen**anzeigen möchten, muss ein angereichertes Paket verwendet werden. Andernfalls wird das Beziehungsdiagramm nicht angezeigt.

Tipp: Sie können ein Paket, das relationale DMR-Objekte (DMR = dimensional modellierte Objekte) enthält, nicht bereichern. Abfragesubjekte, die Eingabeaufforderungen enthalten, können angereichert werden, aber die Daten werden nicht abgerufen.

Der Anreicherungsprozess kann zeit-und speicherintensiv sein, so dass er nur dann ausgeführt werden sollte, wenn sich das Originalpaket geändert hat. Überlegen Sie, ob das Paket nach den folgenden Änderungen an dem Paket neu bereichert werden soll:

- Namen von Abfragesubjekten, Abfrageelementen und Namensbereichen werden geändert.
- Die Datentypen für Abfrageelemente werden geändert. Beispiel: Die Zahl wurde in die Zeichenfolge geändert.
- Es werden neue Abfrageelemente hinzugefügt.
- Filter oder Ausdrücke werden geändert, die die Werte, die das Abfragesubjekt zurückgeben würde, erheblich ändern.
- Ein Bereitstellungsarchiv wird in eine neue Umgebung importiert, die verschiedene Daten aus der Quelle verwendet, die für eine vorherige Anreicherung verwendet wird.

Wenn ein Paket erneut veröffentlicht wird, werden vorhandene angereicherte Metadaten nicht entfernt oder aktualisiert.

Vorbereitende Schritte

Um die Auswirkungen des Anreicherungsprozesses auf das System zu minimieren, sollten Sie erwägen, kleinere Pakete zu erstellen, die nur eine Untergruppe von zweckspezifischen Abfragesubjekten enthalten, und nur die kleineren Pakete bereichern. Beispiel: Ein Paket, das von erweiterten Berichtserstellern verwendet wird, könnte viele Abfragesubjekte enthüllen, bei denen viele der Abfragesubjekte bei der Erstellung von Dashboards oder Sondierungen nicht relevant sind. Sie können ein kleineres Paket aus dem ursprünglichen Paket erstellen und nur die Abfragesubjekte einschließen, die Sie in Ihren Dashboards und Sondierungen benötigen. Die Anreicherung dieses kleineren Pakets erfordert weniger Zeit und weniger Speicher.

Informationen zu diesem Vorgang

Sie können die Metadaten eines Pakets mit dem automatischen oder manuellen Prozess bereichern. Der automatische Prozess wertet alle Abfrageelemente aller ausgewählten Abfragesubjekte in dem Paket aus und wendet die Datenmerkmale automatisch auf sie an. Um die Auswirkungen auf das System zu minimieren, können Sie Namensbereiche oder einzelne Abfragesubjekte abwählen, um sie aus dem Anreicherungsprozess auszuschließen. In dem manuellen Prozess wenden Sie die Datenmerkmale explizit auf einzelne Abfrageelemente an.

Wenn Sie ein Paket anreichern, beginnen Sie normalerweise mit dem automatischen Prozess. Verwenden Sie den manuellen Prozess, um nur eine kleine Teilmenge von Abfrageelementen zu bereichern oder um Werte zu überschreiben, die durch die automatische Option falsch gesetzt wurden.

Die automatische Bereicherung umfasst die Option zum Abrufen von Beispieldaten. Wenn diese Option ausgewählt ist, stellt die Cognos Analytics -Abfrageengine eine Verbindung zur Datenquelle her und liest eine Stichprobe der zugehörigen Daten. Über das Dialogfenster 'enrich' kann die Stichprobengröße geändert werden. Wenn Sie die Stichprobengröße auf einen niedrigen Wert setzen oder gar keine Stichprobenentnahme, wird die Menge an Informationen, die die Anreicherung erfassen kann, reduziert. Die Menge der Stichprobendaten hängt auch von den Anmeldungen ab, die für den Zugriff auf die zu Grunde liegenden Datenquellen verwendet werden. Eine ideale Anmeldung kann auf die Tabellen, Sichten und

Spalten zugreifen, auf denen die Abfragesubjekte basieren, und auf eine repräsentative Anzahl von Zeilen und Werten in den abgefragten Tabellen und Sichten zugreifen.

Um auf die **Enrich-Paket** -Funktionalität zugreifen zu können, benötigen Sie Schreibberechtigungen für das Paket.

Vorgehensweise

1. Suchen Sie das Paket oder seine Verknüpfung in **Teaminhalt** oder **Mein Inhalt**.
2. From the package or shortcut context menu ⋯, select **Enrich-Paket**.

   Tipp: Wenn ein Paket als Datenmodulquelle verwendet wurde, können Sie das Paket in der Modellierungsbenutzeroberfläche aus dem Teilfenster **Quellen** bereichern.
3. Wählen Sie eine der folgenden Optionen aus.

   - **Automatisch bereichern**

     Die meiste Zeit beginnen Sie mit dieser Option. Die Statusinformationen zeigen Ihnen die Daten an, wann das Paket zuletzt veröffentlicht und angereichert wurde (falls es vor dem Paket angereichert wurde).

     – In der Anzeige ' **Tabellen auswählen** ' können Sie die Abfragesubjekte abwählen, die nicht durch den Anreicherungsprozess ausgewertet werden sollen. Standardmäßig werden alle sichtbaren Abfragesubjekte in dem Paket ausgewertet.

       Diese Option gibt Ihnen die Möglichkeit, die Abfragesubjekte auszuschließen, die in Ihren Dashboards oder Sondierungen nicht verwendet werden, und so die Zeit-und Speicherauslastung durch das System während des Anreicherungsprozesses zu reduzieren.

     – Um die Datenstichprobe zu aktivieren, wählen Sie das Markierungsfeld **Beispieldaten abrufen** aus und geben Sie die Anzahl der Zeilen an, die abgerufen werden sollen.

       Das Datenstichprobe enthält einige tiefere Datenmerkmale, die die Produktfunktionen unterstützen, die sich hinter der optimierten Benutzererfahrung in Dashboards, Explorationen und anderen Komponenten befinden. Das Extrahieren zu vieler Zeilen kann sich auf die Systemleistung auswirken. Keine Datenstichprobe oder zu wenige Zeilen liefern möglicherweise nicht genügend Informationen. Durch das Löschen dieses Kontrollkästchens wird die Zeit-und Speicherauslastung während des Anreicherungsprozesses verringert, aber die erwarteten Informationen werden möglicherweise nicht erfasst.

       Weitere Informationen finden Sie unter „Datenstichprobe” auf Seite 53.

     – Klicken Sie auf **Ausführen**.

       Abhängig von der Anzahl der betroffenen Abfragesubjekte kann der Anreicherungsprozess einige Zeit in Anspruch nehmen, möglicherweise sogar Stunden. Nachdem der Prozess abgeschlossen ist, werden in einer Informationsnachricht die Ergebnisse des Prozesses angezeigt. Selbst wenn nur ein bestimmter Prozentsatz der Abfragesubjekte angereichert wurde, haben Sie möglicherweise genügend Daten, um die AI-Funktionen in Ihren Dashboards und Erkundungen zu unterstützen.

     – Klicken Sie auf **Schließen**.

   - **Manuell bereichern**

     Verwenden Sie diese Option, um einzelne Abfrageelemente zu bereichern.

     – Erweitern Sie das Paket. Erweitern Sie anschließend ein Abfragesubjekt, und wählen Sie ein oder mehrere Abfrageelemente aus.

     – Wählen Sie im Dropdown-Menü **Datendarstellung definieren** die Option aus, die die Daten in der Abfrage darstellen sollen (entweder **Zeit** oder **Geografischer Standort**), und wählen Sie deren spezifische Werte aus. Der Wert **Standard** ermöglicht die Weitergabe von Einstellungen aus der Quelle.

     – Klicken Sie auf **OK**.

Datasets

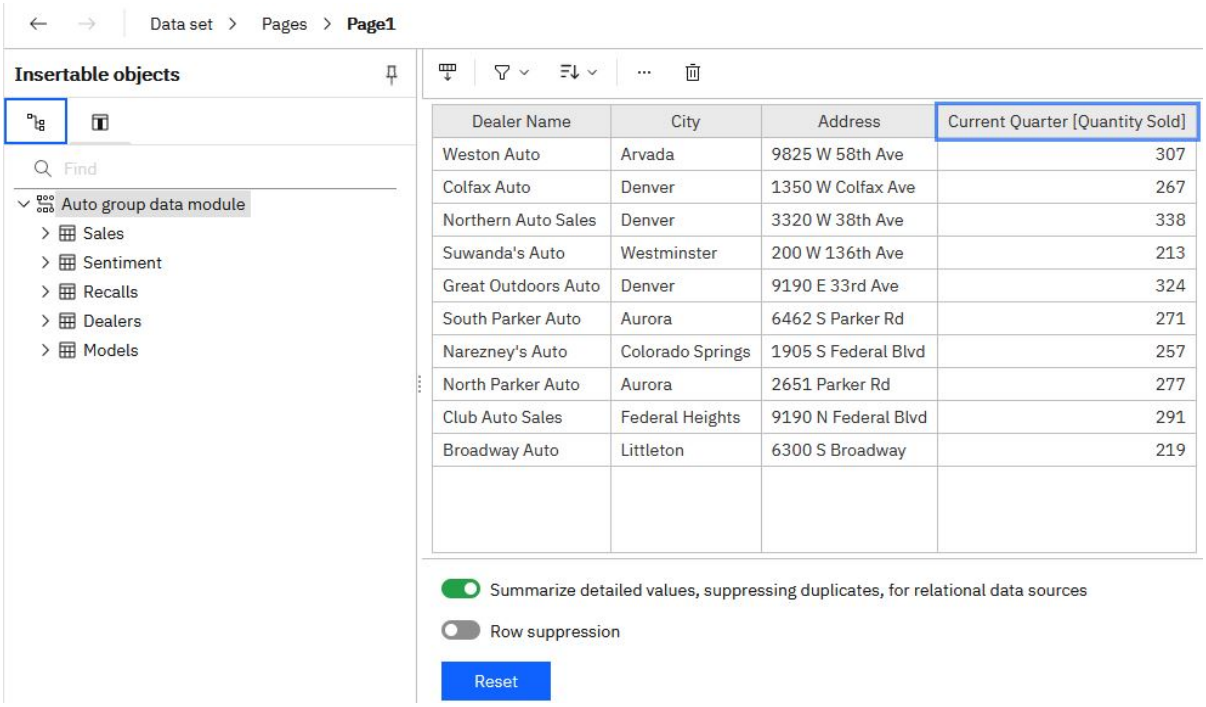
Datasets sind angepasste Sammlungen von Datenelementen, die Sie häufig verwenden. Wenn Sie Aktualisierungen an Datasets vornehmen, werden auch die Dashboards, Storys und Explorationen, die diese Datasets verwenden, bei ihrer nächsten Ausführung aktualisiert.

Sie können Datasets aus Packages oder Datenmodulen erstellen und als Quellen verwenden, um Dashboards, Storys, Explorationen und Datenmodule zu erstellen.

Sie können keinen Bericht direkt aus einem Dataset erstellen. Wenn Sie jedoch die Daten aus dem Dataset in einem Bericht verwenden möchten, erstellen Sie ein Datenmodul aus dem Dataset. Verwenden Sie dann das Datenmodul als Quelle für Ihren Bericht.

Das Dataset-Verfahren basiert auf der Cognos Analytics-Berichtsbasis. Sie fügen Daten in ähnlicher Weise zu einem Dataset hinzu, wie Sie Daten zu einem Listenbericht hinzufügen. Sie können zwischen den Modi **Seitendesign** und **Seitenvorschau** wechseln. Die Ansicht **Abfrage** bietet eine alternative Möglichkeit, Datasets zu bearbeiten. In dieser Ansicht können Sie Abfragen aus vorhandenen Berichten kopieren und einfügen, erweiterte Filter und Eingabeaufforderungen verwalten und Abfragen umbenennen.

Im Folgenden sehen Sie ein Beispiel für eine Datei im Modus **Seitenvorschau**.



Datasets erstellen

Erstellen Sie Datasets, um angepasste Sammlungen von Datenelementen zu gruppieren, die Sie häufig verwenden.

Wenn ein Dataset auf einem Package mit mehreren Verbindungen oder Anmeldedaten basiert, wird die von Ihnen auswählte Datenserververbindung oder Anmeldung mit dem Dataset gespeichert. Wenn sich die Package-Verbindungsinformationen später ändern, wird möglicherweise eine mehrdeutige Verbindungsnachricht angezeigt. Um diese Nachricht zu vermeiden, bearbeiten Sie das Dataset, wählen Sie die neue Verbindung oder Anmeldung aus, und speichern Sie das Dataset mithilfe der Option **Speichern unter**. Wählen Sie 'Ja' aus, wenn Sie gefragt werden, ob Sie das Dataset überschreiben möchten. Das Dataset wird mit der neuen Verbindung oder der neuen Anmeldung gespeichert, und die nachfolgenden Aktualisierungen verwenden die neuen Informationen.

Vorbereitende Schritte

Das Package oder das Datenmodul, das Sie als Quelle für Ihr Dataset verwenden möchten, muss bereits in **Teaminhalt** oder **Eigener Inhalt** gespeichert sein.

Informationen zu diesem Vorgang

Die Liste im Dataset kann nur einer Abfrage zugeordnet werden. Wenn Sie Datenelemente aus verschiedenen Abfragen zu Ihrem Dataset hinzufügen möchten, können Sie eine angepasste Abfrage in der Ansicht **Abfragen** erstellen, die Datenelemente aus verschiedenen Abfragen enthält.

Beim Erstellen oder Bearbeiten von Datasets können Sie Abfragen aus Cognos Analytics-Berichten wiederverwenden. Weitere Informationen finden Sie im Abschnitt „Berichtsabfragen in Datasets wiederverwenden” auf Seite 73.

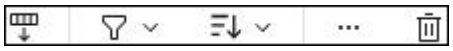
Vorgehensweise

1. Suchen Sie das Package oder Datenmodul in **Teaminhalt** oder **Eigener Inhalt**.
2. Klicken Sie im Kontextmenü ••• des Packages oder Datenmoduls auf die Option **Dataset erstellen**.

   Der Dataset-Editor wird im Modus **Seitendesign** geöffnet.
3. Ziehen Sie die Datenelemente aus dem Bereich **Einfügbare Objekte** in den Arbeitsbereich. Die Elemente werden als Spaltendaten ähnlich wie in einem Listenbericht angezeigt.

   Um eine Vorschau der Daten im Dataset anzuzeigen, wechseln Sie vom Modus **Seitendesign** in den Modus **Seitenvorschau**.
4. Aktivieren Sie bei relationalen Daten oder Datenmodulen das Kontrollkästchen **Detaillierte Werte für relationale Datenquellen auswerten und doppelte Werte unterdrücken**.

   Wenn Sie sich nicht sicher sind, ob dieses Kontrollkästchen ausgewählt werden soll, müssen Sie es abwählen und dann erneut auswählen, um zu sehen, wie die Daten aggregiert werden. Komprimierte Daten, die in weniger Zeilen enthalten sind, ermöglichen normalerweise Berichte und Dashboards mit besserer Leistung. Ein Grund, der dagegenspricht, die Daten in Ihrem Dataset zu aggregieren, ist, dass bestimmte Details im Prozess verloren gehen können, und es kann vorkommen, dass Daten aus einem System nicht mit den Daten eines anderen Systems übereinstimmen. Dies trifft besonders bei Berechnungen (z. B. beim Ermitteln des Durchschnitts) zu.
5. Wählen Sie **Zeilenunterdrückung** aus, wenn Zeilen ohne Daten oder mit Nullen ausgeblendet werden sollen.

   Wenn Sie Zeilen ohne Daten unterdrücken, erhalten Sie eine präzisere Ansicht Ihres Datasets.
6. Grenzen Sie die Daten im Dataset ein, indem Sie die Optionen in der On-Demand-Symbolleiste  verwenden.

   Um die Symbolleiste anzuzeigen, klicken Sie auf eine beliebige Spalte.

   Sie können den Spalten oder einzelnen Elementen des Datasets Filter hinzufügen, indem Sie auf das Element und dann auf das Filter-Symbol in der Symbolleiste klicken. Sie können einen angepassten Filter hinzufügen oder einen der vordefinierten Filtern verwenden.

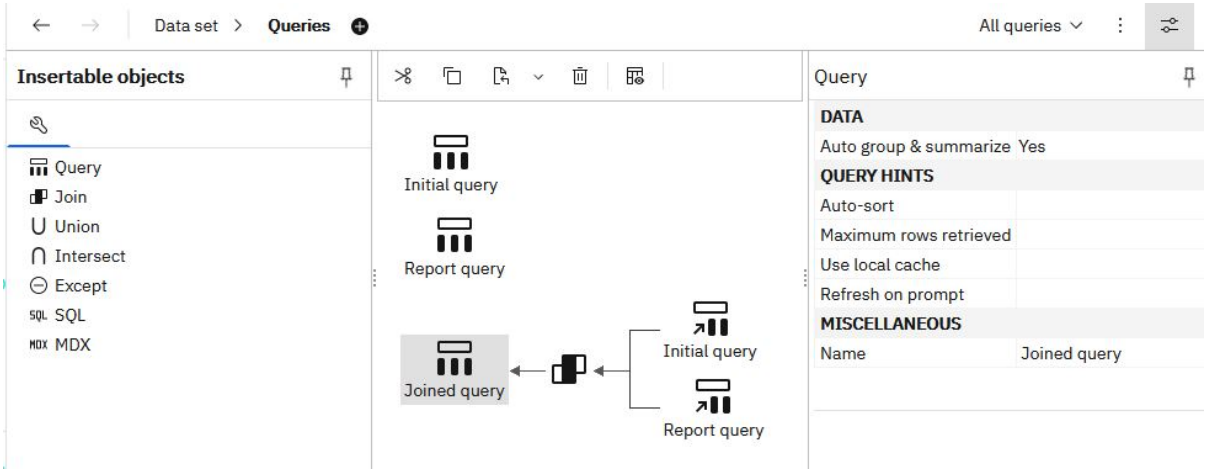
   Um die Werte zu sortieren, klicken Sie auf das Sortiersymbol und wählen Sie aus den verfügbaren Sortieroptionen aus.

   Um den Spaltenausdruck anzuzeigen, klicken Sie auf das Symbol **Mehr** ••• und wählen Sie **Edit Query Expression** aus.
7. Verwenden Sie die Ansicht **Abfrage**, um auf weitere Dataset-Funktionen zuzugreifen.

   Klicken Sie im Menü **Dataset** auf **Abfragen**, um den Abfragenexplorer zu öffnen.

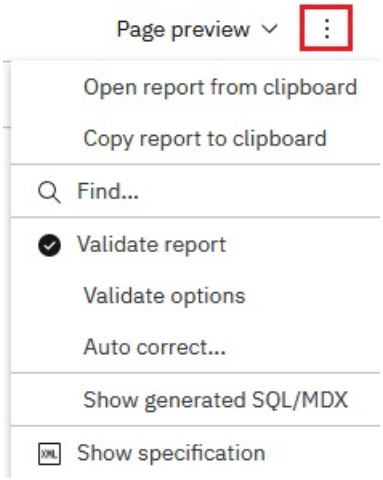
In dieser Ansicht können Sie Abfragen aus vorhandenen Berichten kopieren und einfügen, erweiterte Filter und Eingabeaufforderungen verwalten oder Abfragen umbenennen.

Im Folgenden sehen Sie ein Beispiel für ein Dataset in der Ansicht **Abfragen**:



Anmerkung: Die Abfragenamen werden als Tabellennamen verwendet, wenn das Dataset zum Erstellen von Datenmodulen verwendet wird. Verwenden Sie logische Namen, die die Daten bei der Umbenennung der Abfragen eindeutig beschreiben.

8. Klicken Sie auf das Symbol **Mehr** ⋮, um auf zusätzliche Funktionen zuzugreifen:



Klicken Sie auf **Bericht überprüfen**, um die Datei zu überprüfen, oder klicken Sie auf **Generiertes SQL/MDX anzeigen**, um das SQL-Dataset anzuzeigen.

9. Klicken Sie auf das Symbol für Speichern und wählen Sie eine der folgenden Optionen aus, um das Dataset zu speichern:

   - Um das Dataset erstmalig zu speichern und die Daten zu laden, klicken Sie auf **Daten speichern und laden**. Mit dieser Option werden die Metadaten gespeichert, aber die Daten werden nicht geladen. Abhängig vom jeweiligen Dataset kann das Laden der Daten eine gewisse Zeit in Anspruch nehmen.
   - Um ein aktualisiertes Dataset als neues Dataset zu speichern, klicken Sie auf **Speichern unter**. Mit dieser Option werden die Metadaten gespeichert, aber die Daten werden nicht geladen. Abhängig vom jeweiligen Dataset kann das Laden der Daten eine gewisse Zeit in Anspruch nehmen.
   - Um das Dataset zu speichern und die Daten zu laden, klicken Sie auf **Daten speichern und laden**. Außer dem Speichern neuer oder geänderter Metadaten bewirkt die Option auch das Laden der Daten. Die Daten stehen sofort zur Verfügung, wenn Sie ein Dashboard oder eine Story erstellen.

Ergebnisse

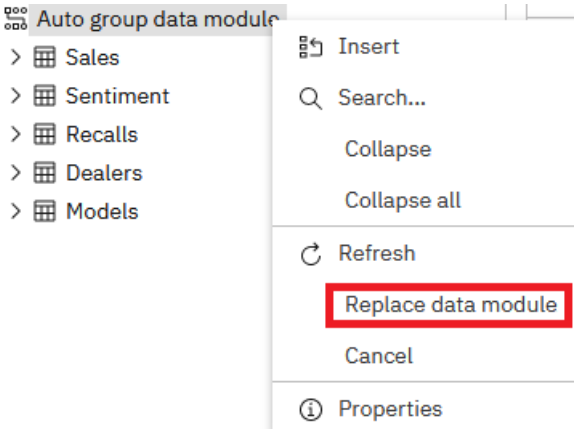
Das Dataset-Objekt wird an einer Position erstellt, an der Sie das Objekt gespeichert haben.

Nächste Schritte

Um das Dataset zu bearbeiten, öffnen Sie sie über **Teaminhalt** oder **Eigener Inhalt**.

Sie können Datenelemente im Dataset mit Datenelementen aus einer anderen Abfrage ersetzen. Klicken Sie im Modus **Seitendesign** oder **Seitenvorschau** auf die Schaltfläche **Zurücksetzen**. Die zuvor ausgewählten Datasets werden entfernt, und Sie können neue Datasets zu der Liste hinzufügen.

Sie können auch das Datenmodul oder das Package ersetzen, das als Quelle für das Dataset verwendet wurde. Klicken Sie im Fensterbereich **Einfügbare Objekte** mit der rechten Maustaste auf den Quellennamen. Wählen Sie dann die Option **Datenmodul ersetzen** oder **Package ersetzen** aus, wie im folgenden Screenshot dargestellt:



Berichtsabfragen in Datasets wiederverwenden

Sie können vorhandene Abfragen aus Cognos Analytics-Berichten wiederverwenden, indem Sie entweder einzelne Abfragen oder ganze Berichtsspezifikationen in Datasets kopieren.

Das Dataset und der Bericht, aus dem Sie die Abfragen kopieren, müssen auf demselben Typ der Datenquelle basieren: entweder auf einem Datenmodul oder auf einem Package.

Wenn Sie eine einzelne Berichtsabfrage kopieren, fügen Sie die Abfrage zum Dataset hinzu und können mit dem Dataset weiterarbeiten.

Wenn Sie die Berichtsspezifikation kopieren, wird das Dataset überschrieben, und Sie können die Abfrage (oder Abfragen) aus dem Bericht im Dataset verwenden. Das Berichtslayout wird nicht kopiert. Das Dataset wird in den Standardnamen **Neues Dataset** umbenannt. Sie können es dann als neues Dataset speichern.

Vorgehensweise

1. Erstellen Sie ein vorhandenes Dataset oder öffnen Sie es.
2. Öffnen Sie über **Teaminhalt** oder **Eigener Inhalt** den Cognos Analytics-Bericht im Bearbeitungsmodus.
3. Führen Sie die folgenden Schritte aus, um eine einzelne Abfrage in Ihr Dataset zu kopieren:
   a) Klicken im Bericht auf das Menü **Bericht** und auf **Abfragen**, um die Berichtsansicht **Abfragen** zu öffnen.
   b) Klicken Sie mit der rechten Maustaste auf die Abfrage, die kopiert werden soll, und klicken Sie auf **Kopieren**.
   c) Wechseln Sie zurück zum Dataset. Klicken Sie im Menü **Dataset** auf **Abfragen**.

d) Klicken Sie mit der rechten Maustaste auf einen leeren Bereich in der Ansicht **Abfragen** und klicken Sie auf **Einfügen**. Die neue Abfrage wird der Ansicht hinzugefügt.

e) Speichern Sie das Dataset.

4. Führen Sie die folgenden Schritte aus, um die Berichtsspezifikation zu kopieren:

a) Klicken Sie auf einer beliebigen Berichtsseite auf das Symbol **Mehr** ⋮ und wählen Sie **Bericht in die Zwischenablage kopieren** aus.

b) Kehren Sie zum Dataset zurück. Klicken Sie auf das Symbol **Mehr** ⋮ und wählen Sie **Bericht aus der Zwischenablage öffnen** aus.

c) Fügen Sie die Berichtsspezifikation in das angezeigte leere Feld ein und klicken Sie auf **OK**.

Sie befinden sich wieder in der Dataset-Listenansicht. Die Datenquelle und die Abfrage im Dataset wurden ersetzt. Der Dataset-Name wird als **Neues Dataset** angezeigt, selbst wenn Sie mit einem anderen Dataset-Namen begonnen haben.

d) Öffnen Sie die Ansicht **Abfragen**. Alle Abfragen aus dem Bericht werden in das Dataset kopiert.

e) Speichern Sie das Dataset mit der Option **Speichern unter**.

5. Klicken Sie im Menü **Dataset** auf **Seiten** > **Seite1**. Sie befinden sich wieder in der Dataset-Listenansicht.
6. Klicken Sie auf die Schaltfläche **Zurücksetzen**, um die Listenzuordnung mit der vorherigen Abfrage aufzuheben.

Die Datenelemente werden aus der Liste entfernt. Sie können nun Datenelemente aus einer anderen Abfrage, einschließlich der kopierten Berichtsabfragen, zur Liste hinzufügen.

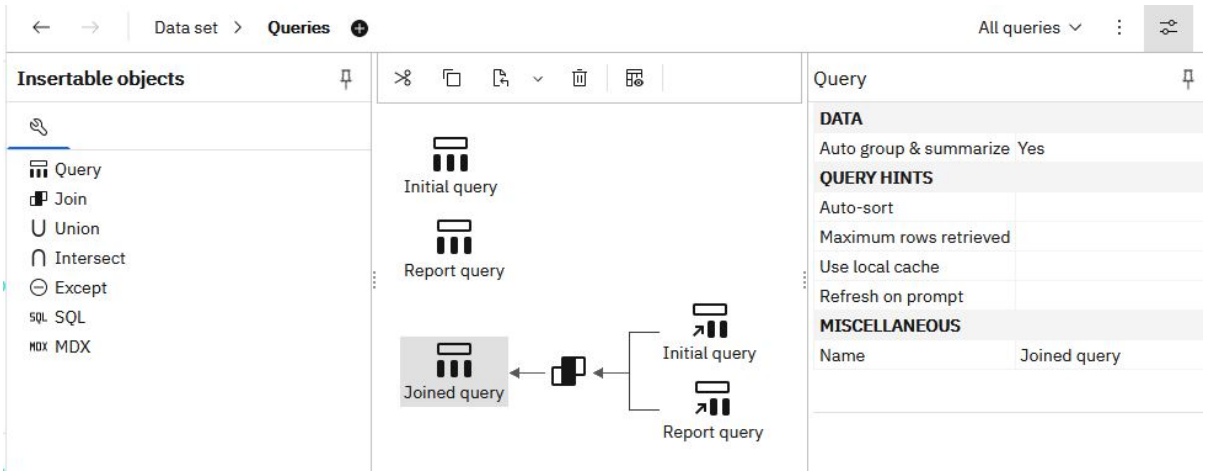
7. Klicken Sie in der Anzeige **Einfügbare Objekte** auf die Registerkarte **Datenelemente** .

Die Berichtsabfragen und die zugehörigen Datenelemente werden auf der Registerkarte angezeigt.

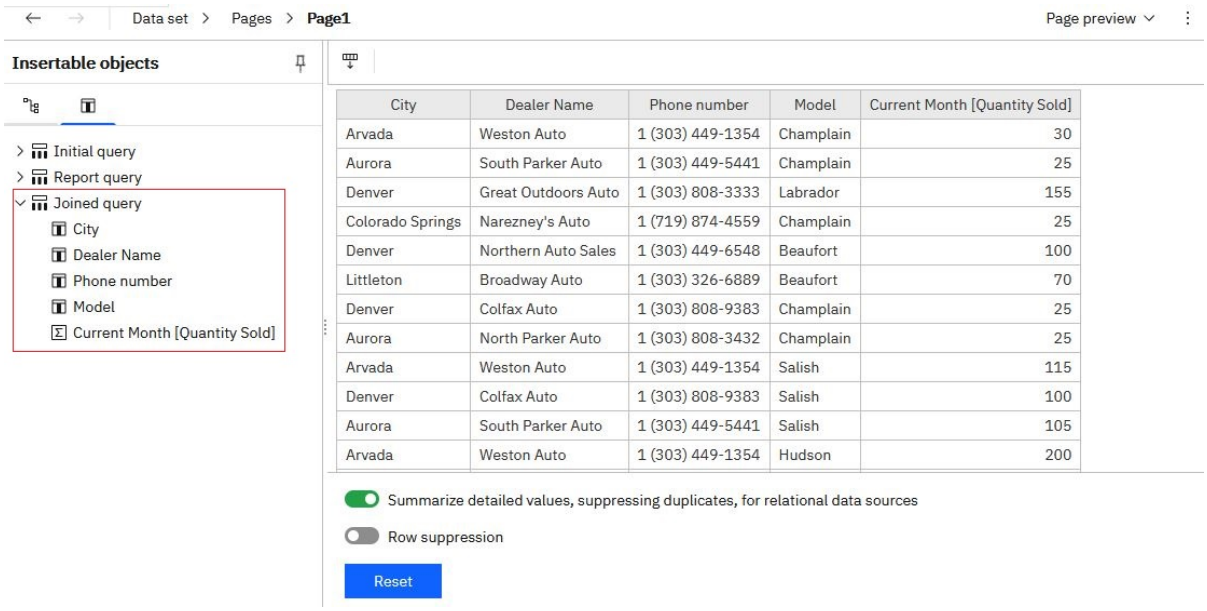
8. Ziehen Sie Elemente aus einer Abfrage in die Dataset-Liste.
9. Speichern Sie das Dataset.

Ergebnisse

Im Folgenden sehen Sie ein Beispiel für die Ansicht **Abfragen**, nachdem eine Abfrage mit dem Namen `Berichtsabfrage` in ein Dataset kopiert wurde. Die Berichtsabfrage wurde mit einer vorab vorhandenen Abfrage mit dem Namen `Ursprüngliche Abfrage` verknüpft.



Später wurden die Datenelemente aus der `Verknüpfungsabfrage` verwendet, um die Liste im Dataset zu füllen.



Hochgeladene Dateien

Wenn Sie schnelle Analysen und Visualisierungen mit Datendateien durchführen möchten, können Sie die Dateien selbst in IBM Cognos Analytics hochladen. Ihre Datendateien müssen die Größen- und Strukturanforderungen erfüllen.

Die Daten in den Dateien müssen sich in einem einfachen Spaltenformat befinden. Pivot-Tabellen oder Kreuztabellen werden nicht unterstützt.

Die Größenbegrenzungen für hochgeladene Dateien werden von Administratoren in **Verwalten** > **Konfiguration** > **System** > **Daten** konfiguriert. Die Einstellungen, die geändert werden müssen, sind **Größenbegrenzung pro Datenupload (MB)** und **Größenbegrenzung für gespeicherte Daten pro Benutzer (MB)**.

Die folgenden Einschränkungen für die Dateigröße gelten für einzelne Benutzer:

- Maximale Größe jeder einzelnen Datei. Der Standardwert ist 100 MB.
- Maximale Größe aller hochgeladenen Dateien. Der Standardwert ist 500 MB.

Die Dateitypen, die Sie in hochladen können, Cognos Analytics sind im Folgenden angegeben.

Microsoft Excel-Arbeitsmappendatei

Zu den unterstützten Microsoft Excel-Dateiformaten gehören `.xls` -und `.xlsx` -Arbeitsbuchdateien.

Die Dateiformate `.xlsb` und `.xlsm` werden nicht unterstützt.

Alle Blätter in einer Arbeitsmappe mit mehreren Tabellenblättern werden gleichzeitig hochgeladen. Jedes Blatt wird als separate Tabelle in Cognos Analytics angezeigt.

Für das Hochladen von Microsoft Excel-Dateien gelten die folgenden Bedingungen:

- XLSX-Dateien, die in OpenOffice gespeichert werden, werden nicht unterstützt.
- Kennwortgeschützte Excel-Dateien werden nicht unterstützt.
- Filter in Excel-Dateien werden ignoriert. Sie können die Filteroptionen in Datenmodulen verwenden, um die Filter erneut anzuwenden.
- Kommentare vor der ersten Kopfzeile werden als Spaltenüberschriften interpretiert.

  Text vor der ersten Zeile, in der das Arbeitsblatt beschrieben wird, wird fälschlicherweise als Spaltenüberschrift gelesen. Wenn Sie eine Beschreibung für das Arbeitsblatt benötigen, lassen Sie eine Zeile am Ende Ihrer Daten leer und fügen Sie die Beschreibung unterhalb der leeren Zeile hinzu.
- Gesamtsummen und Zwischensummen werden als Teil der Daten behandelt.

Gesamtsummen können als nicht summierte Daten fehlinterpretiert werden und zu irreführenden Ergebnissen führen. Ziehen Sie daher eventuell das Entfernen von Gesamtsummen und Zwischensummen aus Ihren Daten vor dem Hochladen der Datei in Betracht.

- Jede Datei kann maximal 2000 Spalten enthalten.

  Um eine bessere Abfrageleistung zu erhalten, sollten Sie jedoch das Hochladen von Dateien mit Hunderten von Spalten vermeiden. Versuchen Sie, vor dem Hochladen der Dateien redundante Spalten und Zeilen aus den Dateien zu entfernen.

  Weitere Informationen finden Sie in „Bewährte Verfahren zur Verbesserung der Abfrageleistung für hochgeladene Dateien" auf Seite 78.

Durch Trennzeichen getrennte Wertedateien

Die unterstützten Trennzeichen umfassen Kommas, Tabulatoren, Semikolons und Pipes (|). Die Dateierweiterung kann `.csv`, `.tsv`, `.tab` oder `.txt` sein.

Die folgenden Bedingungen gelten für das Hochladen von Dateien mit Trennzeichen, die durch Trennzeichen getrennt sind:

- Anführungszeichen als Escapezeichen für Literalwerte. Es werden einzelne Anführungszeichen (') und doppelte Anführungszeichen (") unterstützt.
- Satztrennzeichen trennen Zeilen voneinander. Zeilenumbruch (\n), Wagenrücklauf (\r) sowie Wagenrücklauf, gefolgt von Zeilenumbruch (\r\n), werden unterstützt.
- Wenn Ihre Datei als Unicode codiert ist, muss sie eine Byteanordnungsmarkierung als erstes Zeichen enthalten.
- Jeder Zeichenfolgewert in einer Datei darf maximal 5000 Zeichen enthalten. Alle zusätzlichen Zeichen werden abgeschnitten.
- Die Datums- und Zeitwerte in den Dateien müssen ein unterstütztes Format haben. Andernfalls werden die Daten in Visualisierungen möglicherweise nicht ordnungsgemäß wiedergegeben. Cognos Analytics unterstützt die ISO 8601-Standardformate für die Uhrzeit.

  Die folgenden Datumsformate werden unterstützt:

  - M/d/yy
  - MMM d, y
  - MMMM d, y
  - dd-MM-yy
  - dd-MMM-yy
  - jjjj-MM-tt

  Die folgenden Zeitformate werden unterstützt:

  - h:mm a
  - h:mm:ss a
  - h:mm:ss a z
  - HH:mm
  - HH:mm z
  - HH:mm:ss
  - HH:mm:ss.SS
  - HH:mm:ss z
  - HH:mm:ss.SS z

Jupyter-Notizbuch-Dateien (`.ipynb`)

Sie können Jupyter-Notizbuch-Dateien (`.ipynb`) hochladen, die in einer Jupyter-Umgebung außerhalb von Cognos Analytics erstellt wurden.

Weitere Informationen finden Sie in "Hochladen von externen Notebooks" in der Veröffentlichung *IBM Cognos Analytics - Einführung*.

Komprimierte Dateien

Bei den unterstützten, komprimierten Dateitypen, die Sie hochladen können, handelt es sich um `.zip` -und `.gz` -Dateien.

Sie können mehrere Dateien mit unterstützten Typen in einer `.zip` -oder `.gz` -Datei für einen einmaligen Upload komprimieren. Die Dateien werden zusammen in **Öffentlicher Inhalt** oder **Eigener Inhalt**gespeichert und Sie können schnell mit der Erstellung von Dashboards, Sondierungen oder Datenmodulen auf der Basis der `.zip` -oder `.gz` -Datei beginnen. Sie können auch alle Dateien im Archiv auf einmal neu laden.

Wenn ein komprimiertes Archiv aus zwei oder mehr Dateien besteht, lädt Cognos Analytics die Dateien wie folgt hoch:

- Die Dateien werden nacheinander verarbeitet.
- Beziehungen zwischen den Daten in den Dateien werden erkannt.

Wenn die Daten in den Archivdateien nicht verwandt sind, sollten Sie die Dateien aus den folgenden Gründen separat hochladen:

- Dateien werden gleichzeitig (schneller) und nicht nacheinander verarbeitet.
- Einzelne Dateien können aktualisiert werden, anstatt eine Gruppe von Dateien erneut zu verarbeiten, die nicht geändert wurden.

Dateien hochladen

Sie können unterstützte Dateitypen hochladen, die an einer beliebigen Position gespeichert sind, auf die Ihr Computer über lokalen Zugriff oder LAN-Zugriff verfügt.

Sie können jede Datendatei einzeln oder mehrere Dateien gleichzeitig hochladen. Es können auch mehrere Dateien für einen einstufigen Upload komprimiert werden.

Vorgehensweise

1. Verwenden Sie die folgenden Methoden zum Hochladen von Dateien:

   - Tippen Sie in der vertikalen Anwendungsleiste auf + **Neu** und tippen Sie dann auf **Dateien hochladen**. Suchen Sie die Dateien auf Ihrem lokalen Laufwerk oder auf dem LAN und wählen Sie eine oder mehrere Dateien zum Hochladen aus.
   - Ziehen Sie auf der Begrüßungsseite eine oder mehrere Dateien von Ihrem lokalen Laufwerk auf die Begrüßungsseite, um die Funktion **Schnellstart** zu aktivieren. Wenn **Schnellstart** angezeigt wird, legen Sie die Dateien im entsprechenden Feld ab, um sofort mit dem Erstellen eines Datenmoduls, einer Exploration, eines Dashboards oder eines Notebooks zu beginnen.
   - Tippen Sie unten auf der Begrüßungsseite den Link **Durchsuchen** an. Suchen Sie die Dateien auf Ihrem lokalen Laufwerk und wählen Sie mindestens eine Datei zum Hochladen aus.
   - Klicken Sie in einem Ordner unter **Teaminhalt** oder **Eigener Inhalt** auf das Symbol **Neu** + und wählen Sie **Dateien hochladen** aus. Suchen Sie die Dateien auf Ihrem lokalen Laufwerk oder auf dem LAN und wählen Sie eine oder mehrere Dateien zum Hochladen aus. Die Dateien werden in dem Ordner gespeichert, von dem aus Sie den Upload gestartet haben.

   Tipp: In verschiedenen Phasen des Hochladens werden für Uploads einzelner Dateien Status- und Fehlernachrichten angezeigt sowie konsolidierte Statusnachrichten für Uploads von mehreren Dateien.

2. Optional: Wenn die Nachricht **Daten ersetzen** angezeigt wird, wurde bereits zuvor eine Datei hochgeladen. Sie können diese Datei entweder ersetzen oder Daten an die Datei anhängen. Weitere Informationen finden Sie im Abschnitt „Daten in hochgeladenen Dateien aktualisieren" auf Seite 78.

Ergebnisse

Die hochgeladenen Dateien werden standardmäßig in **Eigener Inhalt** gespeichert. Wenn der Upload aus einem bestimmten Ordner in **Teaminhalt** oder **Eigener Inhalt** gestartet wurde, können die Dateien in diesem Ordner gespeichert werden.

Wenn Sie für hochgeladene Dateien auf Rollen- oder Tenantebene bzw. auf globaler Ebene eine gemeinsam genutzte andere Standardposition in **Teaminhalt** angegeben hat, können Benutzer die hochgeladenen Dateien an dieser Position speichern. Weitere Informationen finden Sie im Abschnitt zum Bearbeiten des Standardbenutzerprofils.

Nächste Schritte

Verwenden Sie hochgeladene Dateien, um Dashboards, Storys, Explorationen, Datenmodule oder Datasets zu erstellen.

Wenn Sie zwei hochgeladene Dateien verknüpfen möchten, erstellen Sie ein Datenmodul, indem Sie sie als Quellen verwenden.

In der Berichterstellung können hochgeladene Dateien nicht direkt verwendet werden. Diese können jedoch in ein Datenmodul integriert werden, das dann als Quelle bei der Berichterstellung verwendet werden kann.

Daten in hochgeladenen Dateien aktualisieren

Sie können Daten in einer hochgeladenen Datei durch Daten aus einer anderen Datei ersetzen oder Daten aus dieser anhängen.

Die Spaltennamen und Datentypen sowie die Reihenfolge der Spalten müssen in beiden Dateien identisch sein. Eine leere Datei ist eine Datei, die einen Header enthält, aber keine Daten. Sie kann daher für die Aktualisierung nicht verwendet werden.

Vorgehensweise

1. Suchen Sie in **Teaminhalt** oder **Eigener Inhalt** nach der hochgeladenen Datei, die Sie aktualisieren möchten.
2. Wählen Sie aus dem Kontextmenü  der Datei eine der folgenden Optionen aus:
   - **Datei ersetzen**

     Mit dieser Option werden alle Datenzeilen in der hochgeladenen Datei durch Datenzeilen aus der von Ihnen ausgewählten Datei ersetzt.
   - **Datei anhängen**

     Mit dieser Option werden neue Datenzeilen aus der von Ihnen ausgewählten Datei an die hochgeladene Datei angehängt.

   Tipp: Während der Aktualisierung der Datei werden Status- und Fehlernachrichten angezeigt.

Bewährte Verfahren zur Verbesserung der Abfrageleistung für hochgeladene Dateien

IBM Cognos Analytics kann große hochgeladene Dateien verarbeiten. Ziehen Sie jedoch einige bewährte Verfahren in Betracht, um die Abfrageleistung zu verbessern und Speicherplatz zu sparen.

Wenden Sie die folgenden bewährten Verfahren vor dem Hochladen von Dateien in IBM Cognos Analytics an:

- Speichern Sie häufig berechnete Ausdrücke als Spalten.

  Durch dieses Verfahren reduziert sich der Umfang der Ausdrucksevaluierung während der Laufzeit. Das Projizieren, Vergleichen und Sortieren einfacher Spaltenreferenzen und einfacher Werte (Literale) ist effizienter als das Evaluieren von Ausdrücken.
- Vermeiden Sie das Speichern einer großen Anzahl von Spalten, die nie von Abfragen verwendet werden.

  Zwar werden Daten sowohl komprimiert als auch codiert, um die Speichermenge zu reduzieren; dennoch empfiehlt es sich, keine redundanten oder unnötigen Spalten zu speichern.
- Sortieren Sie die Eingabe für die Spalte, die am häufigsten in Filtern verwendet wird.

  Bei großen hochgeladenen Dateien kann durch Sortierung der Eingabe die Auswertung von Vergleichselementen verbessert werden. Beim Sortieren der Daten in der in einem Filter häufig verwendeten Spalte (beispielsweise in der Spalte `Land` oder `Filiale`) werden Zeilen mit demselben Wert gruppiert. Wenn eine Abfrage Vergleichselemente für diese Spalte enthält, kann die Abfrage beim Navigieren durch die Daten effizienter bestimmen, welche Datenblöcke ignoriert werden können.

Datentypen zum Speichern von Daten in hochgeladenen Dateien und Datasets

IBM Cognos Analytics wendet eigene Datentypen auf Daten in hochgeladenen Dateien und Datasets an.

Die Daten in hochgeladenen Dateien und Datasets werden in den folgenden Datentypen gespeichert.

- Alle ganzzahligen Typen ('smallint', 'integer' und 'bigint') werden als Datentyp 'bigint' gespeichert.
- Alle näherungsweise berechneten numerischen Typen ('real', 'float' und 'double') werden als Datentyp 'double' gespeichert.
- Alle präzisen numerischen Werte werden als Dezimalzahl bis zur maximalen Genauigkeit von 38 gespeichert.
- Alle Zeichentypen ('char', 'nchar', 'varchar', 'nvarchar', 'clob' und 'nlclob') werden als nationaler Datentyp 'varchar' ohne maximale Genauigkeit gespeichert.
- Alle zeitbezogenen Typen (für Datum, Zeitmarke, Uhrzeit und Zeitmarke/Uhrzeit mit Zeitzone) werden als Zeitmarke gespeichert.
- Intervalltypen werden in einem Format gespeichert, das als Intervall interpretiert wird. Intervallwerte werden vom Berichtsserver wiedergegeben. In früheren Releases wurde der Wert als Zeichenfolge (string) gespeichert.

Wenn es sich bei einem Quellenwert um einen Dezimaldatentyp mit einer Genauigkeit von mehr als 38 handelt, versucht der Abfrageservice, den Wert als Dezimaldatentyp 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. Die Anzahl der Kommastellen eines präzisen Werts kann verringert werden, indem ein Umsetzungsausdruck (CAST) mit einer Genauigkeit von kleiner als 38 angegeben wird.

Nachfolgende Leerzeichen werden aus allen Zeichenwerten entfernt.

Zeitmarken und Uhrzeiten mit Zeitzonen werden auf einen Wert normalisiert, der auf der koordinierten Weltzeit (UTC) basiert.

Kapitel 4. Konfigurieren von Systemeinstellungen

Sie können Systemeinstellungen konfigurieren, die sich auf alle Benutzer und Komponenten in Ihrer Cognos Analytics-Umgebung auswirken.

Konfigurieren der Darstellung

Administratoren können bestimmte Elemente aktivieren, die in der Cognos Analytics-Benutzerschnittstelle angezeigt werden.

Vorgehensweise

1. Wechseln Sie zu **Verwalten** > **Konfiguration** > **System** und wählen Sie **Darstellung** aus.
2. Geben Sie bei Bedarf Werte für die folgenden Einstellungen an:

Eigenschaft	Einstellung	Ergebnis
Inhalt nach Seiten in Konten laden	**Aktiviert** (Standardeinstellung)	Unter **Verwalten** > **Personen** > **Konten** wird die Liste von Benutzer-, Gruppen- und Rolleneinträgen in separate Seiten unterteilt. Wenn Sie Konten verwalten, können Sie schneller zwischen Seiten navigieren, um Einträge zu finden.
	Inaktiviert	Die Liste der Einträge wird in Form einer Liste mit Blätterfunktion angezeigt.
Elemente pro Seite in Konten	*zahl* Standardwert = 200	Wenn **Inhalt nach Seiten in Konten laden** aktiviert ist, ist dies die Anzahl von Namespaceeinträgen pro Seite.
Traditionelle Cognos-Benutzerschnittstelle starten	**1**	Traditionelle BI-Komponenten sind aktiviert. Benutzer können auf Analysis Studio, Drillthrough-Definitionen, Event Studio, Query Studio und Cognos Workspace zugreifen, indem Sie auf **Neu** + und dann auf **Sonstige** klicken.
	0	Das Menü **Sonstige** wird nicht angezeigt.

Eigenschaft	Einstellung	Ergebnis
Eigene Portalseiten aktivieren	**Aktiviert**	Der Ordner **Eigene Portalseiten**  wird unter dem Ordner **Teaminhalt**  angezeigt. Benutzer, die Portalseiten in ihrer Cognos BI 10.x-Umgebung hatten, können deren Inhalte nach Cognos Analytics migrieren. Ihre Portalseiten sehen genauso aus und funktionieren genauso wie in Cognos BI 10.x.
	Inaktiviert (Standardeinstellung)	Der Ordner **Eigene Portalseiten** wird nicht angezeigt.

3. Klicken Sie auf **OK**.

Ergebnisse

Die Konfigurationsänderungen werden gespeichert und an alle Dispatcher weitergegeben. Sie müssen den Service nicht erneut starten, damit die Änderungen wirksam werden.

Konfigurieren der Sicherheit

Administratoren können die Sicherheitseinstellungen in Cognos Analytics konfigurieren.

Vorgehensweise

1. Wechseln Sie zu **Verwalten** > **Konfiguration** > **System** und wählen Sie **Sicherheit** aus.
2. Geben Sie bei Bedarf Werte für die folgenden Einstellungen an:

Eigenschaft	Einstellung	Ergebnis
HTTP Strict Transport - Ablaufzeitraum (Tage)	*zahl*	Die Einstellung für die maximale Gültigkeitsdauer für HTTP Strict Transport Security in Tagen.
Weiterleitungs-URL für Anmeldung	***URL***	Die URL einer Seite, auf die der Benutzer umgeleitet wird, wenn er sich bei Cognos Analytics anmeldet. **Tipp:** Sie können diesen Parameter bei der Integration in Ihre spezifische SSO-Umgebung verwenden.
Weiterleitungs-URL für Abmeldung	*URL*	Die URL einer Seite, auf die der Benutzer umgeleitet wird, wenn er sich von Cognos Analytics abmeldet. **Tipp:** Sie können diesen Parameter bei der Integration in Ihre spezifische SSO-Umgebung verwenden.

Eigenschaft	Einstellung	Ergebnis

Anmeldeparameter in URL zulässig	*durch Kommas getrennte Liste von Parameternamen*	Verwenden Sie diesen Parameter, um die Übergabe von CAM-Namespace-Anmeldeparametern zu ermöglichen.
		Beispiel
		Ihr Unternehmen möchte die folgende Benutzeranmeldesyntax implementieren:
		`http://server:port/bi/v1/disp?CAM_action=logonAs&CAMNamespace=NamespaceName&CAMUsername=UserID&CAMPassword=Password`
		Als Administrator würden Sie im Feld **Anmeldeparameter in URL zulässig** Folgendes eingeben:
		`CAMNamespace,CAMUsername,CAMPassword`

11.1.5 **E-Mail-Domänen in Whitelist aufnehmen**	*liste mit domänen*	Verwenden Sie diesen Parameter, um eine Whitelist mit E-Mail-Domänen festzulegen. Wenn der Parameter festgelegt wird, können E-Mails nur an die angegebenen E-Mail-Domänen gesendet werden. Der Wert ist eine durch Kommas getrennte Liste von Domänen. Beispiel: ibm.com, domain.com, mail.com. Wenn kein Wert angegeben wird, können Nachrichten an jede E-Mail-Domäne gesendet werden.
Geheimer Signierschlüssel für Tokenanmeldung	*alphanumerische zeichenfolge*	Geben Sie den geheimen Signierschlüssel für Tokens ein, die für die Anmeldung generiert werden.

3. Klicken Sie auf **OK**.

Ergebnisse

Die Konfigurationsänderungen werden gespeichert und an alle Dispatcher weitergegeben. Sie müssen den Service erneut starten, um sicherzustellen, dass alle Änderungen wirksam werden.

Verwalten von Datendateiuploads

Sie können steuern, wie Datendateien in IBM Cognos Analytics hochgeladen werden. Führen Sie die folgenden Schritte aus, um die Verschlüsselungs- und Größenbegrenzungen von Daten für hochgeladene Datendateien anzugeben.

Tipps:

- Diese Einstellungen gelten nur für hochgeladene Datendateien, nicht für andere Datentypen wie Datasets.
- Zum Ändern der Position des Verzeichnisses für hochgeladene Datendateien starten Sie Cognos Configuration, klicken Sie auf **Umgebung** und bearbeiten Sie dann den Wert der Eigenschaft **Datendateien-Verzeichnis**. Der Standardwert ist `../data`. Weitere Informationen finden Sie im *IBM Cognos AnalyticsInstallation und Konfiguration - Handbuch*.

Vorgehensweise

1. Wechseln Sie zu **Verwalten** > **Konfiguration** > **System** und wählen Sie die Registerkarte **Daten** aus.
2. Geben Sie bei Bedarf Werte für die folgenden Einstellungen an:

Eigenschaft	Einstellung	Ergebnis
Neue Datendateien verschlüsseln?	**Aktiviert** (Standardeinstellung)	Neue hochgeladene Datendateien werden verschlüsselt.
	Inaktiviert	Neue hochgeladene Datendateien werden nicht verschlüsselt.
Größenbegrenzung pro Datenupload (MB)	*zahl* Standardwert = 100	Die maximale Größe, in MB, einer hochgeladenen Datendatei.
Größenbegrenzung für gespeicherte Daten pro Benutzer (MB)	*zahl* Standardwert = 500	Die maximale Größe, in MB, des Datenspeichers pro Benutzer.

   Tipp: Wenn Größenbegrenzungen aktualisiert werden, kann es einen Moment dauern, bis die Aktualisierung angezeigt wird.
3. Klicken Sie auf **OK**.

Ergebnisse

Die Konfigurationsänderungen werden gespeichert und an alle Dispatcher weitergegeben. Sie müssen den Service nicht erneut starten, damit die Änderungen wirksam werden.

Protokollierung

Protokollnachrichten enthalten Informationen zum Status von Komponenten und wichtigen Ereignissen. Administratoren und Benutzer können diese Nachrichten zur Fehlerbehebung einsetzen.

IBM Cognos Analytics unterstützt verschiedene Arten der Protokollierung, darunter die folgenden Protokollierungstypen: Auditprotokollierung, Protokollierung zu Diagnosezwecken, Protokollierung für Benutzersitzung und Leistungsprotokollierung für Berichte.

Standardmäßig sendet der IBM Cognos-Service für jede Installation Informationen an das lokale Verzeichnis *installationsposition*`/logs`. Die Auditnachrichten werden in der Datei `cogaudit.log` gespeichert und die Diagnosenachrichten in den Dateien `cognosserver.log` und `dataset-service.log`. Für Auditprotokolle kann der Administrator die Position, Größe und die Anzahl der Protokolldateien in IBM Cognos Configuration angeben. Für die Protokollierung zu Diagnosezwecken ist die Größe und Anzahl der Protokolldateien im Teil **Verwalten** von Cognos Analytics festgelegt. Protokolle zu Diagnosezwecken werden immer in das Verzeichnis *installationsposition*`/logs` geschrieben. Die Auditprotokollierung kann so konfiguriert werden, dass sie auch in eine Datenbank, einen fernen Protokollserver oder in ein Systemprotokoll schreibt. Weitere Informationen finden Sie unter „Protokollierung zu Diagnosezwecken” auf Seite 87.

Die Sitzungsprotokollierung kann von einzelnen Benutzern für eine einzige Cognos Analytics-Sitzung aktiviert werden, nachdem Administratoren diese Art der Protokollierung für das System aktiviert haben. Die Nachrichten werden in den folgenden Protokolldateien im Verzeichnis *installationsposition*`/`

logs protokolliert: cognosserver-session-*sitzungs-id*.log und dataset-service-session-*sitzungs-id*.log. Weitere Informationen finden Sie unter „Einrichten der Protokollierung” auf Seite 85.

Leistungsprotokollierung für Berichte

Diese Art der Protokollierung wird in IBM Cognos Analytics - Reporting für Einzelberichte unterstützt. Ein Berichtsersteller aktiviert die Option für die Protokollierung von Leistungsdetails, indem er die Berichtserstellungsoption **Leistungsdetails einbeziehen** auswählt. Die folgenden Details können in der Berichtsausgabe angezeigt werden: **Gesamte Ausführungszeit**, **Abfrageausführungszeit** und **Ausgabezeit**. Kunden können diese Informationen verwenden, um die Leistung selbst zu diagnostizieren oder Probleme zu beheben, bevor sie eine Serviceanforderung absetzen.

Weitere Informationen finden Sie in den Abschnitten zum Ausführen von Berichten und zur Anzeige von Leistungsdetails im *IBM Cognos Analytics - Reporting-Handbuch*.

Einrichten der Protokollierung

Administratoren können sowohl die Sitzungsprotokollierung als auch die Protokollierung zu Diagnosezwecken konfigurieren.

`Sitzungsprotokollierung`

Die Sitzungsprotokollierung wird verwendet, um detaillierte Benutzeraktivitäten in jeder Komponente und jedem Service von IBM Cognos Analytics zu protokollieren, die der Anforderung des Benutzers zugeordnet ist.

Der Benutzer muss die Komponenten, Services oder Protokollierungskonfigurationsdetails nicht kennen. Es gibt keine Leistungsauswirkungen für andere Benutzer.

Die Sitzungsprotokollierung wird normalerweise dann verwendet, wenn ein Benutzer ein Problem reproduzieren kann. Sie kann jederzeit vom Benutzer gestoppt werden.

Eindeutige Protokolldateien werden für jeden Benutzer generiert, der die Sitzungsprotokollierung aktiviert. Die Dateinamen enthalten eine eindeutige **Protokoll-ID**, die generiert wird, wenn die Sitzungsprotokollierung vom Benutzer aktiviert wird.

Der Administrator muss die Sitzungsprotokollierung für das System aktivieren. Dann können einzelne Benutzer es selbst aktivieren oder inaktivieren.

`Protokollierung zu Diagnosezwecken`

Die Protokollierung zu Diagnosezwecken erstellt Serverprotokolldateien, anhand derer Administratoren und Supportmitarbeiter sporadisch auftretende oder servicespezifische Probleme beheben können. Dieselbe Protokollierungskonfiguration zu Diagnosezwecken wird automatisch für alle Server festgelegt.

Weitere Informationen finden Sie unter „Protokollierung zu Diagnosezwecken” auf Seite 87.

Vorgehensweise

1. Wechseln Sie zu **Verwalten** > **Konfiguration** > **System** und wählen Sie **Protokollierung** aus.
2. Geben Sie bei Bedarf Werte für die folgenden Einstellungen an:

Eigenschaft	Einstellung	Ergebnis
Größenbeschränkung für Serverprotokolldatei (MB)	*zahl* Standardwert = 200	Die maximale Größe, in MB, der Serverprotokolldatei. Nachdem eine Serverprotokolldatei ihr Größenlimit erreicht hat, wird eine neue "rollierende" Protokolldatei erstellt. **Tipp:** Serverprotokolldateien werden für die „Protokollierung zu Diagnosezwecken” auf Seite 87 verwendet.
Maximale Anzahl von Sicherungsserverprotokolldateien	*zahl* Standardwert = 10	Die maximale Anzahl rollierender Serverprotokolldateien, die als Sicherungen gespeichert werden. **Tipp:** Serverprotokolldateien werden für die „Protokollierung zu Diagnosezwecken” auf Seite 87 verwendet.
Protokollierung für Benutzersitzung aktivieren	**Aktiviert** (Standardeinstellung)	Die Benutzersitzung wird protokolliert. **Tipp:** Wenn diese Einstellung aktiviert ist, wird die Option **Eigene Sitzung protokollieren** für alle Benutzer in ihren persönlichen Einstellungen verfügbar.
	Inaktiviert	Die Benutzersitzung wird nicht protokolliert.
Größenbeschränkung für Protokolldatei für Benutzersitzungen (MB)	*zahl* Standardwert = 25	Die maximale Größe, in MB, der Protokolldatei der Benutzersitzung für jede Benutzersitzung. Nachdem eine Protokolldatei einer Benutzersitzung ihr Größenlimit erreicht hat, wird eine neue "rollierende" Protokolldatei erstellt.
Maximale Anzahl von Sicherungsprotokolldateien (pro Benutzersitzung)	*zahl* Standardwert = 10	Die maximale Anzahl rollierender Protokolldateien für Benutzersitzungen, die als Sicherungen gespeichert werden.
Sitzungsprotokolldateien nach 48 Stunden löschen	**Aktiviert** (Standardeinstellung)	Alle Protokolldateien von Benutzersitzungen werden nach 48 Stunden gelöscht.
	Inaktiviert	Protokolldateien von Benutzersitzungen werden nicht gelöscht.

3. Klicken Sie auf **OK**, um die Änderungen zu übernehmen.

   Sie müssen den IBM Cognos Analytics-Service nicht neu starten.

Ergebnisse

Die Konfigurationsänderungen werden gespeichert und an alle Dispatcher weitergegeben. Sie müssen den Service nicht erneut starten, damit die Änderungen wirksam werden.

Nächste Schritte

Benutzer können jetzt die Sitzungsprotokollierung in ihren persönlichen Einstellungen aktivieren, indem sie die Option **Eigene Sitzung protokollieren** auswählen und die Einstellung **Sitzungsprotokollierung** aktivieren. Benutzer sollten die für die Sitzung generierte **Protokoll-ID** aufzeichnen, bevor sie die Anmeldung inaktivieren oder den Browser schließen. Der Administrator benötigt diese ID zum Suchen der Sitzungsprotokolldateien `cognosserver-session-`*`protokoll-id`*`.log` und `dataset-service-session-`*`sitzungs-id`*`.log` im Verzeichnis *`installationsposition`*`/logs`.

Protokollierung zu Diagnosezwecken

Die Protokollierung zu Diagnosezwecken kann von Administratoren so konfiguriert werden, dass sie zur Behebung von intermittierenden oder Service-spezifischen Problemen verwendet werden kann. Dieselbe Protokollierungskonfiguration wird automatisch für alle Server festgelegt.

Die Nachrichten für die Protokollierung zu Diagnosezwecken werden in den Dateien `cognosserver.log` und `dataset-service.log` im Verzeichnis *`installationsposition`*`/logs` protokolliert. Die Administratoren können die maximale Größe für Protokolldateien und die maximale Anzahl von Protokolldateien angeben, die beibehalten werden müssen, um negative Auswirkungen auf die Leistung zu vermeiden.

Diese Art der Protokollierung ist ein Ersatz für die JAVA-IPF-Protokollierung (ipfclientconfig.xml) aus früheren Versionen von Cognos Analytics. Cognos Analytics verarbeitet die Protokollnachrichten aus den Produktservices mithilfe intern definierter Protokollfunktionen. Diese Protokollfunktionen werden in Protokollierungsthemen abstrahiert, die in der Schnittstelle **Verwalten** aktiviert werden können.

Die Protokollierung zu Diagnosezwecken hat keine Auswirkungen auf die Sitzungsprotokollierung oder die Auditprotokollierung.

Tipp: Sie können weiterhin 'ipfclientconfig.xml' für native Codekomponenten verwenden, wie z. B. Berichtsserver oder Framework Manager. 'ipfclientconfig.xml' kann die Auditprotokollierung beeinträchtigen, weshalb es mit Vorsicht zu verwenden ist.

Konfigurieren der Diagnoseprotokollierung

Administratoren können Einschränkungen bezüglich der Größe und Anzahl der Protokolldateien, die für die Protokollierung zu Diagnosezwecken verwendet werden, angeben.

Vorgehensweise

1. Starten Sie die Prozedur im Thema „Einrichten der Protokollierung” auf Seite 85.
2. Geben Sie die erforderlichen Werte für die Einstellungen **Größenbeschränkung für Serverprotokolldatei** und **Maximale Anzahl von Sicherungsserverprotokolldateien** an.
3. Klicken Sie auf **OK**.

   Sie müssen den IBM Cognos-Service nicht erneut starten, um die Protokollierung zu Diagnosezwecken zu ändern.

Protokollierung zu Diagnosezwecken für unterschiedliche Themen

Sie können die Protokollierung zu Diagnosezwecken für eine bestimmte Produktkomponente oder Funktion oder einen bestimmten Service aktivieren, indem Sie den Protokollierungsabschnitt ändern.

IBM Cognos Analytics verarbeitet die Protokollnachrichten aus den Produktservices mithilfe intern definierter Protokollfunktionen. Diese Protokollfunktionen werden in Protokollierungsthemen abstrahiert. Das Thema **Standardprotokollierung**, das für die Protokollierung zu Diagnosezwecken festgelegt ist, verwendet einen Satz von Protokollfunktionsnamen, die in bestimmten Fehlerkategorien festgelegt sind.

Dies geschieht, damit die Standardprotokollierung nicht zu ausführlich wird und nur die wichtigsten Nachrichten aufzeichnet.

Sie können die Protokollierung zu Diagnosezwecken für ein integriertes Thema oder ein benutzerdefiniertes Thema aktivieren. Um ein benutzerdefiniertes Thema zu erstellen, können Sie eine JSON-Spezifikation für ein integriertes Thema herunterzuladen und es als Basis für die Erstellung Ihres benutzerdefinierten Abschnitts verwenden. Benutzerdefinierte Themen können geändert werden, integrierte Themen hingegen nicht.

Vorgehensweise

1. Wechseln Sie zu **Verwalten** > **Konfiguration**.
2. Wählen Sie die Registerkarte **Protokollierung zu Diagnosezwecken** aus.
3. Wählen Sie eins der integrierten oder benutzerdefinierten Themen aus, für das Sie die Protokollierung aktivieren möchten.

   Die folgenden integrierten Themen sind verfügbar:

   - **AAA** - Protokollierung der Zugriffsmanagerauthentifizierung (AAA = Access Manager Authentication)
   - **CM** - Content Manager-Protokollierung
   - **DEFAULT LOGGING** - Protokollierung mit Standardeinstellungen
   - **DISP** - Dispatcher-Protokollierung
   - **MOSER** - Protokollierung des Modellierungsservice
   - **POGO_MSGS** - Dispatcher-SOAP-Nachrichtenprotokollierung

   Um beispielsweise die Protokollierung von Authentifizierungsproblemen zu aktivieren, wählen Sie das Thema **AAA** aus.
4. Klicken Sie auf **Anwenden**.
5. Um die **Standardprotokollierung** wiederherzustellen, klicken Sie auf **Zurücksetzen**.
6. Führen Sie die folgenden Schritte aus, um ein benutzerdefiniertes Thema zu erstellen:
   a) Klicken Sie auf die Registerkarte **Integrierte Topics**.
   b) Klicken Sie neben einem integrierten Thema, das Ähnlichkeiten mit dem Thema, das Sie erstellen möchten, aufweist, auf das Symbol 'Mehr'  , und wählen Sie dann **Topic herunterladen** aus.
   c) Bearbeiten Sie die Datei und speichern Sie sie auf Ihrem Computer unter *dateiname*`.json`.
   d) Klicken Sie auf die Registerkarte **Benutzerdefinierte Topics**.
   e) Klicken Sie auf das Symbol **Topic hochladen**  .

      Ihr neues Thema wird als Eintrag auf der Registerkarte **Benutzerdefinierte Topics** angezeigt.

Ergebnisse

Die Protokolle werden jetzt in die Dateien `cognosserver.log` und `dataset-service.log` im Verzeichnis *`installationsposition`*`/logs` geschrieben.

Verwenden der Diagnoseprotokollierung zum Beheben von Fehlern beim Start des Cognos-Service

Probleme beim Starten des IBM Cognos-Service sind ein Beispiel für eine Situation, in der die Protokollierung zu Diagnosezwecken Ihnen beim Ermitteln der Fehlerursache helfen kann.

Wenn der Start des Cognos-Service fehlschlägt, bevor der Dispatcher bereit ist, müssen Sie vor einem erneuten Startversuch des Service in Ihrem Installationsverzeichnis die detailliertere Protokollierung zu Diagnosezwecken aktivieren. Standardmäßig ist die Protokollebene 'Minimal' aktiviert.

Vorgehensweise

1. Öffnen Sie im IBM Cognos Analytics-Verzeichnis *Installationsposition*/wlp/usr/servers/cognosserver die Datei bootstrap.properties.
2. Fügen Sie in dieser Datei die Systemeigenschaft **com.ibm.bi.logging.glug.hint.isready=false** hinzu, um die detaillierte Protokollierung zu aktivieren.
3. Starten Sie den Cognos-Service neu (von Cognos Configuration oder von einer Befehlszeile).

   Beim Start wird die Systemeigenschaft **com.ibm.bi.logging.glug.hint.isready=false** vom Protokollierungsservice geprüft, bevor weitere Services verfügbar sind.

   Der Neustart schlägt wieder fehl, dieses Mal enthält die Datei *Installationsposition*/logs/cognosserver.log allerdings detaillierte Protokolle. Beheben Sie anhand dieser Protokolle den Fehler.
4. Nach dem Beheben des Problems entfernen Sie die Systemeigenschaft **com.ibm.bi.logging.glug.hint.isready=false** aus der Datei bootstrap.properties, um die detaillierte Protokollierung zu inaktivieren. Starten Sie den Cognos-Service anschließend erneut. Nach dem Neustart wird die standardmäßige minimale Protokollierung wiederhergestellt.

   Tipp: Wenn die benötigte Zeit zum Starten des Cognos-Service für Sie nicht von Bedeutung ist und ausreichend Speicherplatz verfügbar ist, können Sie den Wert 'false' für diese Eigenschaft belassen. Auf diese Weise bleibt die detaillierte Protokollierung aktiviert, bis die Nachricht über den bereiten Dispatcher angezeigt wird.

Aktivieren von IBM Cognos Analytics for Jupyter Notebook

Administratoren können IBM Cognos Analytics zum Herstellen einer Verbindung zu einem Computer konfigurieren, auf dem IBM Cognos Analytics for Jupyter Notebook ausgeführt wird.

Vorbereitende Schritte

IBM Cognos Analytics for Jupyter Notebook muss auf einem anderen Computer installiert sein. Weitere Informationen finden Sie unter "Installieren von IBM Cognos Analytics for Jupyter Notebook" im Handbuch zur *Installation und Konfiguration von Cognos Analytics*.

Informationen zu diesem Vorgang

Eine Demonstration, wie IBM Cognos Analytics for Jupyter Notebook aktiviert wird, zeigt dieses Video.

Vorgehensweise

1. Notieren Sie den Namen des Computers, auf dem IBM Cognos Analytics for Jupyter Notebook installiert ist.
2. Wechseln Sie zu **Verwalten** > **Konfiguration** > **System** und wählen Sie **Umgebung** aus.
3. Geben Sie im Feld **Jupyter-Serviceposition** die folgende URL ein:

   http://*jupyter_notebook-servername*:*portnummer*

   Tipp: Verwenden Sie https://, wenn Sie SSL auf dem Jupyter Notebook-Server konfiguriert haben. Beachten Sie, dass der Jupyter Notebook-Server mit SSL geschützt werden muss, wenn der Cognos Analytics-Server mit SSL geschützt wird.
4. Klicken Sie auf **Anwenden**.

Ergebnisse

Die Konfigurationsänderung wird gespeichert und an alle Dispatcher weitergegeben. Sie müssen den Service nicht erneut starten, damit Benutzer eine Verbindung zu Jupyter Notebook herstellen können.

Nächste Schritte

Stellen Sie sicher, dass Sie Ihren vorgesehenen Jupyter Notebook-Benutzern entweder die Notebook-Funktion oder Rollen, die die Notebook-Funktion einschließen, zugeordnet haben. Weitere Informationen finden Sie im Abschnitt "Notebookfunktion" in der Veröffentlichung *IBM Cognos Analytics - Verwaltung*. Nach Ausführung dieser Aufgabe können Benutzer mit der Arbeit mit Jupyter Notebook in IBM Cognos Analytics beginnen.

Erweiterte Einstellungen

Sie können die erweiterten Systemeinstellungen konfigurieren, einschließlich eines Berechtigungsfilters und benutzerdefinierter Schlüssel-Wert-Paare.

Wichtig: Wenden Sie sich an den IBM Support, um detaillierte Informationen zur Konfiguration erweiterter Einstellungen zu erhalten.

Informationen zur Konfiguration erweiterter Systemeinstellungen über die Administrationskonsole finden Sie unter "Konfiguration erweiterter Einstellungen" im Handbuch *IBM Cognos AnalyticsVerwaltung und Sicherheit*.

Anpassen von Nachrichten im Banner für Alerts

11.1.5 Wenn Ihnen die Rolle 'Systemadministrator' zugeordnet wurde, können Sie eine Nachricht aktualisieren, die im Banner für Alerts angezeigt wird.

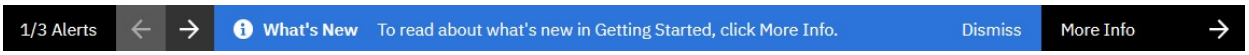
Anmerkung: Die Rolle 'Systemadministrator' ist für IBM Cognos Analytics on Cloud - Hosted-Kunden nicht verfügbar. Wenn Sie eine angepasste Alertnachricht in IBM Cognos Analytics on Cloud - Hosted anfordern möchten, wenden Sie sich bitte an den IBM Support.

Banner für Alerts

Das Banner für Alerts kann zwei Typen von Alerts anzeigen: 1) Alerts bei Neuerungen und 2) Wartungsalerts.

- Alerts bei Neuerungen

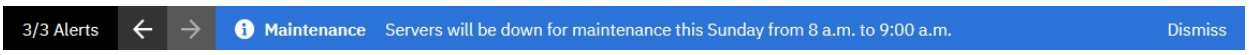
  Standardmäßig können Benutzer auf das Pfeilsymbol → im Banner für Alerts klicken, um zwei Nachrichten zu **Neuerungen** anzuzeigen:

- Wartungsalerts

  Ein Administrator kann einen Wartungsalert hinzufügen, um es Benutzern zu erleichtern, sich fortlaufend über unternehmensspezifische Details zu informieren.

Wartungsnachricht hinzufügen oder entfernen

Sie können eine Nachricht zum Banner für Alerts hinzufügen, um es Benutzern zu erleichtern, sich fortlaufend über anstehende Wartungen zu informieren.

1. Klicken Sie auf **Verwalten** > **Konfiguration** > **System** und wählen Sie **Erweiterte Einstellungen** aus.
2. Geben Sie `Glass.maintenanceMessage` in das Feld **Schlüssel** ein.

   Tipp: Bei der Eingabe muss die Groß-/Kleinschreibung wie angezeigt beachtet werden.
3. Geben Sie Ihre Wartungsnachricht in das Feld **Wert** ein.

Geben Sie in das Feld **Wert** zum Beispiel die folgende Nachricht ein: `Our servers will be down for maintenance this Saturday between 1:00 a.m. and 6:00 a.m.`.

In einem anderen Beispiel wird die Nachricht im Alertbanner in Englisch geschrieben, jedoch sprechen die Benutzer hauptsächlich Spanisch. Als Systemadministrator können Sie die Nachricht durch eine übersetzte Version ersetzen.

4. Führen Sie die folgenden Schritte aus, wenn Sie eine Wartungsnachricht entfernen wollen:
   a. Geben Sie `Glass.maintenanceMessage` in das Feld **Schlüssel** ein.
   b. Klicken Sie auf das Feld **Wert**.

      Tipp: Auch wenn ein Wert bereits gesetzt ist, wird dieser Wert erst dann angezeigt, wenn Sie auf das Feld klicken.

      Die aktuelle Wartungsnachricht wird angezeigt.
   c. Löschen Sie die Nachricht im Feld **Wert**.
5. Klicken Sie auf **Anwenden**.
6. Aktualisieren Sie Ihr Browserfenster.

Je nach der von Ihnen ausgewählten Einstellung, wird Ihre Nachrichten im Banner für Alerts angezeigt bzw. daraus entfernt.

Link zu einer Wartungsnachricht hinzufügen

Fügen Sie einen Link zu einer Wartungsnachricht hinzu, die die Benutzer auf eine Website verweist.

1. Klicken Sie auf **Verwalten** > **Konfiguration** > **System** und wählen Sie **Erweiterte Einstellungen** aus.
2. Geben Sie `Glass.maintenanceMessage` in das Feld **Schlüssel** ein.

   Tipp: Bei der Eingabe muss die Groß-/Kleinschreibung wie angezeigt beachtet werden.
3. Geben Sie in das Feld **Wert** Ihre Wartungsnachricht ein, einschließlich einer Referenz auf den Link, den Sie hinzufügen.

   Geben Sie beispielsweise `Für weitere Informationen zu unserem Produkt klicken Sie auf 'Weitere Informationen'` im Feld **Wert** ein.
4. Geben Sie `Glass.maintenanceLink` in das Feld **Schlüssel** ein.

   Tipp: Bei der Eingabe muss die Groß-/Kleinschreibung wie angezeigt beachtet werden.
5. Geben Sie in das Feld **Wert** die URL der Website ein, zu der Sie eine Verknüpfung herstellen möchten.
6. Klicken Sie auf **Anwenden**.
7. Aktualisieren Sie Ihr Browserfenster.

Ihre Wartungsnachricht wird im Banner für Alerts angezeigt. Wenn Sie rechts neben dem Banner für Alerts auf **Weitere Informationen** klicken, wird die Website, mit der Sie verknüpft sind, auf einer neuen Registerkarte geöffnet.

Alerts bei Neuerungen inaktivieren oder aktivieren

Geben Sie an, ob Nachrichten zu Neuerungen im Banner für Alerts angezeigt werden sollen oder nicht.

Anmerkung: Wenn Sie eine Wartungsnachricht erstellen, aber die Nachrichten zu Neuerungen inaktivieren, wird die Wartungsnachricht dennoch weiterhin angezeigt.

1. Klicken Sie auf **Verwalten** > **Konfiguration** > **System** und wählen Sie **Erweiterte Einstellungen** aus.
2. Geben Sie `Glass.disableWhatsNewAlerts` in das Feld **Schlüssel** ein.

   Tipp: Bei der Eingabe muss die Groß-/Kleinschreibung wie angezeigt beachtet werden.
3. Geben Sie `true` in das Feld **Wert** ein.
4. Wenn die Nachrichten zu Neuerungen wieder im Banner für Alerts angezeigt werden sollen, führen Sie die folgenden Schritte aus:

a. Geben Sie `Glass.disableWhatsNewAlerts` in das Feld **Schlüssel** ein.

b. Geben Sie `false` in das Feld **Wert** ein.

5. Klicken Sie auf **Anwenden**.
6. Aktualisieren Sie Ihr Browserfenster.

Je nach der von Ihnen ausgewählten Einstellung, werden nur die Nachrichten zu Neuerungen nicht mehr im Banner für Alerts angezeigt bzw. wieder im Banner für Alerts angezeigt.

Alle Nachrichten inaktivieren oder aktivieren

Sie können das Banner für Alerts entfernen. Dies führt dazu, dass den Benutzern weder die Nachrichten zu Neuerungen noch Ihre Wartungsnachrichten angezeigt werden.

1. Klicken Sie auf **Verwalten** > **Konfiguration** > **System** und wählen Sie **Erweiterte Einstellungen** aus.
2. Geben Sie `Glass.disableAlertEntry` in das Feld **Schlüssel** ein.

   Tipp: Bei der Eingabe muss die Groß-/Kleinschreibung wie angezeigt beachtet werden.
3. Geben Sie `true` in das Feld **Wert** ein.
4. Wenn die Nachrichten zu Neuerungen und - sofern vorhanden - eine Wartungsnachricht wieder im Banner für Alerts angezeigt werden sollen, führen Sie die folgenden Schritte aus:

   a. Geben Sie `Glass.disableAlertEntry` in das Feld **Schlüssel** ein.

   b. Geben Sie `false` in das Feld **Wert** ein.
5. Klicken Sie auf **Anwenden**.
6. Aktualisieren Sie Ihr Browserfenster.

Je nach der von Ihnen ausgewählten Einstellung, wird das Banner für Alerts den Benutzern entweder angezeigt oder nicht angezeigt.

Ausblenden des Schalters 'Willkommensseite anzeigen'

Sie können verhindern, dass Benutzern der Schalter **Willkommensseite anzeigen** angezeigt wird.

Mithilfe des Schalters **Willkommensseite anzeigen** können Sie auswählen, ob die Willkommensseite angezeigt wird, wenn Sie auf **Startseite** geklickt haben. Die Willkommensseite bietet einen schnellen Zugriff auf Einführungstouren, Videos und integrierte Beispiele.

Der Schalter **Willkommensseite anzeigen** wird standardmäßig angezeigt. Zum Ausblenden des Schalters führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Konfiguration** > **System** und wählen Sie **Erweiterte Einstellungen** aus.
2. Geben Sie `Glass.welcomeScreenDisabled` in das Feld **Schlüssel** ein.
3. Klicken Sie auf das Feld **Wert**.

   Der Standardwert `false` wird angezeigt.
4. Löschen Sie den Wert `false` und geben Sie den Wert `true` in das Feld **Wert** ein.
5. Klicken Sie auf **Anwenden**.
6. Aktualisieren Sie Ihr Browserfenster.

Ergebnisse

Die Willkommensseite wird durch Kacheln von Cognos Analytics-Assets ersetzt, mit denen Sie in letzter Zeit gearbeitet haben.

Definieren von Authentifizierungsparametern für Anmelde-URLs

Verwenden Sie die erweiterte Einstellung 'Glass.urlLoginParameters', um zuzulassen, dass Namespace-Anmeldeparameter, die in einer URL enthalten sind, an den Authentifizierungsprovider übergeben werden.

Beispiel: Der Administrator definiert die Parameter CAMNamespace, CAMPassword und CAMUsername. Ein Benutzer meldet sich nun an, indem er eine Cognos Analytics-ULR eingibt, an die seine Berechtigungsnachweise angehängt werden. Die Parameter werden anschließend zur Authentifizierung an Cognos Access Manager (CAM) übergeben. Die Anmelde-URL hat die folgende Form:

http://*ihr_server*:*ihr_port*/bi?CAMNamespace=*myNamespace*&CAMUsername=*myUser*&CAMPassword=*myPassword*.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Konfiguration** > **System** und wählen Sie **Erweiterte Einstellungen** aus.
2. Geben Sie `Glass.urlLoginParameters` in das Feld **Schlüssel** ein.
3. Geben Sie einen Parameternamen in das Feld **Wert** ein.

   Tipp: Sie können mehrere Parameternamen durch Kommas getrennt eingeben.
4. Klicken Sie auf **Anwenden**.

Setzen des SameSite-Attributs bei Cookies

11.1.7 Konfigurieren Sie das Cookie-Attribut `Configuration.cookieSameSite` , um domänenübergreifende Fehler in Ihrer Cognos-Umgebung zu vermeiden.

Um Cross-Site-Request-Forgery-Angriffe (CSRF) zu verhindern, haben Browser wie Chrome und Firefox den Standardwert des SameSite-Attributs für Cookies geändert. Wenn sich Ihre Cognos-Umgebung über mehrere Domänen erstreckt, können daher Fehler auftreten. Um diese Fehler zu vermeiden, können Sie die erweiterte Einstellung wie folgt konfigurieren:

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Konfiguration** > **System** und wählen Sie **Erweiterte Einstellungen** aus.
2. Geben Sie `Configuration.cookieSameSite` in das Feld **Schlüssel** ein.
3. Geben Sie `lax` in das Feld **Wert** ein.
4. Klicken Sie auf **Anwenden**.
5. Aktualisieren Sie Ihr Browserfenster.

Ergebnisse

Anwendungen in Ihrer Cognos-Umgebung mit einer anderen Domäne erzeugen keine Fehlernachrichten mehr.

Anpassen der Blockgröße von Dateien zum Hochladen in die Cloud

Sie können die Standardgröße der Datenblöcke ändern, die beim Hochladen von Dateien in eine Cloudspeicherposition übertragen werden.

Es kann notwendig sein, die Datenblockgröße anzupassen, wenn ein Benutzer bei dem Versuch, eine Datei in der Cloud zu speichern, die Nachricht `Fehler beim Hochladen von` *`berichtsname`* empfängt.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Konfiguration** > **System** und wählen Sie **Erweiterte Einstellungen** aus.
2. Geben Sie `multipart-chunk-size-mb` in das Feld **Schlüssel** ein.
3. Klicken Sie auf das Feld **Wert**.

Der Standardwert 15 wird angezeigt.

4. Löschen Sie den Wert 15 und geben Sie dann einen Wert ein, der größer ist als die Anzahl der MB jeglicher Dateien, die Sie in der Cloud speichern wollen.

   Geben Sie beispielsweise 50 in das Feld **Wert** ein.

5. Klicken Sie auf **Anwenden**.

Einstellen von Antwort-Headern für HTTP-Anfragen

Wenn in Ihrer Umgebung kein Web-Server enthalten ist, enthalten die Antwortheader für HTTP-Anforderungen keinen Wert für X-FRAME-OPTIONS. Die folgenden Schritte beschreiben, wie Sie X-FRAME-OPTIONS in die Antwort-Header aufnehmen.

Anmerkung: Es wird empfohlen, einen Web-Server in Ihrer Cognos Analytics-Umgebung zu installieren.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Konfiguration** > **System** und wählen Sie dann **Erweiterte Einstellungen**aus.
2. Geben Sie `BIHeaderFilter.responseHeaders` in das Feld **Schlüssel** ein.
3. Geben Sie `[{"name":"X-FRAME-OPTIONS","value":"SAMEORIGIN"}]` in das Feld **Wert** ein.
4. Klicken Sie auf **Anwenden**.
5. Geben Sie `BIResponseWrapper.staticExpiresDays` in das Feld **Schlüssel** ein.
6. Geben Sie 7 in das Feld **Wert** ein.

   Tipp: Damit wird der Wert für die HTTP-Antwort-Header "Expires" und "max-age" festgelegt, wenn auf GET-Anforderungen für statische Inhalte geantwortet wird.

7. Klicken Sie auf **Anwenden**.
8. Seite aktualisieren.

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 Windows -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 siehe *Maximale Anzahl Prozesse und Verbindungen*.

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 95.

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 Siehe *Gesicherte Funktionen und Funktionen*. .

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 94.

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 Artikel „Festlegen von Routing-Regeln für Dispatcher” auf Seite 95beschrieben.

Festlegen von Routing-Regeln für Dispatcher

Sie können Routing-Regeln für Servergruppen festlegen, die es Ihnen ermöglichen, bestimmte Typen von Berichten an unterschiedliche Server zu senden.

Vorgehensweise

1. Wählen Sie **Verwalten** > **Konfiguration** > **Routing-Regeln** aus.
2. Klicken Sie auf **Neue Routing-Regel**.

Tipp: Sie können das Stiftsymbol neben dem Tagnamen auswählen.

3. Ordnen Sie einen Datentag zu.
   a) Klicken Sie auf das nach unten zeigende Winkelsymbol im Feld **Datentag**.

      Alle vorhandenen Tags werden aufgelistet.
   b) Gehen Sie wie folgt vor, wenn Sie einen neuen Tag erstellen möchten:
      i) Klicken Sie auf **Neuer Datentag**.
      ii) Geben Sie einen Tagnamen ein.
      iii) Klicken Sie auf das Symbol 'Hinzufügen' .
      iv) Klicken Sie in **Teaminhalt** oder **Eigener Inhalt** auf mindestens ein Package, Datenmodul bzw. eine hochgeladene Datei.
      v) Klicken Sie auf **Auswählen**.
      vi) Klicken Sie auf **Erstellen**.
   c) Klicken Sie auf den Datentag, den Sie der Routing-Regel zuordnen möchten.

      Tipp: Um die Datenobjekte zu ändern, die einem Tag zugeordnet sind, oder um den Namen des Tags zu ändern, wählen Sie das Stiftsymbol neben dem Tagnamen aus.
4. Ordnen Sie einen Gruppentag zu.
   a) Klicken Sie auf das nach unten zeigende Winkelsymbol im Feld **Gruppentag**.

      Alle vorhandenen Tags werden aufgelistet.
   b) Gehen Sie wie folgt vor, wenn Sie einen neuen Tag erstellen möchten:
      i) Klicken Sie auf **Neuer Gruppentag**.
      ii) Geben Sie einen Tagnamen ein.
      iii) Klicken Sie auf das Symbol 'Hinzufügen' .
      iv) Klicken Sie im Fenster **Datei öffnen** auf einen Namespace, z. B. **Cognos**.
      v) Klicken Sie auf die Gruppen, die Sie der Routing-Regel zuordnen möchten.
      vi) Klicken Sie auf **Öffnen**.
      vii) Klicken Sie auf **Erstellen**.

         Der Tag wird erstellt.
   c) Klicken Sie auf den Gruppentag, den Sie der Routing-Regel zuordnen möchten.

      Tipp: Um die Gruppen zu ändern, die einem Tag zugeordnet sind, oder um den Namen des Tags zu ändern, wählen Sie das Stiftsymbol neben dem Tagnamen aus.
5. Ordnen Sie einen Rollentag zu.
   a) Klicken Sie auf das nach unten zeigende Winkelsymbol im Feld **Rollentag**.

      Alle vorhandenen Tags werden aufgelistet.
   b) Gehen Sie wie folgt vor, wenn Sie einen neuen Tag erstellen möchten:
      i) Klicken Sie auf **Neuer Rollentag**.
      ii) Geben Sie einen Tagnamen ein.
      iii) Klicken Sie auf das Symbol 'Hinzufügen' .
      iv) Klicken Sie im Fenster **Datei öffnen** auf einen Namespace, z. B. **Cognos**.
      v) Klicken Sie auf eine Rolle oder mehrere Rollen, die Sie der Routing-Regel zuordnen möchten.
      vi) Klicken Sie auf **Öffnen**.

vii) Klicken Sie auf **Erstellen**.

Der Tag wird erstellt.

c) Klicken Sie auf den Rollentag, den Sie der Routing-Regel zuordnen möchten.

Tipp: Um die Rollen zu ändern, die einem vorhandenen Tag zugeordnet sind, oder um den Namen des Tags zu ändern, wählen Sie das Stiftsymbol neben dem Tagnamen aus.

6. Ordnen Sie eine Servergruppe zu.

a) Klicken Sie auf das nach unten zeigende Winkelsymbol im Feld **Servergruppe**.

Alle vorhandenen Servergruppen werden aufgelistet.

b) Klicken Sie auf **Details für Servergruppe anzeigen**.

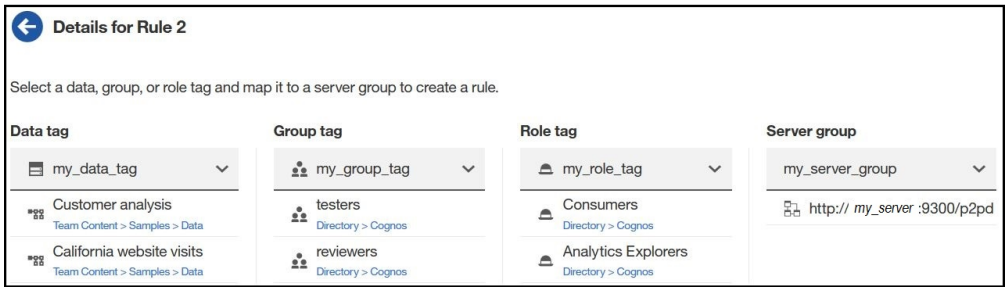
c) Wenn Servergruppen vorhanden sind, wird die URL jeder einzelnen Servergruppe aufgelistet. Fahren Sie mit Schritt „6.e" auf Seite 97 fort.

d) Falls die Nachricht **Keine Servergruppe gefunden** angezeigt wird, klicken Sie auf den Link **Erweiterte Administrationskonsole** und erstellen Sie dann eine Servergruppe.

e) Klicken Sie auf die Servergruppe, die Sie der Routing-Regel zuordnen möchten.

7. Sie können die Routing-Regeln wie folgt weiter ändern:

- Um zusätzliche Routing-Regeln zu erstellen, klicken Sie auf **Neue Routing-Regel**, wie in den vorherigen Schritten beschrieben.
- Um anzuzeigen, welche Datenobjekte, Gruppen, Rollen und Servergruppen-URLs den einzelnen Routing-Regeln zugeordnet sind, klicken Sie neben der Routing-Regel auf die Schaltfläche 'Mehr' und wählen Sie dann **Detailansicht** aus.



Tipp: Wenn Sie zur Liste der Routing-Regeln zurückkehren möchten, klicken Sie auf das Symbol 'Zurück' neben dem Anzeigentitel **Details für Regel *nummer***.

- Um eine Regel mit ähnlichen Zuordnungen wie eine bereits vorhandene Regel zu erstellen, klicken Sie neben der Routing-Regel auf die Schaltläche 'Mehr' und wählen Sie dann **Duplizieren** aus. Anschließend können Sie die Tags nach Bedarf ändern.
- Um eine Regel zu entfernen, klicken Sie neben der Routing-Regel auf die Schaltläche 'Mehr' und wählen Sie dann **Löschen** aus.

8. Klicken Sie auf **Änderungen anwenden**.

Ihre Änderungen an allen Routing-Regeln werden gespeichert.

Ergebnisse

Berichte werden jetzt von einem bestimmten Server verarbeitet, abhängig von den Routing-Tags, die dem Datenobjekt zugeordnet sind, aus dem der Bericht erstellt wurde, und/oder der Gruppe oder Rolle, die den Bericht ausführt.

Kapitel 5. 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

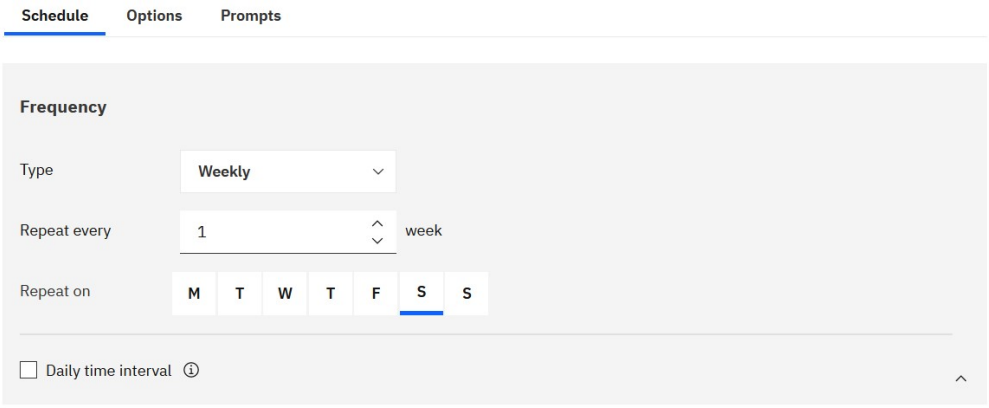
  Wenn Sie nur den Zugriff ausführen, werden Sie aufgefordert, sich bei der Datenbank anzumelden.
- dataSourceSignon-Ausführen

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*.

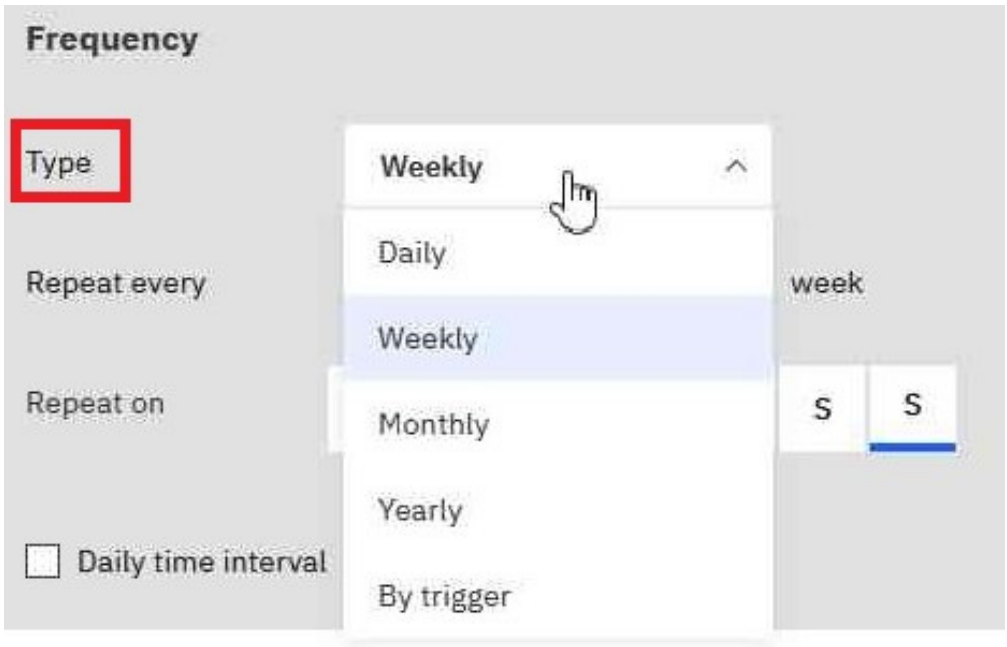
Um die Priorität für einen Eintrag festlegen zu können, müssen Sie über die erforderlichen Berechtigungen für das gesicherte Feature **Terminierungspriorität** verfügen. Weitere Informationen finden Sie unter Funktionen ..

Vorgehensweise

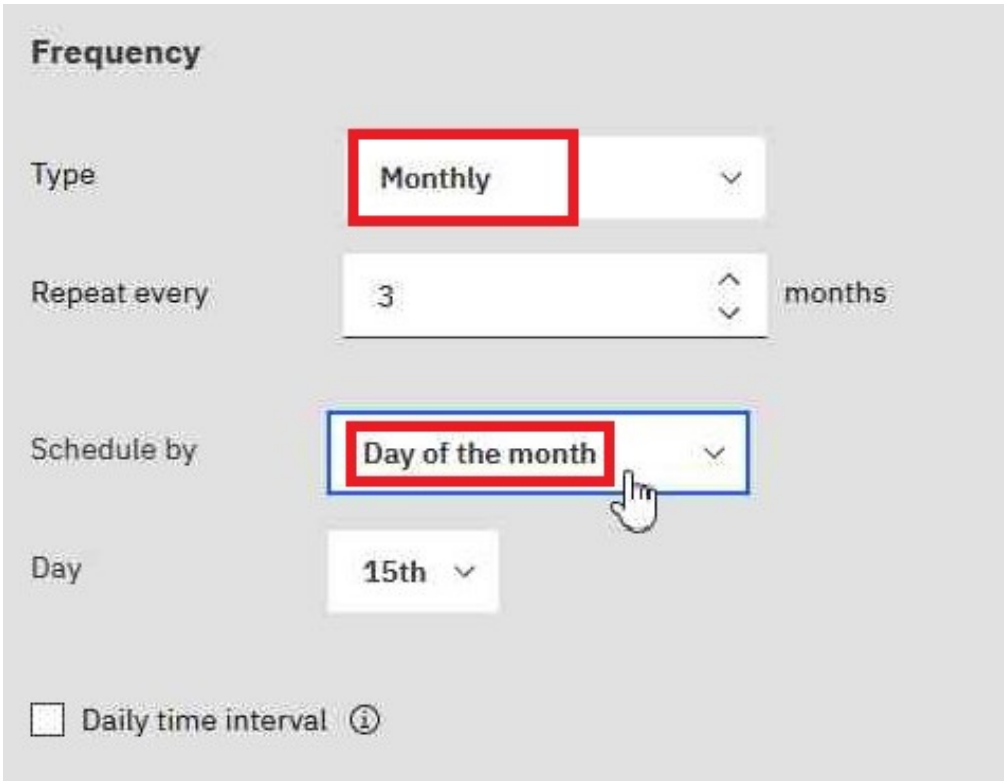
1. Klicken Sie auf das Symbol 'Mehr' ··· , und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie im Teilfenster **Eigenschaften** auf die Registerkarte **Zeitplan** und anschließend:
   - Klicken Sie auf **Zeitplan erstellen**.



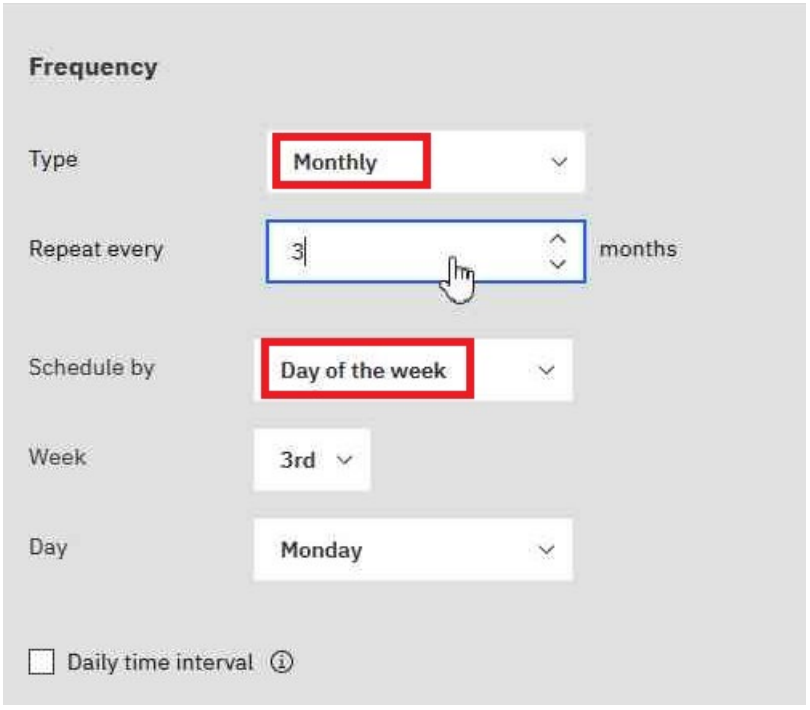
   Tipp: Die verfügbaren Optionen ändern sich bei jeder Auswahl. Warten Sie, bis das Teilfenster aktualisiert wird, bevor Sie weitere Einstellungen auswählen.
3. Geben Sie im Abschnitt **Häufigkeit** an, wann und wie häufig der Bericht ausgeführt wird:
   - Wählen Sie das **Typ** der Zeiteinheit aus, um 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,

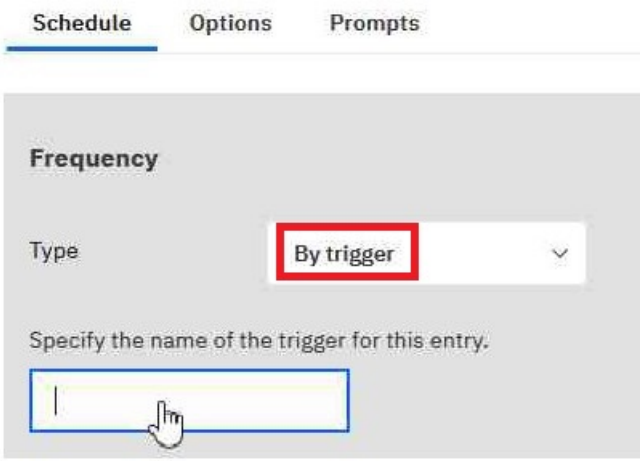


– Wählen Sie **Tag des Monats** im Feld **Planen nach** aus, damit Sie z. B. "Wiederholung alle 3 Monate am 15. des Monats" auswählen können (siehe Abbildung oben).



– 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).

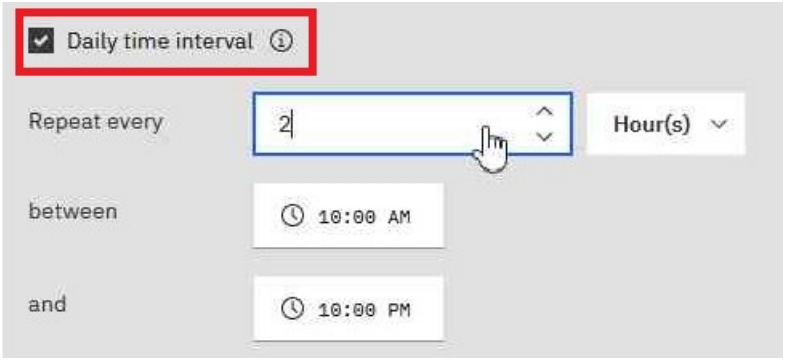
- Wenn Sie einen **Typ** -Wert von **Nach Auslöser**auswählen,



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`.

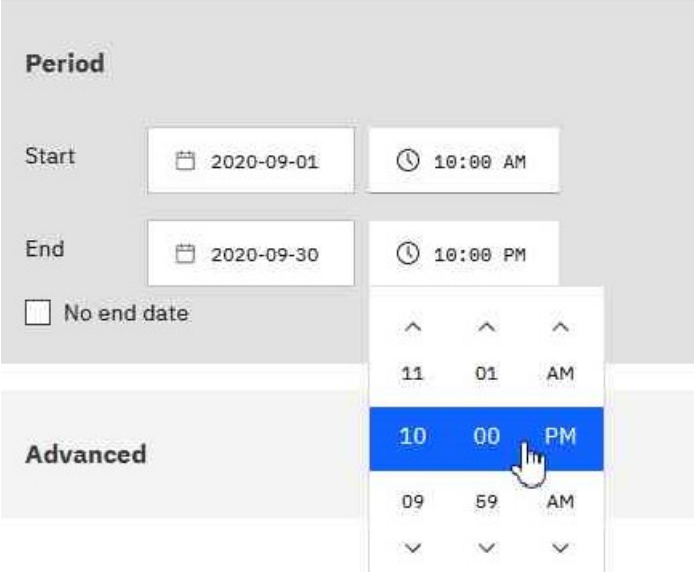
4. Wenn Sie eine tägliche Frequenz für Ihre geplanten Einträge auswählen möchten, gehen Sie wie folgt vor:
   - Wählen Sie das Markierungsfeld **Tägliches Zeitintervall** aus.



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** .

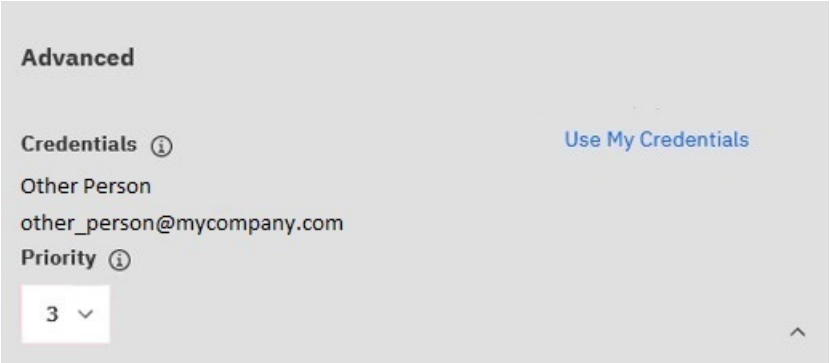


Tipp: Im obigen Beispiel wird der erste Berichtslauf am 1. September um 10:00 Uhr stattfinden, und der letzte Berichtslauf endet am 30. September um 22:00 Uhr.

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*.

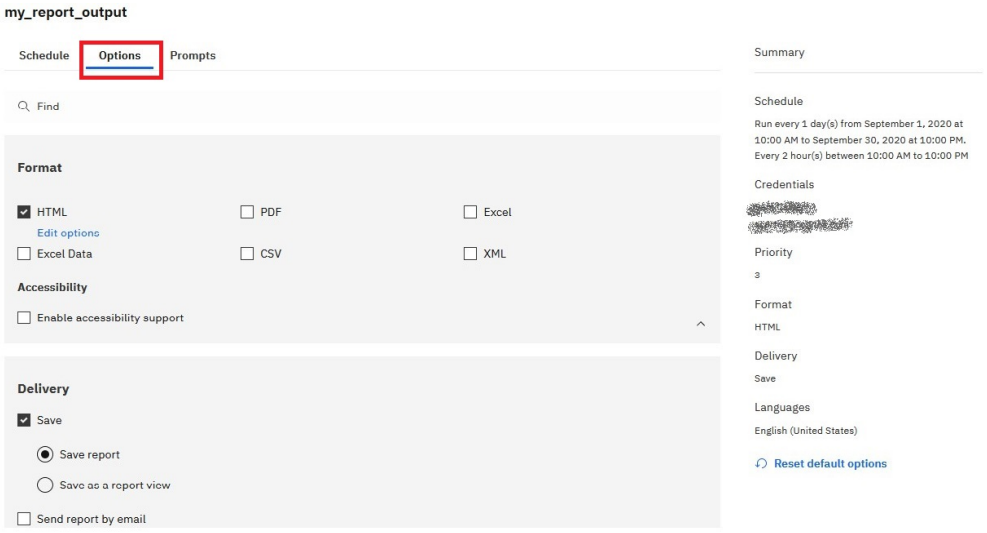
Informationen zum Feld "Priorität"

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** .

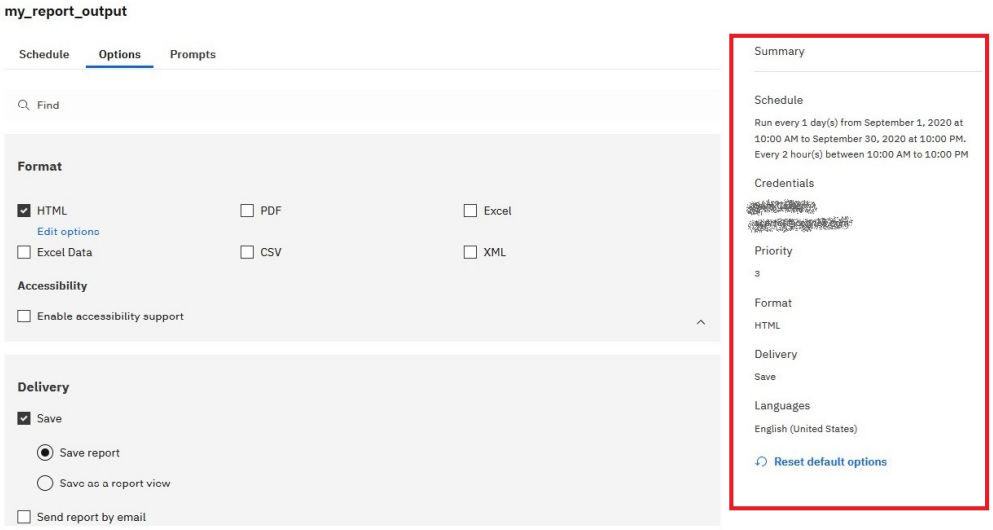


Tipp:

Die Standardoptionen werden angezeigt:

– **Format**: Nur HTML, behindertengerechte behindertengerechte Bedienung
– **Zustellung**: Nur Bericht speichern
– **Sprachen**: Nur Englisch

- Haben Sie das Teilfenster **Zusammenfassung** bemerkt?



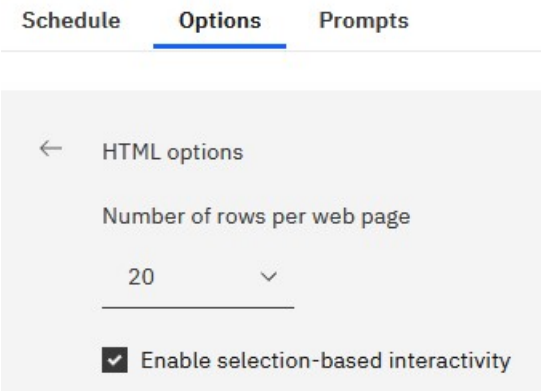
Tipp:

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.

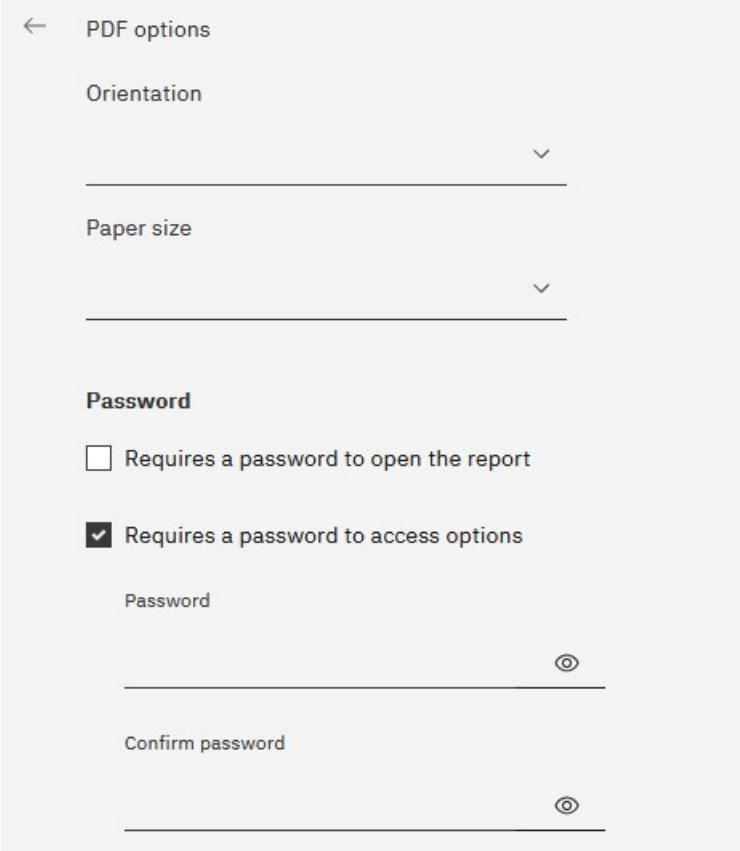


Abbildung 2. PDF-Optionen-Teil 1

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.

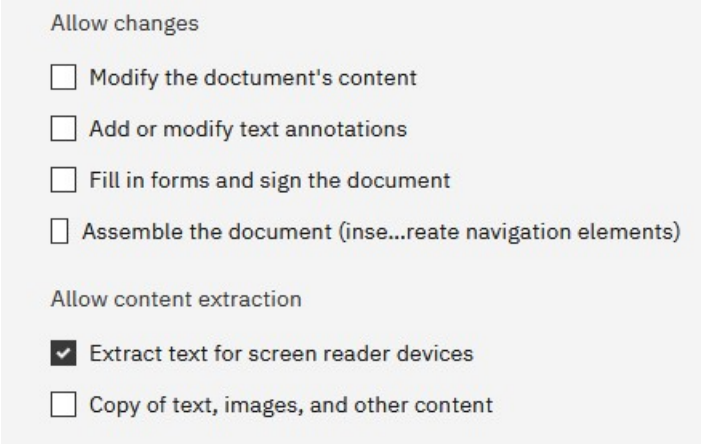


Abbildung 3. PDF-Optionen-Teil 2

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.

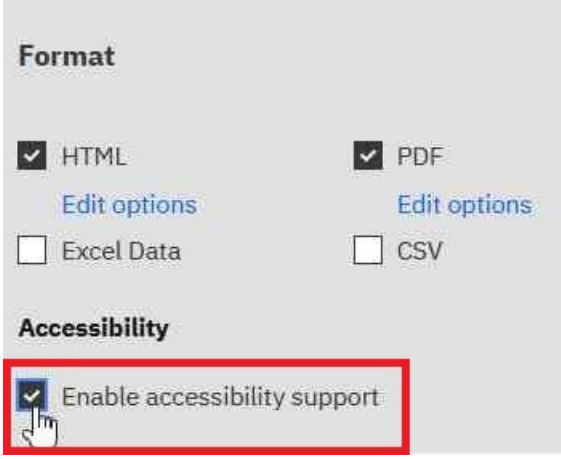


Abbildung 4. PDF-Optionen-Teil 1

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.

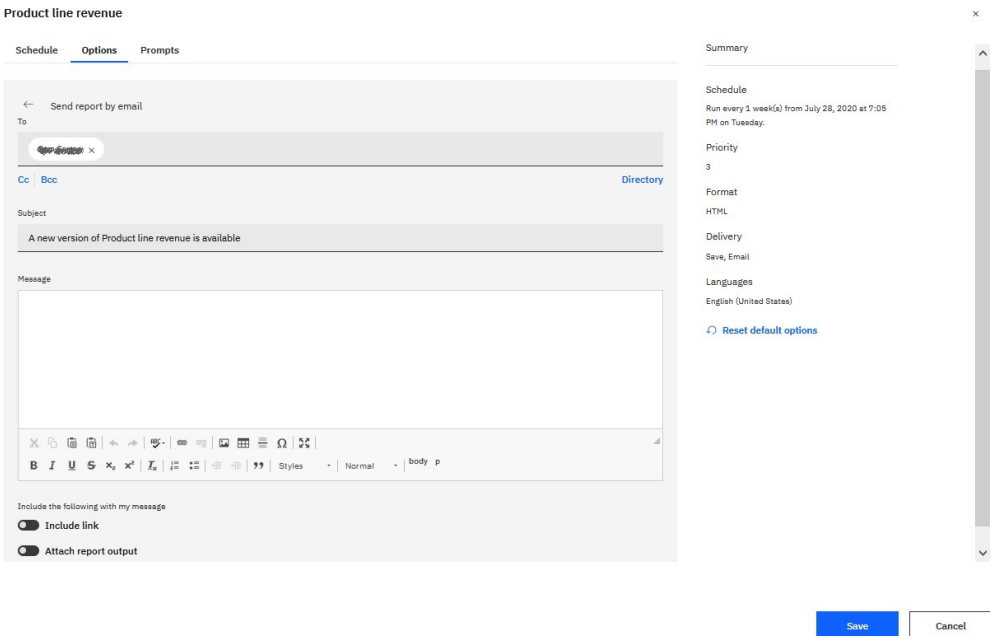
Abbildung 5. PDF-Optionen-Teil 1

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.

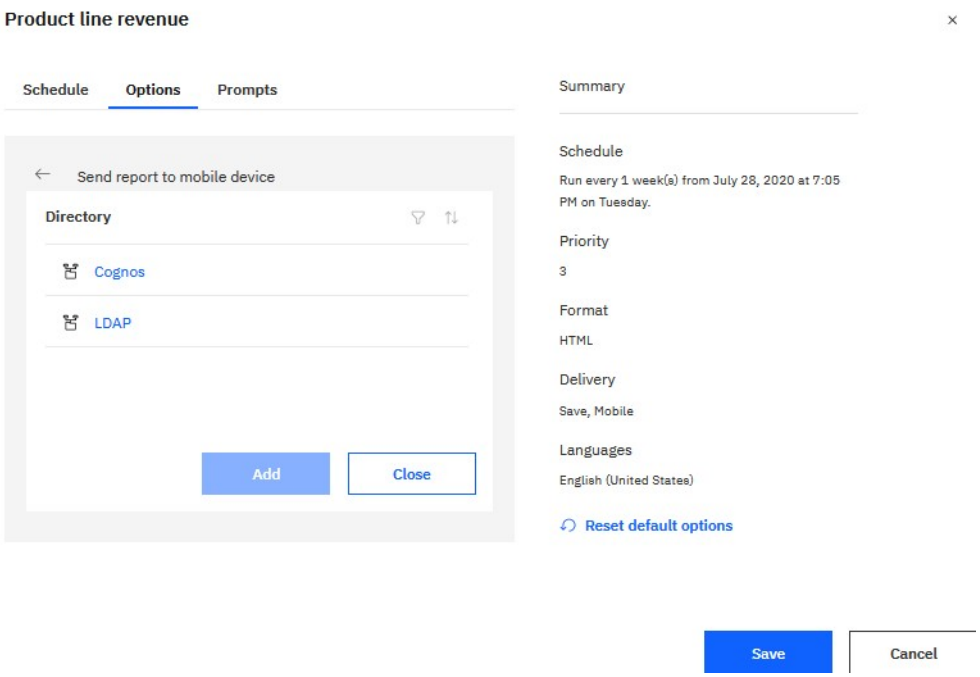


Tipp:

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.

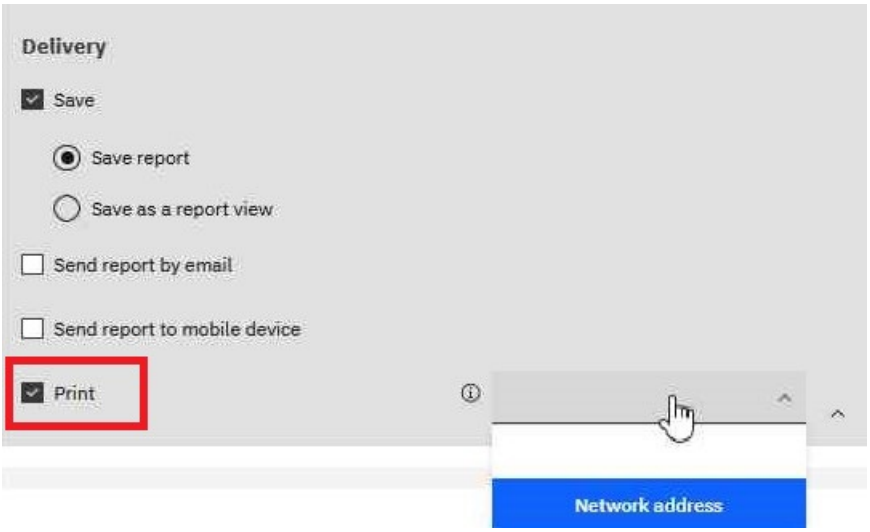


Tipp:

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.



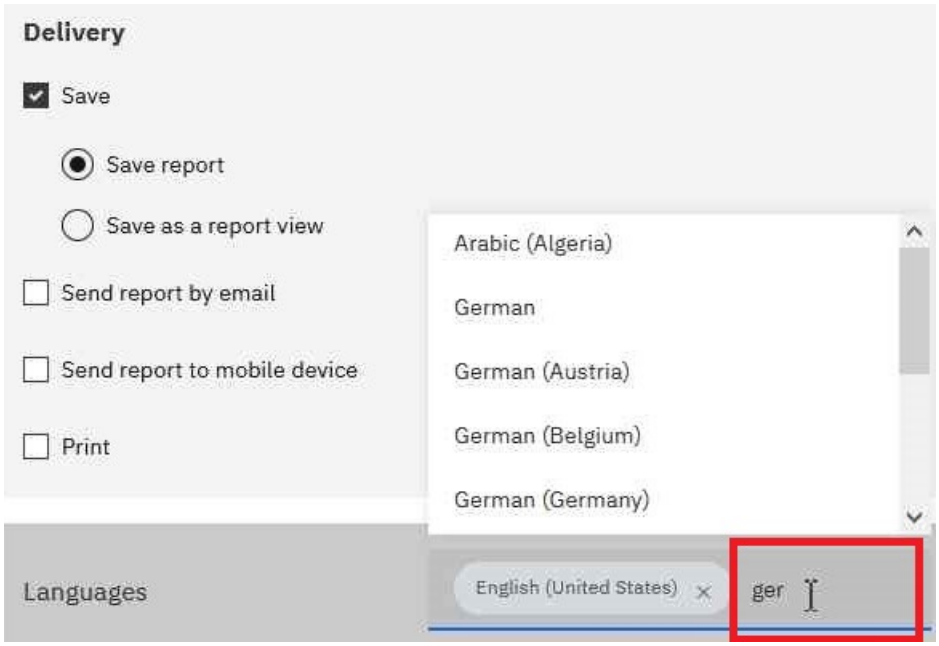
Tipp: Es kann bequem sein, dass Sie eine gedruckte Kopie eines Berichts haben.

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.

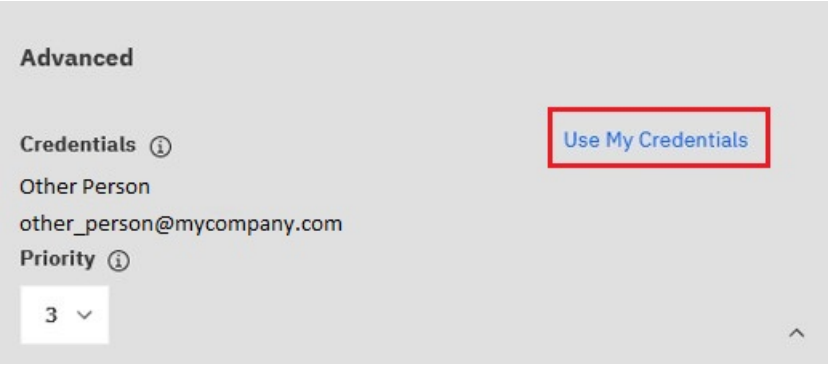
Eigentumsrecht an einem Zeitplan übernehmen

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.

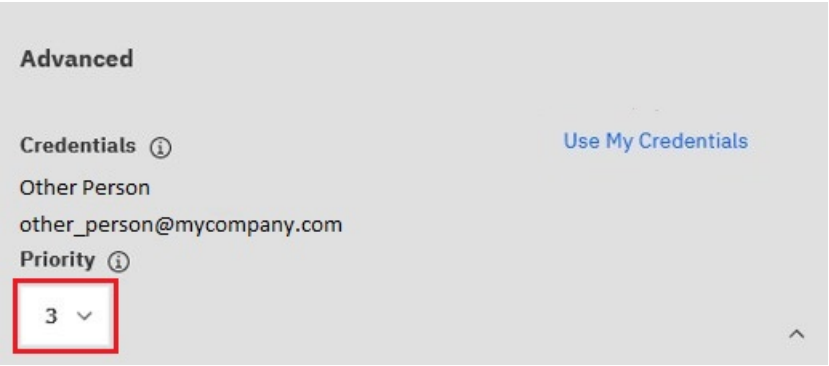
Wenn Sie einen Job terminieren, legen Sie die Priorität für den gesamten Job fest, nicht für einzelne Einträge innerhalb des Jobs. Möglicherweise möchten Sie eine niedrige Priorität für einen Job mit vielen Einträgen festlegen, damit andere Einträge in der Warteschlange nicht verzögert werden.

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 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 die Priorität eines Eintrags in der Warteschlange ändern.

Vorgehensweise

1. Klicken Sie im Menü **Verwalten** auf **Aktivitäten**.
2. Klicken Sie auf das Typsymbol, und klicken Sie dann auf **Bevorstehende**.
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.

Frühere Aktivitäten verwalten über das Tool 'Verwalten'

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.

Vorgehensweise

1. Klicken Sie im Menü **Verwalten** auf **Aktivitäten**.
2. Klicken Sie auf das Typsymbol, und klicken Sie dann auf **Vergangenheit**.

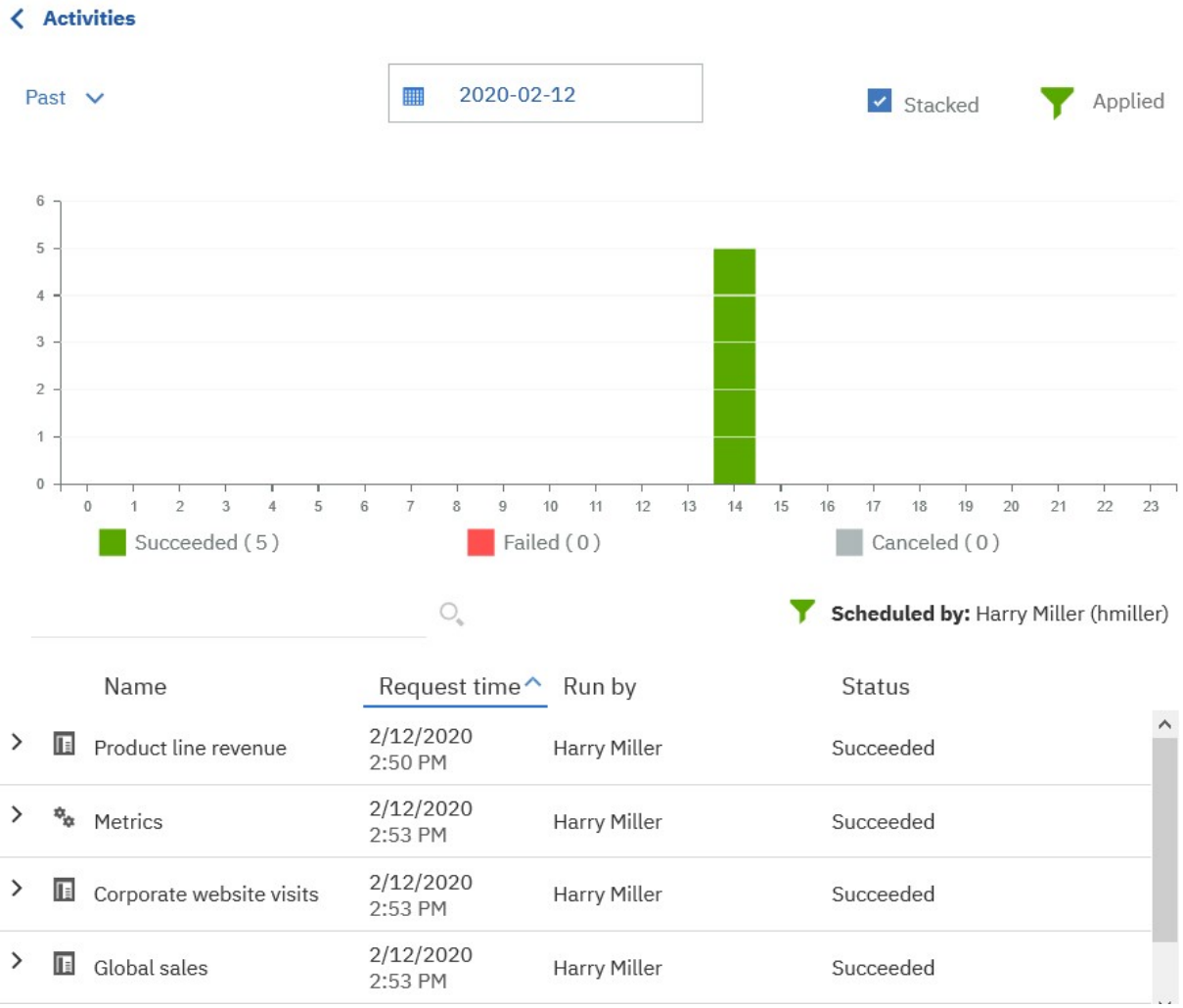
   Es wird ein Diagramm angezeigt, das zeigt, wann vergangene Aktivitäten ausgeführt wurden und ob sie erfolgreich waren, fehlgeschlagen sind oder abgebrochen wurden. Unterhalb des Diagramms werden Details zu den Aktivitäten aufgelistet.
3. Zum Filtern der Aktivitäten, die im Diagramm und in der Liste angezeigt werden, klicken Sie auf das Symbol 'Filter'.

   Tipp: Sie können nach den folgenden Attributen filtern:
   - Der Benutzer, der die Aktivität ausgeführt hat.
   - Der Aktivitätseigner.
   - Der Aktivitätsstatus.

- Der Aktivitätstyp.

Das folgende Diagramm zeigt ein Beispiel dafür, wie vergangene Aktivitäten über das Tool 'Verwalten' 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 Berichtsläufe werden in der Liste unter dem Job angezeigt, der sie enthielt.



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 eine einzelne Aktivität ausführen möchten, klicken Sie auf das Symbol 'Mehr' ... für den Eintrag und wählen Sie eine Aktion aus:

- Klicken Sie auf **Einmal ausführen** , um die Aktivität erneut auszuführen.
- Klicken Sie auf **Versionen anzeigen** , um Details zu den vorherigen Ausführungen des Berichts anzuzeigen.
- Klicken Sie auf **Details ausführen** , um Informationen über die letzte Ausführung des Berichts anzuzeigen.

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.

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, und -Benutzer filtern, der Eigner des Eintragsist.

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 ändern und die Ausführungsprotokoll anzeigen.

Vorgehensweise

1. Klicken Sie im Menü **Verwalten** auf **Aktivitäten**.
2. Klicken Sie auf das Typsymbol , und klicken Sie dann auf **Aktuell**.
3. Sie im Abschnitt **Filter** die Filteroptionen an, die Sie verwenden möchten.

   Tipp: Wenn Sie erweiterte Filteroptionen verwenden möchten, klicken Sie auf **Erweiterte Optionen**.
4. Klicken Sie auf **Anwenden**.

   In der Liste werden die von Ihnen ausgewählten Einträge angezeigt.

Kapitel 6. 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 115.

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 117.

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.

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 Siehe *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, 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.

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.**

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.
- Beenden Sie Benutzersitzungen und passen Sie Tenants an.
- Ändern Sie die Tenancy für Objekte im Content-Store.

Tipp: Die Rolle **Mieteradministratoren** ist einer der integrierten Einträge in Cognos-Namespace.

Informationen zur Rolle von **Systemadministratoren** in einer Multi-Tenant-Umgebung finden Sie unter Kapitel 6, „Mieterverwaltung”, auf Seite 115.

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.

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 115.

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.

Anpassen von Tenants

Sie können Motive auf einzelne Tenants anwenden. Sie können außerdem angeben, dass eine benutzerdefinierte Startseite, ein bestimmter Bericht oder ein bestimmtes Dashboard angezeigt wird, wenn ein Benutzer mit einer bestimmten Tenant-ID IBM Cognos Analytics öffnet. Darüber hinaus können Sie Standardbenutzerschnittstellenfeatures für Tenants entfernen.

Vor dem Festlegen von benutzerdefinierten Motiven und Startseiten (außer Dashboards oder Berichten) müssen Sie die benutzerdefinierten Motive bzw. Startseiten erstellen und hochladen. Weitere Informationen finden Sie unter Kapitel 9, „Anpassen von Cognos Analytics für alle Rollen”, auf Seite 201.

Klicken Sie in **Verwalten** > **Multi-Tenant-Funktionalität** auf einen Tenant. Das Slideout-Fenster für diesen Tenant enthält eine Registerkarte **Anpassung**. Weitere Informationen finden Sie unter „Anwenden von Motiven, Erweiterungen und Ansichten” auf Seite 227.

Festlegen einer Standardstartseite

Klicken Sie neben der Standardstartseite auf das Symbol 'Weiter' . Nun können Sie nach einem Dashboard oder Bericht suchen, das bzw. der als Standardstartseite verwendet werden soll, oder Sie können eine Ansicht in der Liste der Ansichten auswählen, die als Standardstartseite für alle Benutzer dieses Tenants verwendet werden soll.

Entfernen von Features

Sie können Benutzerschnittstellenfeatures auswählen, die für den Tenant entfernt werden sollen. Klicken Sie neben **Features** auf das Symbol 'Weiter' . Eine Liste mit Ansichten wird angezeigt. Diese Liste enthält sowohl die integrierten Ansichten als auch alle benutzerdefinierten Ansichten, die hochgeladen wurden. Klicken Sie auf eine Ansicht, um eine allgemeine Gruppierung der Features für die Ansicht anzuzeigen. Klicken Sie neben einer Gruppierung auf , um die Features einer unteren Ebene einzublenden. Sie können beliebige Features in dieser Liste oder in den darunter liegenden Ebenen abwählen. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Mit **Auf Standardwerte zurücksetzen** können Sie die Änderungen zurücksetzen.

Festlegen eines Standardmotivs

Klicken Sie neben einem Standardmotiv auf . Sie können ein Motiv in der Liste der Motive auswählen, das als Standardmotiv für diesen Tenant verwendet werden soll.

Erstellen eines benutzerdefinierten Ordners

Klicken Sie neben **Benutzerdefinierter Ordner** auf , um einen benutzerdefinierten Inhaltsordner für diesen Tenant anzugeben. Wenn sich ein Benutzer mit dieser Tenant-ID anmeldet, wird der benutzerdefinierte Ordner in der Navigationsleiste unter **Teaminhalt** angezeigt.

Festlegen der Standardposition für hochgeladene Dateien

11.1.5

Klicken Sie auf neben **Standardposition für Upload**, um einen Ordner in **Teaminhalt** als Standardposition für hochgeladene Dateien für diesen Tenant anzugeben.

Parameter

Fügen Sie hier Inhalt für Rollen ein.

Definieren von Regionseinstellungen für Tenants

Ein Systemadministrator kann Regionseinstellungen für einen Tenant angeben.

Die regionalen Einstellungen gelten für alle IBM Cognos Analytics-Komponenten, wie z. B. Berichterstellung, Dashboarding, Modellierung, Verwaltung usw. Ferner gelten diese Einstellungen für Begleitanwendungen wie IBM Cognos Analysis Studio, IBM Cognos Event Studio usw.

Die folgenden Einstellungen können angegeben werden:

Zeitzone
Die Zeitzone für den Tenantbenutzer.

Produktsprache
Die Sprache der IBM Cognos Analytics-Benutzerschnittstelle.

Inhaltssprache
Die Sprache, die zum Anzeigen und Erstellen von Inhalt in IBM Cognos Analytics verwendet wird, wie z. B. für Daten in Berichten, Dashboards und Storys.

Unterstützung bidirektionaler Sprachen
Diese Einstellung gilt für Sprachen wie Arabisch, Hebräisch, Urdu oder Farsi. Mit dieser Einstellung können Sie die Textrichtung in Eintragsnamen, Beschreibungen, Beschriftungen und QuickInfos, Eingabefeldern, Kommentaren sowie in gegliedertem Text wie E-Mail-Adressen, Dateipfade, Navigationspfade, URLs und Datums-/Zeitformate steuern.

Wählen Sie eine der folgenden Optionen in **Basisrichtung für Text** aus: **Von rechts nach links**, **Von links nach rechts**, **Kontextbezogen**. Wenn die Option **Kontextbezogen** ausgewählt wird, hängt die Textrichtung vom ersten Buchstaben im Text ab. Gehört der Buchstabe zu einer Rechts-nach-Links-Schrift, ist die Textrichtung von rechts nach links. Andernfalls ist die Textrichtung von links nach rechts. Zahlen und Sonderzeichen haben keinen Einfluss auf die Textrichtung. Wenn der Text zum Beispiel mit einer Zahl gefolgt von einem arabischen Buchstaben beginnt, ist die Richtung von rechts nach links. Wenn der Text dagegen mit einer Zahl gefolgt von einem lateinischen Buchstaben beginnt, ist die Richtung von links nach rechts.

Vorgehensweise

1. Wählen Sie in **Verwalten** die Registerkarte **Multi-Tenant-Funktionalität** aus.
2. Klicken Sie im Tenantkontextmenü auf **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Regional** und geben Sie die Einstellungen an.

Ergebnisse

Standardmäßig werden diese Einstellungen von allen Tenantbenutzern übernommen. Abhängig von ihren Zugriffsberechtigungen können die Benutzer diese Einstellungen später individuell gestalten.

Einrichten von Benachrichtigungen für Tenants

Ein Systemadministrator kann ein E-Mail-Konto mit dem Namen Tenantabsender konfigurieren, von dem die Tenantbenutzer E-Mails empfangen.

Das Tenantabsenderkonto setzt das beim Konfigurieren des E-Mail-Servers für IBM Cognos Analytics angegebene Standardabsenderkonto außer Kraft.

Tipp: Der Standardabsender wird in IBM Cognos Configuration unter **Datenzugriff** > **Benachrichtigung** konfiguriert.

Vorgehensweise

1. Wählen Sie in **Verwalten** die Registerkarte **Multi-Tenant-Funktionalität** aus.
2. Klicken Sie im Tenantkontextmenü auf **Eigenschaften**.
3. Wählen Sie auf der Registerkarte **Benachrichtigungen** die Option **Tenantabsender** aus und geben Sie die zugehörige E-Mail-Adresse an. Klicken Sie auf **Anwenden**.

Ergebnisse

Das E-Mail-Konto für den Tenantabsender ist jetzt für die Verteilung von IBM Cognos Analytics-Inhalten zugeordnet.

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 122.

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 Siehe *Implementierung von TenantInhalten*. .

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 121.

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 121.

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**.

Kapitel 7. Verwalten des Zugriffs

Administratoren können die Zugriffsebenen der Benutzer, Rollen und Gruppen auf Features und Komponenten in Cognos Analytics definieren.

Als Administrator sind Sie dafür verantwortlich, die vordefinierten Rollen im Namespace 'Cognos-Benutzer' zu schützen. Sie definieren, welche Funktionen den einzelnen Benutzern, Gruppen und Rollen zugeordnet werden. Sie verwalten auch Funktionen, soweit sich diese auf Lizenzrollenberechtigungen beziehen.

Sicherheitseinstellungen nach der Installation

Ihre IBM Cognos-Softwareinstallation muss bereits für die Verwendung eines Authentifizierungsproviders konfiguriert sein. Dies ist im IBM Cognos Analytics-Konfigurationsleitfaden dokumentiert.

Wenn die vordefinierten Rollen während der Initialisierung des Content Stores erstellt werden, ist die Gruppe **Jeder** ein Mitglied der Rolle **Systemadministratoren**. Das bedeutet, dass alle Benutzer uneingeschränkten Zugriff auf den Content Store haben. Um diesen Zugriff einzuschränken, müssen Sie vertrauenswürdige Benutzer als Mitglieder dieser Rolle hinzufügen und dann die Gruppe 'Jeder' aus der Mitgliedschaft entfernen.

Außerdem müssen Sie auch die Mitgliedschaft der vordefinierten Rollen ändern, zu denen die Gruppe **Jeder** gehört, wie **Konsumenten**, **Abfragebenutzer** und **Autoren**. Nehmen Sie daran ähnliche Änderungen vor wie an der Rolle **Systemadministratoren**. Diese Änderungen sollten auch Lizenzbedingungen berücksichtigen.

Wenn Sie die vordefinierten Rollen nicht verwenden möchten, können Sie sie löschen.

Um den Namespace **Cognos-Benutzer** zu schützen, ändern Sie seine ursprünglichen Zugriffsberechtigungen, indem Sie Zugriff auf die erforderlichen Benutzer erteilen.

Wenn Sie Zugriffsberechtigungen festlegen, sollten Sie der Gruppe 'Jeder' nicht explizit Zugriff auf Einträge verweigern. Das Verweigern des Zugriffs überschreibt alle anderen Sicherheitsrichtlinien für den Eintrag. Wenn Sie den Zugriff auf den Eintrag für 'Jeder' verweigern würden, wäre der Eintrag unbrauchbar.

Für eine dauerhaft geschützte Installation sollten Benutzern nur die Berechtigungen und Funktionen erteilt werden, die erforderlich sind, damit diese die ihnen zugewiesenen Aufgaben erledigen können. **Leser** wären normalerweise auf Lese- und Transitberechtigungen für **Öffentliche Ordner** beschränkt und dürften in keinem Studio Berichte erstellen. Konsumenten wären üblicherweise auf Lese-, Transit- und Ausführungsberechtigungen beschränkt.

Bestimmte Funktionen wie **HTML-Elemente im Bericht** und **Benutzerdefiniertes SQL** sollten kompakt verwaltet werden. Diese Funktionen werden während des Berichterstellungsprozesses ebenso wie während der Ausführung von Berichten geprüft. Wenn ein Konsument einen Bericht ausführen muss, für den diese Funktionen erforderlich sind, können Sie unter Umständen das Feature **Als Eigentümer ausführen** verwenden, um die Anzahl der Systembenutzer zu begrenzen, die diese Funktionen benötigen. Das Feature **Als Eigentümer ausführen** verwendet die Berechtigungsnachweise des Berichtseigentümers, um Funktionsprüfungen auszuführen und auf Daten zuzugreifen.

Schützen von Systemadministratoren und Standardrollen

Einer der ersten Schritte beim Einrichten der Sicherheit für die IBM Cognos-Umgebung besteht darin, die ursprüngliche Mitgliedschaft der Rolle 'Systemadministratoren' und anderer Standardrollen zu ändern.

Wenn die Gruppe **Jeder** ein Mitglied einer Standardrolle ist, entfernen Sie die Gruppe aus der Rollenmitgliedschaft.

Anmerkung: Eine Liste der Standardfunktionen, die den einzelnen Rollen zugeordnet sind, finden Sie in „Anfängliche Zugriffsberechtigungen für Funktionen” auf Seite 142.

Vorgehensweise

1. Klicken Sie unter **Verwalten** > **Personen** auf **Konten**.
2. Klicken Sie auf den Namespace **Cognos**.
3. Klicken Sie für die Rolle, die Sie ändern möchten, auf das Symbol 'Mehr'  , und klicken Sie dann auf **Eigenschaften**.
4. Ändern Sie auf der Registerkarte **Mitglieder** die Rollenmitgliedschaft:
   - Stellen Sie sicher, dass ein oder mehrere Benutzer, die in Ihrem Authentifizierungsprovider definiert sind, Mitglieder sind.
   - Entfernen Sie die Gruppe **Jeder**, wenn diese Gruppe ein Mitglied der Rolle ist.
5. 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 dann auf **Anwenden**.
6. Wiederholen Sie die Schritte 3 bis 5 für jede Rolle, die Sie ändern möchten.

Schützen des Cognos-Namespace

Sie können den Cognos-Namespace wie folgt einrichten.

Vorgehensweise

1. Klicken Sie unter **Verwalten** > **Personen** auf **Konten**.
2. Klicken Sie neben dem Cognos-Namespace auf das Symbol 'Mehr'  und klicken Sie dann auf **Eigenschaften**.
3. Legen Sie auf der Registerkarte **Berechtigungen** Zugriffsberechtigungen für den **Cognos**-Namespace fest, um zu verhindern, dass berechtigte Benutzer den Inhalt erstellen, aktualisieren oder löschen.

   Wir empfehlen, dass Sie die Gruppe 'Jeder' entfernen. Sie können Sie jedoch, abhängig von Ihren Anforderungen, auch behalten.
4. Wählen Sie gegebenenfalls das Kontrollkästchen **Für alle untergeordneten Elemente anwenden** aus.
5. Klicken Sie auf **Anwenden**.

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 179.

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 142.

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 154 aufgelistet.

Dieser Funktion ist die folgende gesicherte Funktion zugeordnet:

Erstellen/Bearbeiten

Diese geschützte Funktion steuert den Zugriff auf die Funktionen von **Neu** > **Dashboard** und **Neu** > **Geschichte** . Benutzer benötigen Ausführungsberechtigungen für die Dashboard-und Erstellungs-/Bearbeitungsfunktion, um Dashboards und Storys zu erstellen oder zu bearbeiten.

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* . 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.

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 3. 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 3. 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 4. 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 5. 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.
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 5. 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 6. 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 7. 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 8. 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.

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.

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" auf Seite 179.

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 „Zugriffsberechtigungen und Berechtigungsnachweise" auf Seite 135.

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 9. 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 10. 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			✓		✓
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 11. 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				✓	✓
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			✓		✓

Tabelle 11. 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
Metrische Studio-Verwaltung	Verzeichnisadministratoren	Zuordnen				✓	✓
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 11. 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 12. 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 13. 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 14. 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 15. 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 16. 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 17. 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 18. 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 19. 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 19. 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 20. 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 20. 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 21. 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 22. 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 23. Dashboardfunktionalität und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Analyse-Explorers	Zugriff			✓		✓
Analysebenutzer	Zugriff			✓		✓
Analyseanzeige-funktionen	Zugriff			✓		✓
Verzeichnisadmi-nistratoren	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 24. 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 25. 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 26. 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 27. 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 28. 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 29. 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 30. 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 31. 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 32. 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 32. 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 33. 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 34. 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 35. 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 35. 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 36. 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 37. 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 38. 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 39. 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 40. Generieren von CSV-Ausgabefunktionen und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verzeichnisadministratoren	Zuordnen				✓	✓

Tabelle 40. Generieren von CSV-Ausgabefunktionen und Berechtigungen für zugehörige Gruppen und Rollen (Forts.)						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
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 41. 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 42. 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 43. 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 44. 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 45. 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 46. 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 47. 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 48. 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 49. 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 50. 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 51. 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 52. 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 53. 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 54. 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 55. 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 56. 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 57. Query Studio-Funktion und Berechtigungen für zugehörige Gruppen und Rollen						
Gruppe oder Rolle	**Berechtigungsstufe**	**Berechtigungstyp**				
		Lesen	**Schreiben**	**Ausführen**	**Richtlinie festlegen**	**Traverse**
Verfasser	Zugriff			✓		✓

Tabelle 57. 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 58. 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 59. 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 60. 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 61. 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 62. 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 63. 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 64. 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 65. 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 66. 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 67. 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				✓	✓
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 68. 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 69. 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 70. Hochladen von Dateifunktionen und Berechtigungen für zugehörige Gruppen und Rollen

Gruppe oder Rolle	Berechtigungsstufe	Berechtigungstyp				
		Lesen	Schreiben	Ausführen	Richtlinie festlegen	Traverse
Jeder	Zugriff			✓		✓

Tabelle 70. Hochladen von Dateifunktionen und Berechtigungen 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			✓		✓

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 71. 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 72. 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 73. 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			✓		✓

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 142.
9. Klicken Sie auf **Anwenden**.
10. Klicken Sie auf **OK** , wenn Sie fertig sind.

Verwalten von Lizenzen

Systemadministratoren müssen die IBM Cognos Analytics-Lizenznutzung überwachen.

In den Lizenzinformationen in IBM Cognos Analytics werden die Lizenzen angezeigt, die von einzelnen Benutzern bei ihrer letzten Anmeldung verwendet wurden. Geänderte Funktionen von Benutzern werden in deren Lizenznutzung nicht berücksichtigt, bis die Benutzer sich erneut anmelden. Für bestehende Benutzer sind die Informationen zur Lizenznutzung außerdem unvollständig, bis alle Benutzer sich erneut anmelden.

Ein Bericht zur Lizenznutzung wird erstellt, wenn die Lizenzseite unter **Verwalten** > **Lizenzen** zum ersten Mal geöffnet, die Schaltfläche **Aktualisieren** angeklickt oder das Produkt neu gestartet wird.

Der grundlegende Bericht enthält Informationen zur Lizenznutzung nach Benutzern. Einige Kunden möchten möglicherweise zusätzliche Berichtsfunktionen nutzen, zum Beispiel für Informationen zur Lizenznutzung nach Tenants.

IBM Cognos Analytics verfügt über verschiedene Typen von lizenzierten Rollen, wobei jeder Typ anderen Funktionen zugeordnet ist. In diesem Artikel (https://www.ibm.com/support/docview.wss?uid=ibm10735275) finden Sie die Matrix der Funktionen und Berechtigungen, auf der das IBM Cognos Analytics-Lizenzierungsmodell basiert.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Lizenzen**, um auf die Lizenzseite in IBM Cognos Analytics zuzugreifen.
2. Klicken Sie auf das Feld **Eigene** für die lizenzierte Rolle, um die Anzahl eigener Lizenzen einzugeben. Geben Sie die Anzahl ein und klicken Sie anschließend auf **Anwenden**, um den Wert zu speichern.

   Dieser Wert wird nur zu Informationszwecken verwendet und nicht in den Bericht zur Lizenznutzung einbezogen.
3. Klicken Sie auf **Aktualisieren**, um den Bericht zur Lizenznutzung zu erstellen.

   Sie können den Bericht beliebig oft erstellen.
4. Klicken Sie auf das Symbol zum Anzeigen von Details  , um die Lizenzinformationen für eine bestimmte Rolle anzuzeigen.

   Bei diesen Informationen handelt es sich um eine Teilmenge der Informationen aus dem Gesamtbericht.
5. Wenn Sie den Gesamtbericht anzeigen möchten, klicken Sie auf **Exportieren**, um die Informationen in einer CSV-Datei zu speichern, und öffnen Sie anschließend die Datei.

   Tipp: Die Werte in der Spalte **Ebene** der exportierten Datei entsprechen bestimmten Lizenzrollen wie folgt:

Ebene	Lizenzrolle
3	Analytics-Administrator
2	Analytics-Explorer
1	Analytics-Benutzer

Ebene	Lizenzrolle
0	Analytics-Anzeigeberechtigter
-1	Die Lizenzrolle ist unbekannt, da sich der Benutzer noch nicht angemeldet hat.

Nächste Schritte

Weitere Informationen enthalten die folgenden Abschnitte:

- Predefined license roles
- Assigning capabilities based on license roles
- Upgrade scenario: If your customized roles have the same names as the new license roles

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 4.

In der folgenden Tabelle werden die vordefinierten Lizenzrollen aufgelistet.

Tabelle 74. 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.
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 189.

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 75. 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.
	Datenquellenverbindungen		✓	✓	✓	
	Verteilerlisten und Kontakte				✓	
	Visualisierungen verwalten				✓	
	Metrische Studio-Verwaltung				✓	Sie benötigen eine separate Metriklizenz

Tabelle 75. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)

Funktion	Gesicherte Funktion	Analyseviewer	Analysebenutzer	Analyseexplorer	Analyseadministrator	Kommentare
	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				✓	
	Benutzer, Gruppen und Rollen				✓	
AI			✓	✓	✓	
	Lernen	✓	✓	✓	✓	
	Assistent verwenden		✓	✓	✓	
Analysestudio			✓	✓	✓	
11.1.7 -Ausgaben anhängen			✓	✓	✓	
Cognos Analytics for Mobile		✓	✓	✓	✓	

Tabelle 75. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)

Funktion	Gesicherte Funktion	Analyseviewer	Analysebenutzer	Analyseexplorer	Analyseadministrator	Kommentare
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
	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			✓	✓	✓	

Tabelle 75. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)						
Funktion	**Gesicherte Funktion**	**Analyseviewer**	**Analysebenutzer**	**Analyseexplorer**	**Analyseadministrator**	**Kommentare**
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			✓	✓	✓	
Indexierte Suche ausführen		✓	✓	✓	✓	
Executive-Dashboard			✓	✓	✓	
	Erweiterte Dashboard-Funktionen verwenden		✓	✓	✓	
	Interaktive Dashboard-Features verwenden		✓	✓	✓	
Exploration			✓	✓	✓	
Externe Repositorys		✓	✓	✓	✓	

Tabelle 75. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)

Funktion	Gesicherte Funktion	Analyseviewer	Analysebenutzer	Analyseexplorer	Analyseadministrator	Kommentare
	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
Einträge ausblenden		✓	✓	✓	✓	
Relationale Metadaten importieren				✓	✓	
Job			✓	✓	✓	
Abstammung		✓	✓	✓	✓	
Inhalt verwalten					✓	
Eigene Datenquellensignonen verwalten			✓	✓	✓	

Tabelle 75. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)

Funktion	Gesicherte Funktion	Analyseviewer	Analysebenutzer	Analyseexplorer	Analyseadministrator	Kommentare
Metrikstudio			✓	✓	✓	Sie benötigen eine separate Metrikklizenz
	Ansicht bearbeiten		✓	✓	✓	Sie benötigen eine separate Metrikklizenz
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
PowerPlay Studio			✓	✓	✓	Sie benötigen eine separate PowerPlay-Lizenz
Abfragestudio			✓	✓	✓	
	Erweitert		✓	✓	✓	
	Erstellen		✓	✓	✓	
Berichtsstudio			✓	✓	✓	
	Externe Daten zulassen		✓	✓	✓	
	Platzen		✓	✓	✓	

Tabelle 75. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)

Funktion	Gesicherte Funktion	Analyseviewer	Analysebenutzer	Analyseexplorer	Analyseadministrator	Kommentare
	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		✓	✓	✓	
	Zeitplan für Woche		✓	✓	✓	
	Zeitplan für Jahr		✓	✓	✓	
	Nach Priorität planen		✓	✓	✓	
Self-Service-Paketassistent				✓	✓	
Eingabespezifische Funktionen festlegen			✓	✓	✓	
Share Pin Board			✓	✓	✓	

Tabelle 75. Funktionen von Cognos Analytics 11.1 nach Lizenzrollen (Forts.)						
Funktion	**Gesicherte Funktion**	**Analyseviewer**	**Analysebenutzer**	**Analyseexplorer**	**Analyseadministrator**	**Kommentare**
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 181.

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 181 .

- 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**.

Kapitel 8. Konfigurieren von Plattformen für gemeinsames Arbeiten

Sie können Cognos Analytics so konfigurieren, dass die Benutzer ihren Inhalt in **Slack** oder als **E-Mail** senden können.

Tipp: Sie können diese Funktion auch anpassen, um zu beschränken, auf welche Weise Personen in ausgewählten Rollen Inhalt senden können. Weitere Informationen finden Sie unter „Beispiel: Selektive Inaktivierung der gemeinsamen Nutzung von Inhalten per E-Mail” auf Seite 199.

Informationen hierzu finden Sie im Abschnitt "Inhalte gemeinsam nutzen" im *IBM Cognos Analytics Einführung - Benutzerhandbuch*.

Integration in eine Plattform für gemeinsames Arbeiten

Wenn Ihr Unternehmen das Slack*-Tool für die Zusammenarbeit verwendet, können Sie einen oder mehrere Slack-Arbeitsbereiche in Cognos Analytics integrieren. Cognos Analytics-Benutzer können dann eine Verbindung zu den Slack-Arbeitsbereichen herstellen, um Nachrichten und Cognos Analytics-Inhalte mit anderen Benutzern zu teilen.

Informationen zu den anfänglichen Zugriffsberechtigungen, die für die Verwaltung der Zusammenarbeit erteilt werden, finden Sie in "Collaboration Administration" im Abschnitt "Anfängliche Zugriffsberechtigungen für Funktionen" in *IBM Cognos Analytics - Verwaltung und Sicherheit*.

Informationen dazu, wie Benutzer Inhalte teilen können, finden Sie im Handbuch *IBM Cognos Analytics - Einführung*.

Anmerkung: Plattformen für gemeinsames Arbeiten in IBM Cognos Analytics wurden nicht von Slack Technologies Incorporated entwickelt, sind nicht mit Slack Technologies Incorporated verbunden und werden von Slack Technologies Incorporated nicht unterstützt.

Erstellen einer Slack-Anwendung

Erstellen Sie in Slack eine Anwendung, sodass Sie in Cognos Analytics eine Verbindung zu Slack herstellen können.

Vorbereitende Schritte

Ihr Unternehmen muss über ein registriertes Slack-Konto verfügen.

Vorgehensweise

1. Gehen Sie zu https://api.slack.com/apps.
2. Melden Sie sich bei dem Slack-Konto für Ihr Unternehmen an.
3. Klicken Sie auf **Neue App erstellen**.
4. Geben Sie im Dialog **Slack-App erstellen** einen Namen für Ihre Anwendung ein, z. B. `Cognos Analytics`, und wählen Sie **Slack-Arbeitsbereich für Entwicklung** aus.
5. Wählen Sie den Arbeitsbereich aus, bei dem Sie sich angemeldet haben.
6. Klicken Sie auf **App erstellen**.

   Die Slack-Anwendung wird erstellt.
7. Klicken Sie auf der Seite **Slack-API** auf die Registerkarte **Basisinformationen** und blättern Sie nach unten zum Abschnitt **App-Berechtigungsnachweise**.
8. Notieren Sie sich die Werte für **Client-ID** und **Geheimer Clientschlüssel**. Sie benötigen diese Angaben beim Konfigurieren von Slack in Cognos Analytics.

Tipp: Klicken Sie in jedem Feld auf die Schaltfläche **Anzeigen**, um die Werte zu sehen.

9. Klicken Sie im Abschnitt **Features** auf **OAuth & Berechtigungen**.
10. Fügen Sie im Abschnitt **Weiterleitungs-URLs** die folgende Weiterleitungs-URL hinzu:

    http://*ca-servername*:*port*/bi/v1/collaboration/auth/slack

    Dabei ist *ca-servername*:*port* der vollständig qualifizierte Name und die Portnummer Ihres Cognos Analytics-Servers.

    Tipp: Sie können mehrere Weiterleitungs-URLs konfigurieren. Dies erlaubt es Ihnen, dieselbe Slack-Anwendung in mehreren Cognos Analytics-Umgebungen zu verwenden, z. B. "Entw", "Test" und "Prod".
11. Klicken Sie auf **Hinzufügen**.
12. Klicken Sie auf **URLs speichern**.
13. Wenn Sie keinen Verwaltungszugriff auf Ihren Slack-Arbeitsbereich haben, führen Sie die folgenden Schritte aus:
    a) Wechseln Sie zum Abschnitt **Bereiche** und wählen Sie im Feld **Berechtigungsbereiche auswählen** die Option **Auf Profilinformationen des eigenen Arbeitsbereichs zugreifen (Benutzer:Lesen)** aus.
    b) Klicken Sie auf **Änderungen speichern**.
    c) Blättern Sie zum Abschnitt **OAuth-Tokens & Weiterleitungs-URLs** und klicken Sie auf **Genehmigung anfordern**.

    Wenn Ihre Anforderung durch den Slack-Administrator genehmigt wurde, empfangen Sie eine Nachricht vom Slackbot, die angibt, dass Ihre Anforderung genehmigt wurde. Die Schaltfläche **App in Arbeitsbereich installieren** wird im Abschnitt **OAuth & Berechtigungen** Ihrer App angezeigt.
    d) Klicken Sie auf **App in Arbeitsbereich installieren**.
14. Bestätigen Sie, dass Ihr Slack-Arbeitsbereich funktioniert.
    a) Installieren Sie Slack auf Ihrem Computer, falls noch nicht geschehen.
    b) Melden Sie sich bei Ihrer Slack-App mithilfe des E-Mail-Kontos und Kennworts an, das Sie zum Erstellen der Slack-App verwendet haben.
    c) Testen Sie Ihren Slack-Arbeitsbereich.

    Tipp: Informationen zum Einrichten und Verwenden von Slack finden Sie in der verfügbaren Dokumentation unter www.slack.com.

Nächste Schritte

Sie können jetzt „Hinzufügen einer Plattform für gemeinsames Arbeiten in Cognos Analytics” auf Seite 196.

Hinzufügen einer Plattform für gemeinsames Arbeiten in Cognos Analytics

Sie können Cognos Analytics mit einer Plattform für gemeinsames Arbeiten eines Drittanbieters, zum Beispiel Slack, verbinden. Dies ermöglicht Cognos Analytics-Benutzern, Cognos Analytics-Inhalte miteinander zu teilen.

Vorbereitende Schritte

Bevor Sie gemeinsames Arbeiten in Cognos Analytics konfigurieren, müssen Sie eine Anwendung in Slack erstellen.

Vorgehensweise

1. Stellen Sie sicher, dass Ihnen die Collaboration Administration-Funktion zugeordnet ist.
2. Melden Sie sich bei Cognos Analytics an.

3. Klicken Sie im Slideout-Fenster **Verwalten** > **Gemeinsames Arbeiten** auf das Symbol für **Plattform für gemeinsames Arbeiten hinzufügen** .
4. Geben Sie einen Namen für die Plattform für gemeinsames Arbeiten ein, zum Beispiel `Cognos Analytics-Collaboration`.
5. Geben Sie auf der Registerkarte **Einstellungen** die folgenden Details zur Plattform für gemeinsames Arbeiten ein:
   - Client-ID

     Geben Sie die Client-ID ein, die Sie sich notiert haben, als Sie die Slack-Anwendung erstellt haben.
   - Geheimer Clientschlüssel

     Geben Sie den geheimen Clientschlüssel ein, den Sie sich notiert haben, als Sie die Slack-Anwendung erstellt haben.
   - URL des Arbeitsbereichs

     Geben Sie die URL des Arbeitsbereichs ein, die Sie bei Slack registriert haben, jedoch ohne die Angabe `.slack.com` am Ende.
6. Klicken Sie auf das Symbol für **Arbeitsbereich hinzufügen** .
7. Klicken Sie auf **Testen**.
8. Wenn Sie nicht bereits vom Slack-Arbeitsbereich authentifiziert wurden, wird möglicherweise eine Nachricht mit der Bitte geöffnet, sich anzumelden. Melden Sie sich mit Ihren Slack-Berechtigungsnachweisen an.

   Es wird eine Nachricht angezeigt, in der Sie aufgefordert werden, den Zugriff auf die von Ihnen erstellte Slack-Anwendung zu autorisieren.
9. Klicken Sie auf **Autorisieren**.
10. Klicken Sie auf **Speichern**.

Ergebnisse

Die Plattform für gemeinsames Arbeiten wird erstellt. Der Name der Plattform wird im Slideout-Fenster **Verwalten** > **Gemeinsames Arbeiten** angezeigt. Um die zugehörigen Arbeitsbereiche anzuzeigen oder um zusätzliche hinzuzufügen, klicken Sie auf den Plattformnamen und blättern Sie im Slideout-Fenster nach unten.

Nächste Schritte

Wenn Sie Ihre Plattform für gemeinsames Arbeiten für Cognos Analytics-Benutzer inaktivieren möchten, klicken Sie auf die Registerkarte **Allgemein** und wählen Sie dann das Kontrollkästchen **Diesen Eintrag inaktivieren** aus. Benutzern sehen weiterhin das Symbol **Gemeinsames Arbeiten** in der Symbolleiste. Der Plattformname ist jedoch inaktiv und abgeblendet.

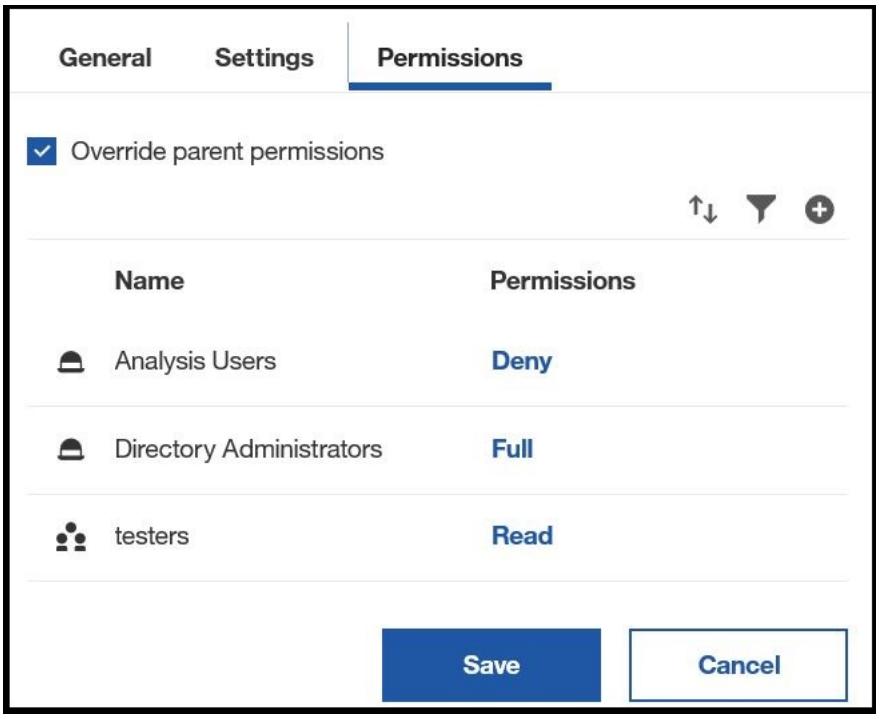
Wenn Sie Ihre Plattform für gemeinsames Arbeiten für Cognos Analytics-Benutzer ausblenden möchten, klicken Sie auf die Registerkarte **Allgemein** und wählen Sie dann das Kontrollkästchen **Diesen Eintrag ausblenden** aus.

Anmerkung: Wenn Benutzer das Kontrollkästchen **Ausgeblendete Einträge anzeigen** auf der Registerkarte **Eigene Vorgaben** > **Allgemein** ausgewählt haben, sehen sie den Namen der Plattform für gemeinsames Arbeiten als abgeblendeten Text. Wenn sie **Ausgeblendete Einträge anzeigen** nicht ausgewählt haben, sehen sie den Namen nicht.

Wenn Sie auf den Namen der Plattform für gemeinsames Arbeiten und dann auf **Berechtigungen** klicken, können Sie den Zugriff steuern, den unterschiedliche Benutzer, Rollen und Gruppen auf die Plattform für gemeinsames Arbeiten haben. Sie können einen der folgenden drei Werte zuordnen:

- **Vollständig** - ermöglicht den Verwaltungszugriff auf die Plattform für gemeinsames Arbeiten.

- **Lesen** - ermöglicht Benutzern, Slack-Nachrichten über die Plattform für gemeinsames Arbeiten zu senden.
- **Verweigern** - blendet die Plattform für gemeinsames Arbeiten für die ausgewählten Benutzer, Gruppen oder Rollen aus und verhindert so, dass diese Nachrichten über die Plattform zu senden.



Aktivierung der gemeinsamen Nutzung von Inhalten per E-Mail

Konfigurieren Sie einen Mail-Server so, dass Benutzer Cognos Analytics-Inhalte in einer E-Mail gemeinsam nutzen können.

Vorgehensweise

1. Starten Sie IBM Cognos Configuration in dem Verzeichnis, in dem Content Manager installiert ist.
2. Klicken Sie im Fenster **Explorer** unter **Datenzugriff** auf **Benachrichtigung**.
3. Geben Sie im Fenster **Eigenschaften** für die Eigenschaft **SMTP-Mail-Server** den Hostnamen und den Port Ihres SMTP-E-Mail-Servers (ausgehend) ein.

   Damit Sie per E-Mail gesendete Inhalte öffnen können, müssen Sie den Hostnamen im **Gateway-URI** von 'localhost' in die IP-Adresse oder den Namen des Computers ändern. Andernfalls enthält die URL in der E-Mail die Komponente 'localhost' und Remotebenutzer können die Inhalte nicht öffnen.

   Damit als Verknüpfung gesendete Inhalte geöffnet werden können, müssen Sie sicherstellen, dass der **Gateway-URI** auf Berichts- und Benachrichtigungsservern einen Web-Server mit IBM Cognos-Inhalten angibt, auf den zugegriffen werden kann. Wenn mobile Benutzer über eine Fernverbindung auf Verknüpfungen zugreifen, sollte ein externer URI in Betracht gezogen werden.
4. Klicken Sie auf das Feld **Wert** neben der Eigenschaft **Benutzerkonto und Kennwort** und klicken Sie anschließend auf die Schaltfläche zum Bearbeiten, wenn Sie angezeigt wird.
5. Geben Sie die entsprechenden Werte in das Dialogfeld **Wert - Benutzerkonto und Kennwort** ein und klicken Sie anschließend auf **OK**.

   Wenn für den SMTP-Server keine Anmeldeberechtigungsnachweise erforderlich sind, entfernen Sie die Standardinformationen für die Eigenschaft **Benutzerkonto und Kennwort**. Wenn Sie dazu aufgefordert werden, zu bestätigen, dass diese Eigenschaft leer bleiben soll, klicken Sie auf **OK**. Stellen Sie sicher, dass der Standardbenutzername entfernt wurde. Ist dies nicht der Fall, wird das Standardkonto verwendet und Benachrichtigungen funktionieren nicht ordnungsgemäß.

6. Geben Sie im Fenster **Eigenschaften** die entsprechenden Werte für das Standardabsenderkonto ein.
7. Klicken Sie im Fenster **Explorer** mit der rechten Maustaste auf **Benachrichtigung** und klicken Sie dann auf **Test**.

   IBM Cognos Analytics testet die E-Mail-Server-Verbindung.

Ergebnisse

Benutzer können jetzt **E-Mail** als Collaboration-Plattform auswählen, wenn sie ihren Inhalt Cognos Analyticsgemeinsam nutzen.

Beispiel: Selektive Inaktivierung der gemeinsamen Nutzung von Inhalten per E-Mail

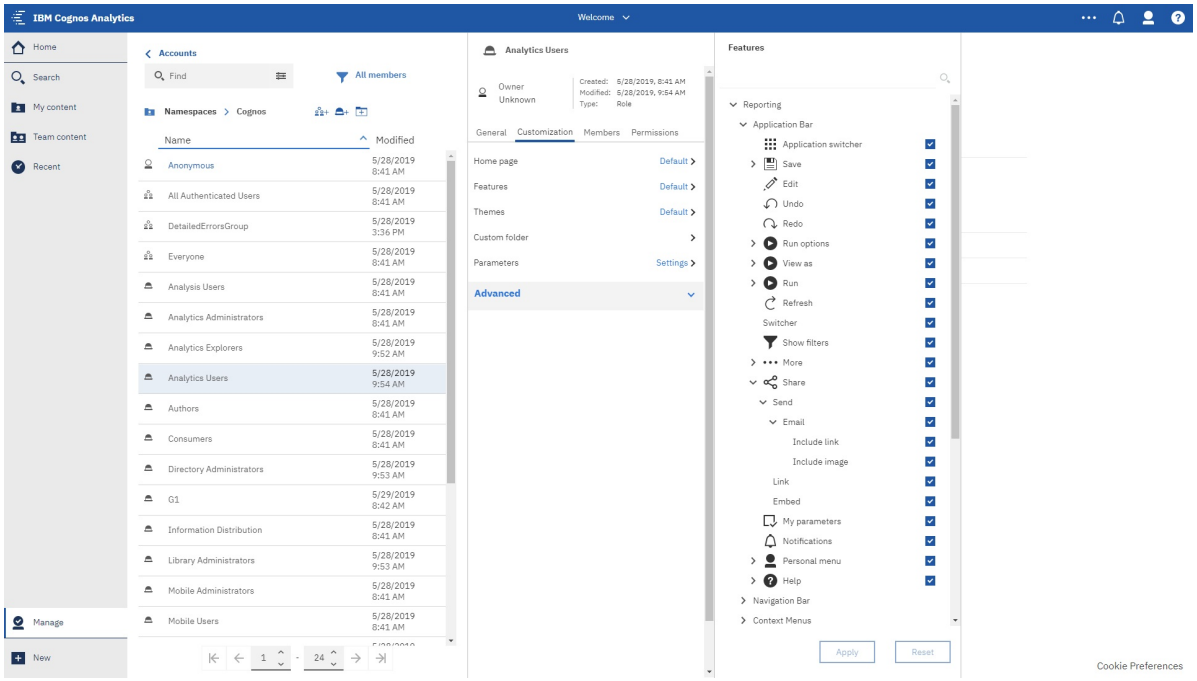
Sie können genau steuern, bei welchen Szenarios Cognos Analytics-Inhalte per E-Mail gesendet werden können, indem Sie **1.** bestimmte Rollen oder **2.** alle Rollen anpassen.

Im vorliegenden Beispiel haben Sie für alle Benutzer die gemeinsame Nutzung von Inhalten per E-Mail aktiviert. Sie möchten nun jedoch verhindern, dass Personen mit der Rolle 'Analytics-Benutzer' Cognos Analytics-Berichte oder Dashboardinhalte senden.

Tipp: Wenn Sie die gemeinsame Nutzung von Inhalten per E-Mail für alle Personen inaktivieren möchten, können Sie das Feature für alle Rollen anpassen.

Vorgehensweise

1. Melden Sie sich als Administrator an.
2. Wechseln Sie zu **Verwalten** > **Personen** > **Konten** und klicken Sie auf den Namespace **Cognos**.
3. Klicken Sie auf die Schaltfläche 'Mehr' ... neben der Rolle **Analytics-Benutzer**.
4. Klicken Sie auf **Eigenschaften**.
5. Klicken Sie auf die Registerkarte **Anpassung**.
6. Inaktivieren Sie die gemeinsame Nutzung von E-Mail-Inhalten für Dashboard- und Berichtsinhalte.
   a) Klicken Sie auf die Winkelschaltfläche > hinter **Features**.
   b) Klicken Sie auf die Winkelschaltfläche > vor **Berichterstellung**, um die Liste zu erweitern.
   c) Klicken Sie auf die Winkelschaltfläche > vor **Anwendungsleiste**, um die Liste zu erweitern.
   d) Klicken Sie auf die Winkelschaltfläche > vor **Teilen**, um die Liste zu erweitern.
   e) Klicken Sie auf die Winkelschaltfläche > vor **Senden**, um die Liste zu erweitern.



f) Wählen Sie das Kontrollkästchen **E-Mail** ab.

Tipp: Durch diese Aktion wird auch das Kontrollkästchen **E-Mail** für **Dashboards** inaktiviert, da die gemeinsame E-Mail-Nutzung sowohl für Dashboards als auch für Berichte verwendet werden kann.

g) Klicken Sie auf **Anwenden**.

Kapitel 9. Anpassen von Cognos Analytics für alle Rollen

Die IBM Cognos Analytics-Benutzerschnittstelle basiert auf einem erweiterbaren Modell. In diesem Modell sind die Benutzerschnittstellenanzeigen als Ansichten definiert (z. B. `home`, `authoring`, `dashboard` oder `modeller`). Sie können diese Ansichten für alle Benutzer und Rollen anpassen, indem Sie Benutzerschnittstellenelemente, wie z. B. Schaltflächen und Menüs, hinzufügen und entfernen. Sie können neue Ansichten zur Erweiterung der Cognos Analytics-Benutzerschnittstelle definieren. Darüber hinaus können Sie die Standardstartseite und die Standardanmeldeseite ersetzen oder in allen Ansichten das Standardbranding durch ein eigenes Branding (mit Farben, Logos und Brandingtext) ersetzen.

Anpassungen werden als komprimierte Dateien gepackt, die eine Datei mit dem Namen `spec.json` enthalten, mit der die Anpassung definiert wird. Abhängig vom Typ der Anpassung kann die komprimierte Datei auch andere Dateien enthalten. Anpassungen können auch in Bereitstellungen enthalten sein.

Verwenden Sie zum Verwalten von Anpassungen für alle Benutzer und Rollen das Slideout-Fenster **Verwalten** > **Anpassungen**. Über dieses Fenster können Sie Ihre Anpassungen auf den Cognos Analytics-Server hochladen und auswählen, welche Anpassungen verwendet werden sollen.

Anmerkung:

Wenn Sie das Slideout-Fenster **Verwalten** > **Anpassungen** verwenden, werden Ihre Anpassungen auf alle Benutzer und Rollen angewendet.

Wenn Sie zum Beispiel die Beispielerweiterung mit dem Namen `SampleExtensionExcludeNotifications.zip` hochladen, wird das Symbol **Benachrichtigungen**  aus der Anwendungsleiste in der Perspektive 'Home' für alle Benutzer und Rollen entfernt. Außerdem wird hiermit das Kontrollkästchen **Benachrichtigungen** aus der Featureliste entfernt, wenn ein Administrator die Eigenschaften einer beliebigen Rolle auswählt, auf die Registerkarte **Anpassung** klickt und zu **Features** > **Home** > **Anwendungsleiste** navigiert.

Aus diesem Grund sollten Sie eine Erweiterung verwenden, falls Sie beabsichtigen, ein Feature für jeden Nutzer in Ihrer Cognos-Umgebung hinzuzufügen oder zu entfernen. Falls Sie jedoch beabsichtigen, unterschiedliche Features für Benutzer und Rollen bereitzustellen, sollten Sie einzelne Rollenanpassungen anstelle einer Erweiterung verwenden.

Wenn Sie Rollenanpassungen zum Festlegen bestimmter Features für Benutzerrollen verwenden und dann eine Erweiterung anwenden, die auf diesen Features basiert, setzt die Erweiterung alle Ihre Rollenanpassungen außer Kraft.

Zum Zuweisen von Startseiten, Funktionen, Motiven, benutzerdefinierten Ordnern und Parametern zu bestimmten Rollen verwenden Sie das Slideout-Fenster **Verwalten** > **Konten** > **Namespaces**. Weitere Informationen finden Sie unter „Anpassen von Rollen” auf Seite 7.

Im Slideout-Fenster **Verwalten** > **Multi-Tenant-Funktionalität** können Sie benutzerdefinierte Motive und Startseiten bestimmten Tenants zuweisen. Wählen Sie dazu in der Eigenschaftsanzeige des entsprechenden Tenants die Registerkarte **Anpassung** aus. Weitere Informationen finden Sie unter „Anpassen von Tenants” auf Seite 119.

Bei einigen Anpassungen müssen Sie JavaScript als Programmiersprache verwenden. Diese Anpassungen sind in den folgenden Abschnitten beschrieben.

- „Erstellen eines benutzerdefinierten Aktionscontrollers” auf Seite 209
- „Erstellen einer Ansicht (mit Ausnahme von Anmeldeansichten)” auf Seite 220
- „Erstellen einer Anmeldeansicht” auf Seite 222

Bei den anderen Anpassungsarten sind keine Programmierungskenntnisse erforderlich.

Die für die Definition der Anpassungen verwendeten JSON-Schemas weisen einen vorläufigen Status auf und werden möglicherweise in zukünftigen Releases von Cognos Analytics so geändert, dass sie mit früheren Versionen nicht kompatibel sind.

Anpassungsbeispiele

Es stehen Anpassungsbeispiele zur Verfügung, die das Erstellen von Motiven, Erweiterungen und Ansichten veranschaulichen. Sie können diese Beispiele ändern, um eigene Anpassungen zu erstellen.

Bei einer einfachen Installation (Easy Install) werden diese Beispieldateien zusammen mit dem Produkt installiert, bei einer angepassten Installation können Sie als Option ausgewählt werden. Nach der Produktinstallation finden Sie die Dateien im Ordner *Installationsverzeichnis*/samples.

Die Anpassungsbeispiele sind in den folgenden Abschnitten beschrieben.

- „Beispielmotive” auf Seite 204
- „Beispielerweiterungen” auf Seite 216
- „Beispielansichten” auf Seite 225

Verwenden von Beispielen

Die Anpassungsbeispiele veranschaulichen die Implementierung häufig verwendeter Anpassungen. Sie können den Beispielcode anzeigen und ändern, um Anpassungen für Benutzer zu erstellen. Extrahieren Sie zum Prüfen der Inhalte eines Anpassungsbeispiels die ZIP-Datei. Jedes Beispiel beinhaltet eine spec.json-Datei, die die Logik für die Anpassung enthält. Abhängig von der Anpassung können auch weitere Dateien oder Ordner mit Bilddateien, JavaScript-Dateien und HTML-Dateien vorhanden sein.

Beachten Sie zum Hochladen und Verwenden eines Beispielmotivs oder einer Beispielerweiterung die Anweisungen in „Anwenden von Motiven, Erweiterungen und Ansichten” auf Seite 227.

Erstellen von Motiven

Sie können das IBM Cognos Analytics-Standardmotiv für die Cognos Analytics-Benutzerschnittstelle mit einem Motiv überschreiben, das Ihr Unternehmensbranding widerspiegelt.

Die Beispielanpassung SampleTheme.zip veranschaulicht das Erstellen eines Motivs. Das ZIP-Archiv enthält die Datei spec.json mit der Definition des Motivs und den Ordner images, der die diesem Motiv zugeordneten Abbildungen enthält. Bilddateinamen können keine Leerzeichen enthalten.

Achtung:

Wenn Sie ein Beispielmotiv verwenden, können Sie Ihr Kennwort nach seinem Ablauf nicht mehr zurücksetzen.

Ihr bestimmtes Motiv kann aus einem Ordner wie z. B. "myTheme" bestehen, der eine Datei JSON-Datei und images (mit Ihren Grafiken) enthält. Wenn Sie die ZIP-Datei erstellen, schließen Sie den Ordner (z. B. "myTheme") nicht in die ZIP-Datei ein. Cognos Analytics kann sie nicht verarbeiten. Wählen Sie stattdessen die JSON-Datei und den Ordner images ein und verwenden Sie dann ein Archivierungsprogramm, um die ZIP-Datei zu erstellen. Verwenden Sie nicht Windows Explorer-Funktion "Senden an komprimierten Ordner", um die ZIP-Datei zu erstellen. Das Ergebnis wäre eine nicht kompatible Datei.

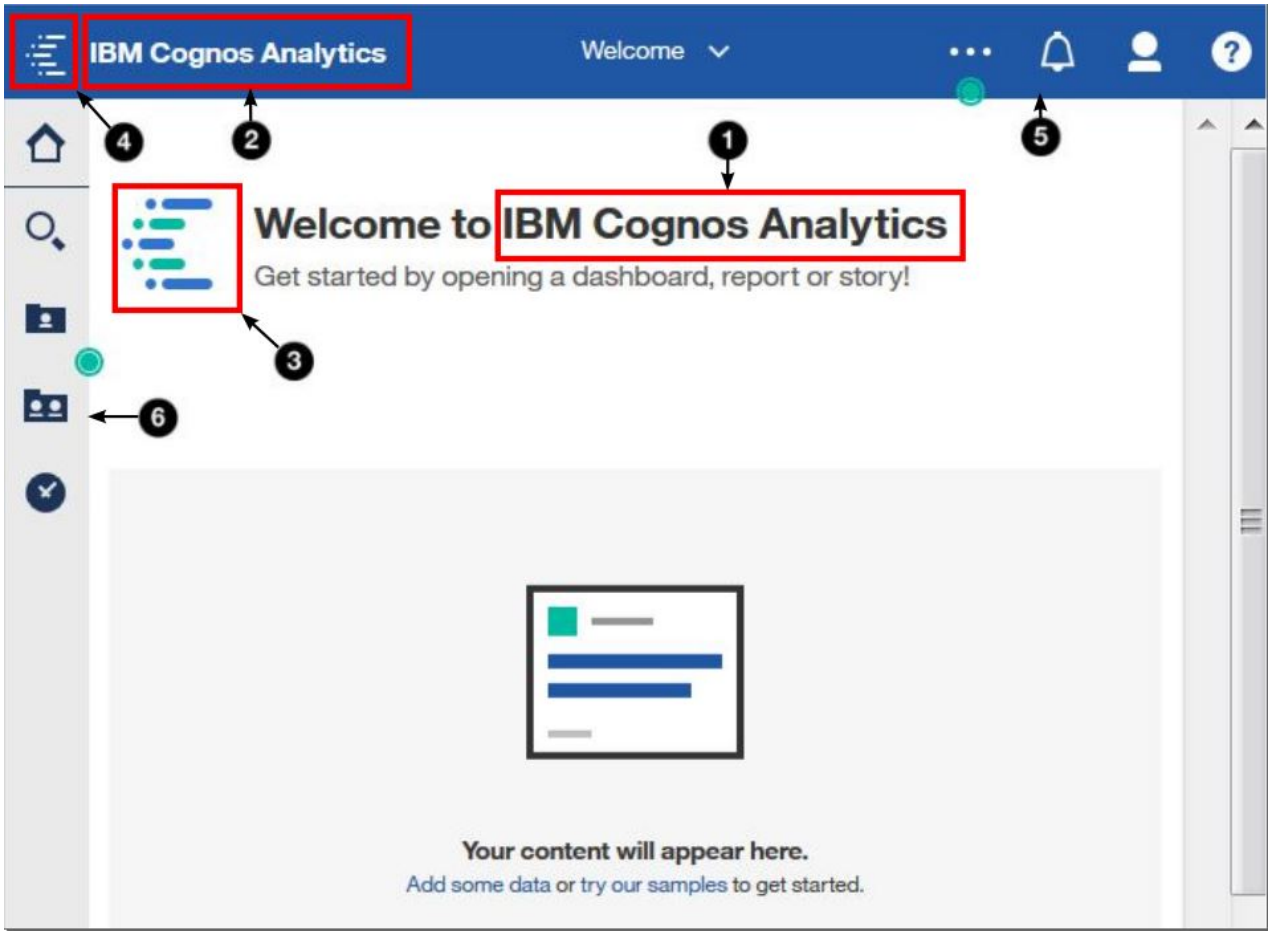
Die Datei spec.json ist hier dargestellt.

```
{
  "name": "Sample_Theme",
  "schemaVersion": "2.0",
  "brandText": "the Sample Outdoors Company",
  "brandTextSmall": "Sample Outdoors Company",
  "images": {
    "brandIcon": "images/logo_large.png",
    "brandIconSmall": "images/logo_small.png",
    "favicon": "images/logo_fav.png"
  },
```

```
  "colors": {
    "appbarBackground": "#eeeeee",
    "appbarForeground": "black",
    "appbarSelectLine": "#033f38",
    "appbarPushButtonBackground": "#c8d2d1",
    "navbarBackground": "#1c96d4",
    "navbarForeground": "white",
    "navbarSelectLine": "#033f38",
    "navbarPushButtonBackground": "#007670"
  }
}
```

Die aktuellen Beispiele enthalten die Elemente `brandTextSmall` und `favicon` nicht. Sie sind hier zu Dokumentationszwecken aufgeführt.

Die Objekte in dieser Datei entsprechen den hier aufgeführten Cognos Analytics-Benutzerschnittstellenelementen. Wenn im Motiv Motivelemente weggelassen werden, wird das Cognos Analytics-Standardmotivelement verwendet.



Diese Tabelle ordnet die Benutzerschnittstellenelemente den JSON-Objekten zu.

Tabelle 76. Objekte für Motive

Benutzerschnittstellenreferenz	JSON-Beschreibung	Definition
1	`brandText`	Brandingtext. Wenn Sie für diesen Eintrag keine Angabe machen möchten, geben Sie eine leere Zeichenfolge ein.

Tabelle 76. Objekte für Motive (Forts.)		
Benutzerschnitts-tellenreferenz	**JSON-Beschreibung**	**Definition**
2	`brandTextSmall`	Kurzer Brandingtext. Wird hier keine Angabe gemacht, wird `brandText` verwendet. Wenn Sie für diesen Eintrag keine Angabe machen möchten, geben Sie eine leere Zeichenfolge ein.
3	`brandIcon`	Brandingsymbol
4	`brandIconSmall`	Kleines Brandingsymbol
5	`appbarBackground`	Hintergrundfarbe für die Anwendungsleiste
5	`appbarForeground`	Vordergrundfarbe für die Anwendungsleiste
5	`appbarSelectLine`	Linienfarbe für die Anwendungsleisten-auswahl
5	`appbarPushButtonBackground`	Hintergrundfarbe für eine Schaltfläche in der Anwendungsleiste
6	`navbarBackground`	Hintergrundfarbe der Navigationsleiste
6	`navbarForeground`	Vordergrundfarbe der Navigationsleiste
6	`navbarSelectLine`	Linienfarbe für die Navigationsleisten-auswahl
6	`navbarPushButtonBackground`	Hintergrundfarbe für eine Schaltfläche in der Navigationsleiste
	`favicon`	Symbol für die Anzeige auf der Registerkarte des Web-Browsers.

Beispielmotive

Die folgenden Beispiele veranschaulichen die Verwendung von Motiven.

Diese Beispiele sind im Ordner *<Installationsposition>*`/samples/themes` installiert.

`SampleTheme.zip`
Ein Motiv, mit dem das Branding und das Farbschema für die Cognos Analytics-Benutzerschnittstelle geändert werden.

`SampleThemeBlueGreen.zip`
Ein Motiv, mit dem das Farbschema für die Cognos Analytics-Benutzerschnittstelle geändert wird.

`SampleThemeDarkBlue.zip`
Ein Motiv, mit dem das Farbschema für die Cognos Analytics-Benutzerschnittstelle geändert wird.

`SampleThemeLight.zip`
Ein Motiv, mit dem das Farbschema für die Cognos Analytics-Benutzerschnittstelle geändert wird.

Erstellen von Erweiterungen

Sie können Erweiterungen erstellen, mit denen neue Funktionen zur IBM Cognos Analytics-Benutzerschnittstelle hinzugefügt werden. So können Sie beispielsweise Schaltflächen hinzufügen, mit denen ein bestimmter Bericht oder ein bestimmtes Dashboard geöffnet wird, wenn darauf geklickt wird. Darüber hinaus können Sie Standardschaltflächen von der Benutzerschnittstelle entfernen.

Zum Erstellen und Hochladen von Erweiterungen müssen Sie die Berechtigungen eines Portal- oder Systemadministrators besitzen.

Erweiterungen sind in einer Datei mit dem Namen `spec.json` definiert, die sich im Stammverzeichnis der ZIP-Datei für die Erweiterung befindet. Abhängig von der jeweiligen Erweiterung sind möglicherweise auch Ordner vorhanden, in denen Bilder, HTML-Dateien und JavaScript-Dateien enthalten sind. Struktur und Inhalt der Datei `spec.json` sind in „Beschreibung der Datei spec.json" auf Seite 229 beschrieben. Die allgemeine Struktur der Datei ist hier dargestellt.

```
{
    "name":"...",
    "schemaVersion": "1.0",
    "extensions": [{
        "perspective": "common",
        "features": [{
            "id": "...",
            "toolItems": [<Toolelement1>,<Toolelement2>,...],
            "collectionItems": [<Gruppenelement1>,<Gruppenelement2>,...],
            "excludeFeatures": [<auszuschließendes Feature1>,<auszuschließendes Feature2>,...],
            "excludeItems": [<auszuschließendes Element1>,<auszuschließendes Element2>,...]
        }]
    }
}
```

Der Wert des Elements `perspective` gibt an, welche Ansichten diese Erweiterung verwenden. Der Wert `common` bedeutet, dass die Erweiterung für alle Ansichten verwendet wird. Die Elemente im Array `features` werden der Aktion der Erweiterung entsprechend verwendet. Sie werden in den folgenden Abschnitten veranschaulicht.

Durch das Erstellen von Erweiterungen können Sie vorhandene Ansichten ändern und neue Ansichten erstellen. Die Aktionen, die mit einer Erweiterung ausgeführt werden können, sind hier aufgeführt und in den folgenden Abschnitten beschrieben. Mit einer einzelnen Erweiterung können eine oder mehrere Aktionen ausgeführt werden.

- Hinzufügen einer Schaltfläche zur Anwendungs- oder Navigationsleiste, über die eine Aktion ausgeführt werden kann, z. B. Anzeigen einer Website, Ausführen eines Berichts oder Öffnen eines Dashboards, einer Story oder eines Ordners.
- Hinzufügen eines Menüelements zu einem vorhandenen Menü, über das eine Aktion ausgeführt werden kann, z. B. Anzeigen einer Website, Ausführen eines Berichts oder Öffnen eines Dashboards, einer Story oder eines Ordners.
- Hinzufügen eines Menüs zusammen mit den zugehörigen Menüelementen.
- Entfernen eines Standardbenutzerschnittstellenfeatures oder -elements.
- Hinzufügen benutzerdefinierter Formen zur Verwendung in Dashboards.
- Hinzufügen benutzerdefinierter Widgets zur Verwendung in Dashboards.

Hinzufügen einer Schaltfläche oder eines Menüelements

Sie können Schaltflächen und Menüelemente hinzufügen, mit denen eine Reihe verschiedener Aktionen durchgeführt werden kann, z. B. Anzeigen einer Website, Ausführen eines Berichts oder Öffnen eines Dashboards, einer Story oder eines Ordners. Sie können auch benutzerdefinierte Aktionen erstellen.

Für alle Schaltflächen ist ein Aktionscontroller erforderlich. Es sind vier integrierte Aktionscontroller zur Ausführung allgemeiner Aktionen verfügbar. Diese Aktionen sind nachfolgend aufgeführt.

bi/glass/api/IFrameOpener
Öffnet eine Webseite.

bi/glass/api/ReportOpener
Führt einen Bericht aus.

bi/glass/api/DashboardOpener
Öffnet ein Dashboard.

bi/glass/api/FolderOpener
Öffnet einen Ordner.

Sie können benutzerdefinierte Aktionscontroller auch mit JavaScript schreiben.

Der Inhalt der Datei `json.spec` ist für Schaltflächen und Menüelemente ähnlich, daher wird er nicht separat beschrieben. Der Hauptunterschied besteht darin, dass der Wert des Elements `type` für eine Schaltfläche `button` lautet, für ein Menüelement dagegen `menuItem`. Weitere Unterschiede sind in den folgenden Abschnitten dokumentiert.

Verwenden integrierter Aktionscontroller

Es sind vier integrierte Aktionscontroller verfügbar. Mit diesen Aktionscontrollern kann eine Webseite geöffnet, ein Bericht ausgeführt, ein Ordner geöffnet und ein Dashboard oder eine Story geöffnet werden. Die Aktionscontroller werden in den folgenden Abschnitten beschrieben.

Öffnen einer Webseite

Verwenden Sie den Aktionscontroller `bi/glass/api/IFrameOpener`, um eine Webseite zu öffnen. Die verfügbaren Optionen sind hier aufgeführt.

url
Gibt die URL der zu öffnenden Webseite an.

title
Gibt den anzuzeigenden Webseitentitel an.

Mit der Beispielerweiterung `SampleExtensionButtonWebsite.zip` wird eine Webseite geöffnet. Die Datei `spec.json` ist hier dargestellt.

```
{
    "name":"Sample_Button_Website",
    "schemaVersion": "1.0",
    "extensions": [{
        "perspective": "common",
        "comment": "Es steht eine spezielle Metaperspektive mit der Bezeichnung COMMON zur Ver
fügung. Das Hinzufügen
                von Beiträgen zu dieser Perspektive bewirkt, dass die Erweiterung
                auf alle Perspektiven angewendet wird.",
        "features": [{
            "id": "sample.common.button.openWebsite",
            "toolItems": [
            {
                "comment": "Mit diesem Code wird eine benutzerdefinierte Schaltfläche für die
Website angezeigt,
                                        über die die angegebene URL in einem iFrame geöffnet
wird.",
                "id": "sample.iframeOpener.website",
                "containerId": "com.ibm.bi.glass.navbarTrailingGroup",
                "label": "Website",
                "type": "Button",
                "icon": "images/web.png",
                "weight": 100,
                "actionController": "bi/glass/api/IFrameOpener",
                "options": {
                    "url": "http://www.ibm.com/analytics/us/en/technology/products/cognos-analy
tics/",
                    "title": "Website"
                }
            }
            ]
        }]
    }]}
```

Die Schaltflächenbeschriftung lautet `Website` und als Schaltflächensymbol wird das Bild `web.png` verwendet, das sich im Ordner `images` befindet. Der Aktionscontroller ist `bi/glass/api/IFrameOpener`, der zwei Optionen erfordert: die URL der Webseite (`url`) und den Titel der Webseite, der beim Öffnen der Seite angezeigt wird (`title`). Die anderen Elemente in der Datei `spec.json` werden in „Beschreibung der Datei spec.json” auf Seite 229 beschrieben.

Ausführen eines Berichts

Mit dem Aktionscontroller `bi/glass/api/ReportOpener` können Sie einen Bericht ausführen. Die verfügbaren Optionen sind hier aufgeführt. Es muss entweder `id` oder `path` angegeben werden.

id
Gibt die Speicher-ID des auszuführenden Berichts an.

path
Gibt den Pfad des auszuführenden Berichts an.

Mit der Beispielerweiterung `SampleExtensionButtonReport.zip` wird ein Bericht ausgeführt. Die Datei `spec.json` ist hier dargestellt.

```
{
    "name":"Sample_Button_Report",
    "schemaVersion": "1.0",
    "extensions": [{
        "perspective": "common",
        "comment": "Es steht eine spezielle Metaperspektive mit der Bezeichnung COMMON zur Ver
fügung. Das Hinzufügen von Beiträgen zu dieser Perspektive bewirkt, dass die
                Erweiterung für alle Perspektiven angewendet wird.",
        "features": [{
            "id": "sample.common.button.openReport",
            "toolItems": [
            {
                "comment": "Hiermit wird eine Schaltfläche hinzugefügt, über die ein gängiger
Bericht direkt geöffnet werden kann.",
                "id": "sample.report.opener",
                "containerId": "com.ibm.bi.glass.navbarLeadingGroup",
                "label": "QTD revenue",
                "type": "Button",
                "icon": "common-report",
                "weight": 800,
                "comment": "Je höher der Wert für 'weight' ist, desto weiter oben wird das
Element im Container angezeigt.",
                "actionController": "bi/glass/api/ReportOpener",
                "options": {"path": ".public_folders/Samples/Extensions/QTD revenue"}
            }
            ]
        }]
    }]}
```

Der Aktionscontroller ist `bi/glass/api/ReportOpener`, der eine Option erfordert: den Pfad des Berichts (`path`). `.public_folders` ist der Stammordner für **Teaminhalt** und `.my_folders` ist der Stammordner für **Eigener Inhalt**. Wenn der Berichtsname einen Schrägstrich (/) enthält, muss dieser als %2F codiert werden. Die anderen Elemente in der Datei `spec.json` werden in „Beschreibung der Datei spec.json" auf Seite 229 beschrieben.

Öffnen eines Dashboards oder einer Story

Verwenden Sie den Aktionscontroller `bi/glass/api/DashboardOpener`, um ein Dashboard oder eine Story zu öffnen. Die verfügbaren Optionen sind hier aufgeführt. Es muss entweder `id` oder `path` angegeben werden.

id
Gibt die Speicher-ID des Dashboards oder der Story an, das/die geöffnet werden soll.

path
Gibt den Pfad des Dashboards oder der Story an, das/die geöffnet werden soll.

Mit der Beispielerweiterung `SampleExtensionButtonDashboard.zip` wird ein Dashboard geöffnet. Die Datei `spec.json` ist hier dargestellt.

```
{
    "name":"Sample_Button_Dashboard",
    "schemaVersion": "1.0",
    "extensions": [{
        "perspective": "common",
        "comment": "Es steht eine spezielle Metaperspektive mit der Bezeichnung COMMON zur Ver
fügung. Das Hinzufügen von Beiträgen zu dieser Perspektive bewirkt, dass die
                Erweiterung für alle Perspektiven angewendet wird.",
```

```
        "features": [{
            "id": "sample.common.button.openDashboard",
            "toolItems": [
            {
                "comment": "Mit diesem Code wird eine Schaltfläche hinzugefügt, über die ein
                            zentrales Dashboard direkt geöffnet werden kann.",
                "id": "sample.dashboard.opener",
                "containerId": "com.ibm.bi.glass.navbarLeadingGroup",
                "label": "Line dashboard",
                "type": "Button",
                "icon": "common-dashboard",
                "weight": 900,
                "comment": "Je höher der Wert für 'weight' ist, desto weiter oben wird das
Element im Container angezeigt.",
                "actionController": "bi/glass/api/DashboardOpener",
                "options": {"path": ".public_folders/Samples/Extensions/Line dashboard"}
            }
            ]
        }]
    }]}
```

Der Aktionscontroller ist `bi/glass/api/DashboardOpener`; die einzige erforderliche Option ist der Pfad des Dashboards (`path`), der auf dieselbe Weise bestimmt wird wie der Pfad für einen Bericht. Die anderen Elemente in der Datei `spec.json` werden in „Beschreibung der Datei spec.json” auf Seite 229 beschrieben.

Öffnen eines Ordners

Verwenden Sie den Aktionscontroller `bi/glass/api/FolderOpener`, um einen Ordner zu öffnen. Die verfügbaren Optionen sind hier aufgeführt. Es muss entweder `id` oder `path` angegeben werden.

id
Gibt die Speicher-ID des zu öffnenden Ordners an.

path
Gibt den Pfad des zu öffnenden Ordners an.

skipAncestors
Gibt an, ob Vorfahrenordner beim Öffnen des Ordners angezeigt (`false`) oder ausgeblendet (`true`) werden sollen. Der Standardwert ist `false`.

Mit der Beispielerweiterung `SampleExtensionButtonFolder.zip` wird ein Ordner geöffnet. Die Datei `spec.json` ist hier dargestellt.

```
{
    "name":"Sample_Button_Folder",
    "schemaVersion": "1.0",
    "extensions": [{
        "perspective": "common",
        "comment": "Es steht eine spezielle Metaperspektive mit der Bezeichnung COMMON zur Ver
fügung. Das Hinzufügen von Beiträgen zu dieser Perspektive bewirkt, dass die
                            Erweiterung für alle Perspektiven angewendet wird.",
        "features": [{
            "id": "sample.common.button.openFolder",
            "toolItems": [
            {
                "comment": "Mit diesem Code wird eine Schaltfläche für den einfachen Zugriff
                auf einen wichtigen Ordner hinzugefügt.",
                "id": "sample.folder.opener",
                "containerId": "com.ibm.bi.glass.navbarLeadingGroup",
                "label": "2016 reports",
                "type": "Button",
                "icon": "common-folder",
                "weight": 700,
                "push": "true",
                "comment": "Je höher der Wert für 'weight' ist, desto weiter oben wird das
Element im Container angezeigt.",
                "actionController": "bi/glass/api/FolderOpener",
                "options": {"path": ".public_folders/Samples/Extensions"}
            }
            ]
        }]
    }]}
```

Diese Beispiel enthält das Element `"push": "true"`. Dieses Element ist beim Öffnen eines Ordner erforderlich, da sich eine Schaltfläche zum Öffnen eines Ordners in einem von zwei Status befinden kann: geöffnet oder geschlossen. (Dieses Element wird für ein Menüelement nicht verwendet.) Wenn nach dem Öffnen eines Ordners erneut auf die Schaltfläche geklickt wird, wird der Ordner geschlossen. Der Aktionscontroller ist `bi/glass/api/FolderOpener`; die einzige erforderliche Option ist der Pfad des Ordners (`path`), der auf dieselbe Weise bestimmt wird wie der Pfad für einen Bericht. Die anderen Elemente in der Datei `spec.json` werden in „Beschreibung der Datei spec.json" auf Seite 229 beschrieben.

Erstellen eines benutzerdefinierten Aktionscontrollers

Sie können benutzerdefinierte Aktionscontroller für die Ausführung von Aktionen erstellen, die mit den integrierten Aktionscontrollern nicht zur Verfügung stehen. Benutzerdefinierte Aktionscontroller werden in JavaScript geschrieben, wobei die AMD-API (Asynchronous Module Definition) verwendet wird.

Mit der Beispielerweiterung `SampleExtensionContextMenuItem.zip` wird ein benutzerdefinierter Aktionscontroller implementiert, durch den ein Menüelement zum Kontextmenü für alle Berichtsobjekte hinzugefügt wird. Die Datei `spec.json` ist hier dargestellt.

```
{
    "name":"Sample_Context_Menu_Item",
    "comment": "Mit dieser Erweiterung wird ein neues Menüelement zum Kontextmenü
               für alle Berichtsobjekte hinzugefügt.",
    "comment": "Mit dem Menüelement wird ein Alertfeld geöffnet, das Informationen
                      zum ausgewählten Bericht enthält.",
    "schemaVersion": "1.0",
    "extensions": [{
        "perspective": "common",
        "comment": "Es steht eine spezielle Metaperspektive mit der Bezeichnung COMMON zur Ver
fügung. Das Hinzufügen von Beiträgen zu dieser Perspektive bewirkt, dass die
             Erweiterung für alle Perspektiven angewendet wird.",
        "features": [{
            "id": "sample.home.context.item",
            "toolItems": [
            {
                "id": "custom.context.menu.item1",
                "containerId" : "com.ibm.bi.contentApps.listViewMenu",
                "comment": "containerId ist die ID des übergeordneten Menüs.",
                "type": "MenuItem",
                "actionController":
                  "v1/ext/Sample_Context_Menu_Item/js/controllers/SampleContextMenuItem",
                "label": "Sample menu item",
                "icon": "common-properties",
                "weight":950
            }
            ]
        }]
    }]}
```

Bei dem benutzerdefinierten Aktionscontroller handelt es sich um die Datei `SampleContextMenuItem.js`, die sich im Ordner `js/controllers` in der Erweiterung befindet. Diese Datei ist hier dargestellt.

```
/**
 * Licensed Materials - Property of IBM
 *
 * IBM Cognos Products: BI Glass
 *
 * Copyright IBM Corp. 2015
 *
 * US Government Users Restricted Rights - Use, duplication or disclosure restricted by
 GSA ADP Schedule Contract with IBM Corp.
 */
define([], function() {
    'use strict';

    var SampleAction = function(){

        /**
         * Wird bei jeder Erstellung dieser Ansicht von AppController aufgerufen.
         *
         * @public
         * @returns {Promise} - Promise, das in das DOM-Stammelement für diese Ansicht aufge
löst wird.
```

```
         */
        this.isVisible = function(context, target) {
            return target.options[0].type === 'report';
        },

        /**
         * Wird bei jedem Löschen dieser Ansicht von AppController aufgerufen.
         *
         * @public
         */
        this.execute = function(context, target) {
            var info = 'Dieses Beispielmenüelement öffnet einen Alert.
                \nDer Alert enthält Informationen zum ausgewählten Bericht.
                \n\nType: ' + target.options[0].type + '\nName: ' + target.options[0].name
                + '\nID: ' + target.options[0].id;
            alert(info);
        }



    };

    return SampleAction;

});
```

Dieser JavaScript-Code verwendet die Aktions-API in einem JavaScript-AMD-Modul. Für diese Module ist die JavaScript Q-Bibliothek erforderlich. Die Aktions-API besteht aus zwei Methoden.

void execute(context, target)

context
Dieses Objekt enthält Dienstprogramm-Methoden.

target
Dieses Objekt enthält Informationen zu der Schaltfläche oder dem Menüelement, die bzw. das durch die Erweiterung erstellt wird.

- Für eine Schaltfläche oder ein Menüelement in einem Anwendungsleisten- oder Navigationsleistenmenü enthält dieses Objekt die Optionseigenschaft für das Element.
- Für ein Menüelement in einem Kontextmenü eines Objekts enthält dieses Objekt ein Array mit dem Typ, dem Namen und der Speicher-ID des Objekts.

boolean isVisible(context, target)
Diese Methode ist nur für Menüelemente anwendbar. Das Menüelement wird angezeigt, wenn für diese Methode der Wert `true` zurückgegeben wird; andernfalls wird das Menüelement ausgeblendet.

Hinzufügen eines Menüs

Sie können ein Menü und die zugehörigen Menüelemente zur Anwendungs- oder Navigationsleiste hinzufügen.

Mit der Beispielerweiterung `SampleExtensionMenuQuicklinks.zip` werden ein Menü und sechs Menüelemente hinzugefügt. Ein Teil der Datei `spec.json` ist hier dargestellt.

```
{
    "name":"Sample_Menu_Quicklinks",
    "schemaVersion": "1.0",
    "extensions": [{
        "perspective": "common",
        "comment": "Es steht eine spezielle Metaperspektive mit der Bezeichnung COMMON zur Ver
fügung. Das Hinzufügen von Beiträgen zu dieser Perspektive bewirkt, dass die
         Erweiterung für alle Perspektiven angewendet wird.",
        "features": [{
            "id": "sample.common.menu.openMulipleItems",
            "toolItems": [
            {
                "comment": "Mit diesem Code wird ein benutzerdefiniertes Menüelement zur Anwen
dungsleiste
                in der abschließenden Gruppe hinzugefügt.",
                "id":"custom.appbar.trailingGroup.menu",
                "containerId": "com.ibm.bi.glass.appbarTrailingGroup",
                "type": "Menu",
                "label": "Quick links",
```

```
                "icon": "images/debug.svg",
                "weight": 650
            },
            {
                "comment": "Mit diesem Code wird ein Untermenüelement zum erstellten benutzerde
finierten Menü hinzugefügt.",
                "id": "custom.appbar.trailingGroup.menuItem1",
                "containerId" : "custom.appbar.trailingGroup.menu",
                "comment": "containerId ist die ID des übergeordneten Menüs.",
                "type": "MenuItem",
                "actionController": "v1/ext/Sample_Menu_Quicklinks/js/controllers/SampleMenu
Quicklinks",
                "comment": "actionController bestimmt die Aktionen für die Menüelemente.",
                "label": "Home",
                "icon": "common-home",
                "weight":900
            },
            {
                "comment": "Mit diesem Code wird ein Untermenüelement zum erstellten benutzerde
finierten Menü hinzugefügt.",
                "id": "custom.appbar.trailingGroup.menuItem2",
                "containerId" : "custom.appbar.trailingGroup.menu",
                "comment": "containerId ist die ID des übergeordneten Menüs.",
                "label": "Line dashboard",
                "type": "MenuItem",
                "icon": "common-dashboard",
                "weight":800,
                "actionController": "bi/glass/api/DashboardOpener",
                "comment": "actionController bestimmt die Aktionen für die Menüelemente.",
                "options": {"path": ".public_folders/Samples/Extensions/Line dashboard"}
            },...
            ]
        }]
    }]}
```

In diesem Beispiel befindet sich das Menü in der abschließenden Gruppe der Anwendungsleiste.

Entfernen eines Benutzerschnittstellenelements

Sie können Standardbenutzerschnittstellenelemente aus allen Ansichten oder aus bestimmten Ansichten, die Sie angeben, entfernen.

Mit der Beispielerweiterung `SampleExtensionExcludeNotifications.zip` wird die Schaltfläche **Benachrichtigungen** aus der Navigationsleiste entfernt. Die Datei `spec.json` ist hier dargestellt.

```
{
    "name":"Sample_Exclude_Notifications",
    "schemaVersion": "1.0",
    "extensions": [{
        "perspective": "home",
        "comment": "Dieser Code wird nur für die Perspektive HOME angewendet.",
        "features": [{
            "id": "sample.home.exclude.notifications",
            "excludeItems":["com.ibm.bi.share.notifications"],
            "comment": "Mit EXCLUDEITEMS wird die Benachrichtigungsschaltfläche von der
                      Navigationsleiste der Perspektive HOME entfernt.",
            "comment": "EXCLUDEITEMS muss auf der Ebene der einzelnen Perspektive angewendet
werden.
                    Die globale Anwendung über die Perspektive COMMON ist nicht möglich."
        }]
    }]}
```

Informationen zur Bestimmung der ID, die in den Werten für das Element `excludeItems` zu verwenden ist, finden Sie in „Bestimmen der ID eines Benutzerschnittstellenobjekts” auf Seite 235.

Hinzufügen von Dashboardformen

Sie können benutzerdefinierte Formen zur Verwendung in Dashboards erstellen.

Mithilfe des Beispiels `SampleExtensionCustomShape.zip` werden drei neue Formen zur Verwendung in Dashboards erstellt. Dieses Beispiel wird wie jede andere Erweiterung installiert. Nach der Installation werden die folgenden drei neuen Formen in der Anzeige **Formen** angezeigt.

Anmerkung: Nur .svg-Dateien können als Dashboardformen verwendet werden.

Der Inhalt der Datei `spec.json` ist nachfolgend dargestellt.

```
{
    "name":"Sample_Custom_Shape",
    "comment":"Mit diesem Beispiel werden 3 benutzerdefinierte Bilder zum unteren Bereich des
Fensters in Dashboarding hinzugefügt.",
    "schemaVersion": "2.0",
    "extensions": [{
        "perspective": "dashboard",
        "comment": "Die benutzerdefinierten Formen sind nur für die Dashboardperspektive anwend
bar.",
        "features": [{
            "id": "com.ibm.bi.dashboard",
            "collectionItems": [
            {
                "containerId": "com.ibm.bi.dashboard.shapes",
                "id": "sample_custom_shape_music",
                "name": "Music",
                "options": {
                    "templatePath": "v1/ext/Sample_Custom_Shape/images/music_32.svg"
                }
            },
            {
                "containerId": "com.ibm.bi.dashboard.shapes",
                "id": "sample_custom_shape_relationship",
                "name": "Relationship",
                "options": {
                    "templatePath": "v1/ext/Sample_Custom_Shape/images/relationship_32.svg"
                }
            },
            {
                "containerId": "com.ibm.bi.dashboard.shapes",
                "id": "sample_custom_shape_traffic",
                "name": "Traffic",
                "options": {
                    "templatePath": "v1/ext/Sample_Custom_Shape/images/traffic_32.svg"
                }
            }
        ]
        }
        ]
    }]
}
```

Die benutzerdefinierten Formen sind im Ordner `images` des Beispiels enthalten.

Erstellen einer Bildergalerie

Sie können eine Bildergalerie erstellen, die benutzerdefinierte Bilder für die Verwendung in Dashboards und Berichten enthalten.

Mit den Beispielen in `SampleExtensionCustomMedia.zip` und `SampleExtensionCustomMediaAll.zip` werden neue Bilder für die Verwendung in Dashboards und Berichten erstellt. Diese Beispiele werden wie jede andere Erweiterung installiert.

Nachdem Sie die Bildergalerie erstellt haben, können Benutzer die Bilder wie folgt auswählen:

- Dashboardautoren können die Registerkarte **Bildbibliothek** im Fenster **Widgets** auswählen. Weitere Informationen finden Sie im *Benutzerhandbuch zu Dashboards und Storys*.
- Berichtsersteller können das **Toolbox**-Symbol  und dann **Layout** auswählen, das **Bildobjekt**  in den Bericht ziehen und anschließend doppelklicken. Weitere Informationen finden Sie im *Reporting-Handbuch*.

Die in der Bildbibliothek verfügbaren Bilder haben die folgenden Beschreibungen:

- Blitze über einer Stadt bei Nacht
- Blitze an einem dunkelvioletten Himmel
- Starker Verkehr in einer Stadt bei Nacht
- Wanderer auf einem Hügel im Wald
- Mehrere Zelte auf einem Berg
- Graph mit hervorgehobenem steigendem Umsatz
- Graph mit steigendem Umsatz
- Gruppe von Personen in einem Call-Center

Sample_Custom_Media

Der Inhalt der Datei `spec.json` für `Sample_Custom_Media` ist nachfolgend dargestellt.

```
{
    "name": "Sample_Custom_Media",
    "comment":"Mit diesem Beispiel werden benutzerdefinierte Bilder zum unteren Bereich des
Fensters MEDIEN in Dashboarding hinzugefügt.",
    "comment":"Derzeit unterstützen wir nur das Hinzufügen von JPG- und PNG-Dateien.",
    "schemaVersion": "1.0",
    "extensions": [{
        "perspective": "dashboard",
        "comment": "Die benutzerdefinierten Bilder sind nur für die DASHBOARD-Perspektive vorge
sehen.",
        "features": [{
            "id": "com.ibm.bi.common.media",
            "comment": "Dies ist die ID für das Fenster MEDIEN. Es handelt sich um den Contai
ner für die nachfolgenden Bilder.",
            "collectionItems": [{
                "containerId": "com.ibm.bi.common.media",
                 "id": "customImage1",
                 "name": "Blitze über Stadt",
           "comment": "NAME ist der Text der QuickInfo für das Bild.",
                 "options": {
                     "altText": "Blitze über einer Stadt bei Nacht.",
            "comment": "ALTTEXT wird als Eigenschaft für das ausgewählte Bild angezeigt.",
                     "imageLink": "v1/ext/Sample_Custom_Media/images/SE_background.jpg"
                     }
                }, {
                "containerId": "com.ibm.bi.common.media",
                "id": "customImage2",
                "name": "Blitze am Himmel",
                "options": {
                    "altText": "Blitze an einem dunkelvioletten Himmel.",
                    "imageLink": "v1/ext/Sample_Custom_Media/images/weather_background3.jpg"
                    }
                }, {
                "containerId": "com.ibm.bi.common.media",
                "id": "customImage3",
                "name": "Stadtverkehr bei Nacht",
                "options": {
                     "altText": "Starker Verkehr in einer Stadt bei Nacht.",
                     "imageLink": "v1/ext/Sample_Custom_Media/images/story_scene1_back
ground.jpg"
                      }
                 }, {
                 "containerId": "com.ibm.bi.common.media",
                 "id": "customImage4",
                 "name": "Wanderer auf Hügel",
                 "options": {
                      "altText": "Wanderer auf einem Hügel im Wald.",
                      "imageLink": "v1/ext/Sample_Custom_Media/images/login_background.jpg"
                      }
                 }, {
                 "containerId": "com.ibm.bi.common.media",
                 "id": "customImage5",
                 "name": "Zelte auf Berg",
                 "options": {
                      "altText": "Mehrere Zelte auf einem Berg.",
                      "imageLink": "v1/ext/Sample_Custom_Media/images/welcome_background.jpg"
                      }
                  }, {
                  "containerId": "com.ibm.bi.common.media",
                  "id": "customImage6",
```

```
                    "name": "Hervorgehobener steigender Umsatz",
                    "options": {
                         "altText": "Graph mit hervorgehobenem steigendem Umsatz.",
                         "imageLink": "v1/ext/Sample_Custom_Media/images/story_scene5_back
ground2.jpg"
                         }
                    }, {
                    "containerId": "com.ibm.bi.common.media",
                    "id": "customImage7",
                    "name": "Steigender Umsatz",
                    "options": {
                         "altText": "Graph mit steigendem Umsatz.",
                         "imageLink": "v1/ext/Sample_Custom_Media/images/story_scene5_back
ground.jpg"
                         }
                     }]
                }]
        }]
}
```

Sample_Custom_Media_All

Der Inhalt der Datei spec.json für Sample_Custom_Media_All ist nachfolgend dargestellt.

```
{
    "name": "Sample_Custom_Media_All",
    "comment":"Mit dieser Beispielerweiterung werden 8 benutzerdefinierte Bilder zur Register
karte BILDBIBLIOTHEK der Anzeige WIDGETS in Dashboarding und Storys hinzugefügt.,
    "comment":"Darüber hinaus werden dieselben 8 benutzerdefinierten Bilder zum Bildauswahldia
log unter BILDERGALERIE in der Berichterstellung hinzugefügt.,
    "comment":"Zum gegenwärtigen Zeitpunkt werden nur JPG- und PNG-Dateien unterstützt.",
    "comment":"Erweiterungen dieses Typs sind nicht kumulativ. Sie müssen alle benötigten benut
zerdefinierten Bilder in einer Erweiterung angeben.",
    "comment":"Andernfalls erhält die zuletzt hochgeladene (nicht aktualisierte) Erweiterung
Priorität und wird als endgültige Bildbibliothek verwendet.",
    "schemaVersion": "1.0",
    "extensions": [{
            "perspective": "common",
            "comment": "Die benutzerdefinierten Bilder werden für alle Perspektiven angewendet
- Berichterstellung, Dashboarding und Storys.",
            "features": [{
                    "id": "com.ibm.bi.common.media",
                    "comment": "Dies ist die ID für die Widgetanzeige. Es handelt sich um den
Container für die nachfolgenden Bilder.",
                    "collectionItems": [{
                            "containerId": "com.ibm.bi.common.media",
                            "id": "customImage1",
                            "name": "Blitze über Stadt",
                            "comment": "NAME ist der Text der QuickInfo für das Bild auf der
Bildbibliotheksregisterkarte.",
                            "options": {
                                "altText": "Blitze über einer Stadt bei Nacht.",
                                "comment": "Der alternative Text wird in der Beschreibungseigen
schaft für das ausgewählte Bild angezeigt, sobald es in das Dashboard eingefügt wird.",
                                "imageLink": "v1/ext/Sample_Custom_Media_All/images/SE_back
ground.jpg"
                                }
                            }, {
                                "containerId": "com.ibm.bi.common.media",
                                "id": "customImage2",
                                "name": "Blitze am Himmel",
                                "options": {
                                    "altText": "Blitze an einem dunkelvioletten Himmel.",
                                    "imageLink": "v1/ext/Sample_Custom_Media_All/images/wea
ther_background3.jpg"
                                    }
                            }, {
                                "containerId": "com.ibm.bi.common.media",
                                "id": "customImage3",
                                "name": "Stadtverkehr bei Nacht",
                                "options": {
                                    "altText": "Starker Verkehr in einer Stadt bei Nacht.",
                                    "imageLink": "v1/ext/Sample_Custom_Media_All/images/sto
ry_scene1_background.jpg"
                                    }
                            }, {
                                "containerId": "com.ibm.bi.common.media",
                                "id": "customImage4",
                                "name": "Wanderer auf Hügel",
```

```
                            "options": {
                                "altText": "Wanderer auf einem Hügel im Wald.",
                                "imageLink": "v1/ext/Sample_Custom_Media_All/images/login_back
ground.jpg"
                            }
                        }, {
                            "containerId": "com.ibm.bi.common.media",
                            "id": "customImage5",
                            "name": "Zelte auf Berg",
                            "options": {
                                "altText": "Mehrere Zelte auf einem Berg.",
                                "imageLink": "v1/ext/Sample_Custom_Media_All/images/welco
me_background.jpg"
                            }
                        }, {
                            "containerId": "com.ibm.bi.common.media",
                            "id": "customImage6",
                            "name": "Call-Center",
                            "options": {
                                "altText": "Gruppe von Personen in einem Call-Center.",
                                "imageLink": "v1/ext/Sample_Custom_Media_All/images/call_cen
ter.jpg"
                            }
                        }, {
                            "containerId": "com.ibm.bi.common.media",
                            "id": "customImage7",
                            "name": "Hervorgehobener steigender Umsatz",
                            "options": {
                                "altText": "Graph mit hervorgehobenem steigendem Umsatz.",
                                "imageLink": "v1/ext/Sample_Custom_Media_All/images/sto
ry_scene5_background2.jpg"
                            }
                        }, {
                            "containerId": "com.ibm.bi.common.media",
                            "id": "customImage8",
                            "name": "Steigender Umsatz",
                            "options": {
                                "altText": "Graph mit steigendem Umsatz.",
                                "imageLink": "v1/ext/Sample_Custom_Media_All/images/sto
ry_scene5_background.jpg"
                            }
                        }
                    ]
                }
            ]
        }
    ]
}
```

Hinzufügen eines Dashboard-Widgets

Sie können benutzerdefinierte Widgets zur Verwendung in Dashboards erstellen.

Sie können benutzerdefinierte Widgets zur Verwendung in Dashboards erstellen. Benutzerdefinierte Widgets werden wie andere Erweiterungen installiert. Die Widgetaktion wird durch eine JavaScript-Datei bestimmt, die beliebige JavaScript-Aktionen ausführen und die Ergebnisse im Widget anzeigen kann.

Ein einfaches benutzerdefiniertes Widget enthält eine Datei mit dem Namen `spec.json`, eine JavaScript-Datei und einen Ordner, der vom Widget verwendete Bilder enthält. Die Datei `spec.json` ist hier dargestellt.

```
{
    "name":"SampleWidgetExt_old",
    "schemaVersion": "1.0",
    "extensions": [{
        "perspective": "dashboard",
        "comment": "Beispiele für benutzerdefinierte Widgets für Dashboards",
        "features": [{
            "id": "com.ibm.bi.dashboard.widgets",
            "collectionItems": [{
                "containerId": "com.ibm.bi.dashboard.widgets",
                "id": "Hello",
                "title": "Hello!",
                "iconUrl": "v1/ext/SampleWidgetExt/images/ibm.png",
                "widget": "v1/ext/SampleWidgetExt/helloParam.js",
                "scroll": "scrollNone",
                "disableTitle": true,
```

```
                "params" : {
                    "name": "IBM"
                }
            }]
        }]
    }]
}
```

Mit diesem Widget wird die JavaScript-Datei `helloParam.js` aufgerufen, die hier dargestellt wird.

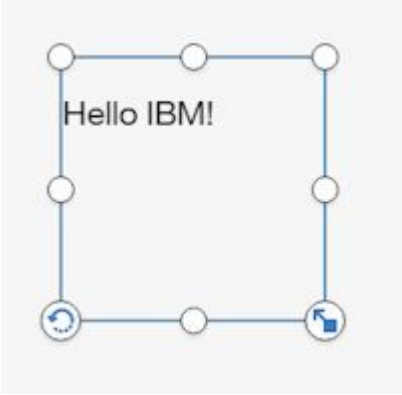
```
define([
    'jquery',
    'dashboard/widgets/CustomWidget'
], function( $, Base) {

    var Widget = Base.extend({
        onInit: function(params) {
            this.name = params.name;
        },
        onRender: function() {
            var root = this.getContentRootNode();
            $(root).append('<h1 class="titleColor titleFontSize">Hello ' + this.name + '!</
h1>');
        }
    });

    return Widget;
});
```

Der Ordner `images` enthält die Abbildung `ibm.png`.

Nach Installation der Erweiterung wird Benutzern, die ein Dashboard erstellen, ein neues Symbol angezeigt: **Benutzerdefinierte Widgets** (). Nach dem Anklicken von **Benutzerdefinierte Widgets** () können die Benutzer das benutzerdefinierte Widget auf den Erstellungsbereich für Dashboards ziehen. Das benutzerdefinierte Widget ist hier dargestellt.



Beispielerweiterungen

Die folgenden Beispiele veranschaulichen die Verwendung von Erweiterungen.

Bei einer einfachen Installation (Easy Install) werden diese Beispieldateien zusammen mit dem Produkt installiert, bei einer angepassten Installation können Sie als Option ausgewählt werden. Nach der Produktinstallation finden Sie die Dateien im Ordner *Installationsverzeichnis*/samples/extensions.

SampleExtensionButtonDashboard.zip
Eine Erweiterung, mit der eine Schaltfläche zum Öffnen eines Dashboards in allen Ansichten hinzugefügt wird.

SampleExtensionButtonFolder.zip
Eine Erweiterung, mit der eine Schaltfläche zum Öffnen eines Ordners in allen Ansichten hinzugefügt wird.

SampleExtensionButtonOpenPerspective.zip

Eine Erweiterung, mit der eine benutzerdefinierte Ansicht erstellt und eine Schaltfläche () zum Öffnen der benutzerdefinierten Ansicht zur Navigationsleiste aller Ansichten hinzugefügt wird.

SampleExtensionButtonReport.zip

Eine Erweiterung, mit der eine Schaltfläche zum Öffnen eines Berichts in allen Ansichten hinzugefügt wird.

SampleExtensionButtonWebsite.zip

Eine Erweiterung, mit der eine Schaltfläche zum Öffnen einer Website in allen Ansichten hinzugefügt wird.

SampleExtensionContextMenuItem.zip

Eine Erweiterung, mit der ein Menüelement () zum Popup-Menü für alle Berichtsobjekte hinzugefügt wird. Wenn das Menüelement ausgewählt wird, öffnet es einen Alert, der Informationen zum Bericht anzeigt.

SampleExtensionCustomMedia.zip

Eine Erweiterung, mit der in Dashboards verwendbare benutzerdefinierte Bilder hinzugefügt werden.

SampleExtensionCustomMediaAll.zip

Eine Erweiterung, mit der sowohl in Dashboards als auch in Berichten verwendbare benutzerdefinierte Bilder hinzugefügt werden.

SampleExtensionCustomShape.zip

Eine Erweiterung, mit der in Dashboards verwendbare benutzerdefinierte Formen hinzugefügt werden.

SampleExtensionExcludeDelete.zip

Eine Erweiterung, mit der die Schaltfläche **Löschen** von allen Objekten in allen Ansichten entfernt wird.

SampleExtensionExcludeNotifications.zip

Eine Erweiterung, mit der die Schaltfläche **Benachrichtigungen** von allen Ansichten entfernt wird.

SampleExtensionMenuQuicklinks.zip

Eine Erweiterung, mit der ein Menü zu allen Ansichten hinzugefügt wird.

SampleExtensionMenuUrlLinks.zip

Eine Erweiterung, die veranschaulicht, wie ein Menü zur App-Leiste hinzugefügt wird, das 2 Menüelemente zum Öffnen externer URLs enthält.

SampleExtensionOpenFolderShowHideParent.zip

Eine Erweiterung, die die Verwendung der Option `skipAncestors` beim Öffnen eines Ordners zeigt.

SampleExtensionsAll.zip

In dieser Erweiterung sind die Erweiterungen `SampleExtensionButtonDashboard.zip`, `SampleExtensionButtonFolder.zip`, `SampleExtensionButtonWebsite.zip`, `SampleExtensionButtonReport.zip`, `SampleExtensionContextMenuItem.zip`, `SampleExtensionExcludeDelete.zip`, `SampleExtensionMenuQuicklinks.zip` und `SampleExtensionExcludeNotifications.zip` kombiniert.

SampleExtensionTabs.zip

Eine Erweiterung, mit der eine Gruppe Registerkarten, die schnellen Zugriff auf bestimmte Berichte und Dashboards bieten, zur Startansicht hinzugefügt wird.

11.1.0 **SampleExtensionHelpMenu.zip**

Eine Erweiterung, die dem Hilfesymbolmenü in der oberen Anwendungsleiste in allen Perspektiven eine benutzerdefinierte URL hinzufügt.

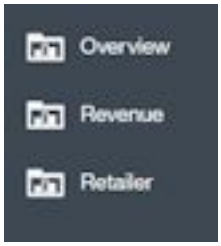
Anmerkung: Ab Release 11.1.6 wird SampleExtensionHelpMenu.zip nicht mehr unterstützt.

Verwenden der Erweiterung für die Registerkartensammlung

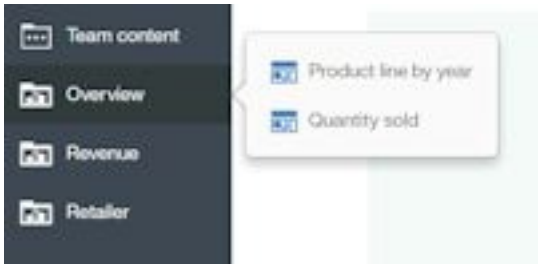
Diese Aufgabe enthält eine Beschreibung der Installation und Verwendung der Erweiterung für die Registerkartensammlung.

Informationen zu diesem Vorgang

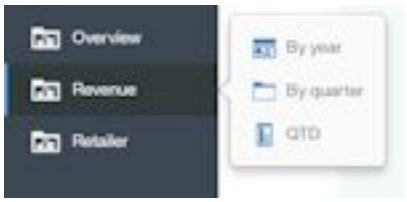
Die Erweiterung für die Registerkartensammlung emuliert die in älteren Versionen von IBM Cognos Business Intelligence verfügbaren Portalseiten. Mit dieser Erweiterung werden drei Schaltflächen wie hier gezeigt zur Navigationsleiste hinzugefügt.



Jede Schaltfläche entspricht einer Registerkarte auf einer Portalseite. Klicken Sie auf die Schaltfläche **Übersicht**, um einen Unterordner anzuzeigen, der zwei Elemente enthält: das Dashboard **Produktreihe je Jahr** und den Bericht **Absatzmenge**. Der Unterordner ist äquivalent zu einer untergeordneten Registerkarte auf einer Portalseite.



Klicken Sie auf die Schaltfläche **Einnahmen**, um einen Unterordner anzuzeigen, der drei Elemente enthält: das Dashboard **Nach Jahr**, den Ordner **nach Quartal** mit vier Berichten und den Bericht **Quartal bisher**.



Klicken Sie auf die Schaltfläche **Einzelhändler**, um ein Dashboard zu öffnen.

Vorgehensweise

Laden Sie das Bereitstellungsarchiv **Samples_for_Install** hoch. (Falls dies bereits geschehen ist, können Sie diesen Schritt überspringen.)

1. Öffnen Sie **IBM Cognos Administration** über **Verwalten** > **Administrationskonsole**.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Inhaltsadministration**.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neuer Import**.
4. Wählen Sie im ersten Schritt des Assistenten **Neuer Import** die Option **Samples_for_Install** aus und führen Sie die verbleibenden Schritte im Assistenten aus.

Laden Sie die Beispielerweiterung `SampleExtensionTabs.zip` hoch.

5. Wählen Sie im Slideout-Fenster **Verwalten** > **Anpassungen** die Registerkarte **Erweiterungen** aus, klicken Sie auf **Erweiterung hochladen** ( ), navigieren Sie zum Ordner *<Installationsverzeichnis>*`/samples/extensions` und wählen Sie `SampleExtensionTabs.zip` aus.

Ergebnisse

Sie können diese Erweiterung jetzt verwenden.

Erstellen von Ansichten

Die Benutzerschnittstelle von IBM Cognos Analytics besteht aus Ansichten. Dazu gehören beispielsweise die Startansicht, die Anmeldeansicht, die Authoring-Ansicht, die Dashboardansicht und die Modellierungsansicht. Sie können benutzerdefinierte Ansichten erstellen und damit die integrierten Ansichten erweitern.

Ansichten sind in einer Datei mit dem Namen `spec.json` definiert, die sich im Stammverzeichnis der ZIP-Datei für die Ansicht befindet. Benutzerdefinierte Ansichten enthalten auch das HTML-Element `div`, durch das das zentrale Fenster der Benutzerschnittstelle von Cognos Analytics ersetzt wird. Darüber hinaus können benutzerdefinierte Ansichten dazu verwendet werden, Menüs und Schaltflächen zur Anwendungsleiste und zur Navigationsleiste hinzuzufügen bzw. von diesen zu entfernen oder die Anwendungsleiste und/oder die Navigationsleiste selbst zu entfernen. Struktur und Inhalt der Datei `spec.json` sind in „Beschreibung der Datei spec.json" auf Seite 229 beschrieben. Die allgemeine Struktur der Datei ist hier dargestellt.

```
{
    "name": "<Name>",
    "schemaVersion": "2.0",
    "extensions": [{
        "perspective":"<Ansichtsname>",
        "type":"<Start- oder Anmeldeansicht>",
        "excludeCommon": true,
        "features": [{
            "id": "<ID>",
            "toolItems": [<Toolelement1>,<Toolelement2>,...],
            "content": {
                "type":"<Pfad der JavaScript-Datei>",
                "options": {
                    ...
                    }
                }
            },
            "cssStyles": [
                "<Pfad der CSS-Datei>"
                ]
        }]
    }]
}
```

Ansichten sind als Erweiterungen gepackt und die ZIP-Datei einer Ansicht kann auch Erweiterungselemente enthalten. So wird mit Beispiel `SampleExtensionButtonOpenPerspective.zip` z. B. eine benutzerdefinierte Ansicht definiert und darüber hinaus eine Schaltfläche zur Navigationsleiste der Startansicht hinzugefügt, über die die benutzerdefinierte Ansicht aufgerufen wird.

Das Element `content` enthält den Pfad und den Namen der JavaScript-Datei, die zur Erstellung der benutzerdefinierten Ansicht ausgeführt wird. Das Element `options` enthält alle Optionen, die für die JavaScript-Datei erforderlich sind. Die JavaScript-Dateien nutzen die AMD-API (Asynchronous Module Definition).

Bei einer Anmeldeansicht handelt es sich um einen speziellen Ansichtstyp. Dieser Ansichtstyp ermöglicht es Ihnen, eine benutzerdefinierte Anmeldeseite für Cognos Analytics zu erstellen. Der Wert des Elements `type` bestimmt, ob es sich bei einer Ansicht um eine Anmeldeansicht (der Wert ist `login`) handelt oder nicht (der Wert ist `home`).

Im Gegensatz zu Erweiterungen müssen Ansichten explizit aufgerufen werden, damit sie geöffnet werden. Es gibt drei Möglichkeiten, eine Ansicht aufzurufen.

- Zum Öffnen der Ansicht kann eine Schaltfläche oder ein Menüelement definiert werden.
- Die Ansicht kann über eine URL wie folgt geöffnet werden.

  ```
  http://<Server>:<Port>/bi/?perspective=<Ansichtsname>
  ```

- Die Ansicht kann als Standardstartansicht für einen Benutzer, für eine Rolle oder für alle Benutzer festgelegt werden. Weitere Informationen finden Sie unter „Anwenden von Motiven, Erweiterungen und Ansichten" auf Seite 227.

Erstellen einer Ansicht (mit Ausnahme von Anmeldeansichten)

Das Beispiel SampleWelcome.zip ist ein Beispiel für eine Ansicht, die die integrierte Startansicht durch eine alternative Version ersetzt, die das Branding für die **Beispielfirma für Outdoor-Ausrüstung** enthält.

Das Beispiel SampleWelcome.zip enthält eine spec.json-Datei zur Definition der Ansicht. Diese Datei ist hier dargestellt.

```
{
  "name": "Sample_Welcome",
  "schemaVersion": "2.0",
  "extensions": [{
    "perspective":"Sample welcome",
    "type":"home",
    "features": [{
      "id": "com.sample.welcome",
      "excludeItems": ["com.ibm.bi.glass.common.cognosLogo"],
      "toolItems": [{
        "id": "brandLogoHomePage",
        "containerId" : "com.ibm.bi.glass.appbarLeadingGroup",
        "type": "bi/glass/app/plugins/GlassPlugin",
        "class": "cognosIcon cognosLogo",
        "label":"theme.current.brandTextSmall",
        "icon": "theme.current.images.brandIconSmall",
        "weight": 995
        }],
      "content": {
        "type":"v1/ext/Sample_Welcome/js/views/SampleWelcomeView",
        "options": {
          "info":{
            "title":"Sample welcome",
            "icon":"v1/ext/Sample_Welcome/images/bee_blue.svg"
          }
        }
      },
      "cssStyles": [
        "v1/ext/Sample_Welcome/css/SampleWelcomeCSS.css"
        ]
    }]
  }]
}
```

Die Ansicht wird in den Anpassungsadministrationsanzeigen als Sample welcome bezeichnet. Die Datei spec.json ist über einen Link mit der Datei SampleWelcomeView.js im Unterordner js/views der Ansicht verknüpft. Der Eintrag "type":"home" gibt an, dass diese Ansicht als Standardstartansicht festgelegt werden kann. Das Element cssStyles definiert die CSS-Datei, die bei der Anzeige der Ansicht verwendet wird.

Die Datei SampleWelcomeView.js ist hier dargestellt.

```
/**
 * Licensed Materials - Property of IBM
 *
 * IBM Cognos Products: BI Glass
 *
 * Copyright IBM Corp. 2015
 *
 * US Government Users Restricted Rights - Use, duplication or disclosure restricted
 * by GSA ADP Schedule Contract with IBM Corp.
 */
define(['q',
  'text!./SampleWelcomeView.html',
  ], function(Q, html) {
  'use strict';

  var ContentView = function(){

    /**
     * Wird bei jeder Erstellung dieser Ansicht von AppController aufgerufen.
     *
     * @public
     * @returns {Promise} - Promise, das in das DOM-Stammelement für diese Ansicht aufgelöst
wird.
     */
    this.open = function(context, options) {
      this.logger = context.logger;
```

```
      this.options = options;
      var deferred = Q.defer();

      var root = document.createElement('div');
      root.setAttribute('class','welcome');

      root.innerHTML = html;
      deferred.resolve(root);
      return deferred.promise;
    };

    /**
     * Wird bei jedem Löschen dieser Ansicht von AppController aufgerufen.
     *
     * @public
     */
    this.close = function() {
      this.logger.info('close');
    };

    /**
     * Wird bei jeder Anzeige dieser Ansicht von AppController aufgerufen.
     *
     * @public
     */
    this.onShow = function() {
      this.logger.info('onShow');
    };

    /**
     * Wird bei jedem Ausblenden dieser Ansicht von AppController aufgerufen.
     *
     * @public
     */
    this.onHide = function() {
      this.logger.info('onHide');
    };

    /**
     * Wird von AppController aufgerufen, wenn Anzeigeinformationen für diese Ansicht erforder
lich sind.
     *
     * @public
     * @returns {Object} displayInfo - displayInfo für diese Ansicht
     * @returns {string} displayInfo.title - Titel
     * @returns {string} displayInfo.icon - Symbol
     */
    this.getDisplayInfo = function() {
      this.logger.info('getDisplayInfo');
      return {
        'title':this.options.info.title,
        'icon': this.options.info.icon
      };
    };

  };

  return ContentView;

});
```

Diese Datei referenziert die Datei `SampleWelcomeView.html`, die beim Aufrufen der Ansicht angezeigt wird.

Dieser JavaScript-Code verwendet die Ansichts-API in einem JavaScript-AMD-Modul. Bei dieser Implementierung wird die JavaScript Q-Bibliothek verwendet. Die Ansichts-API besteht aus den folgenden Methoden.

promise open(content. options)
Diese Methode wird beim Öffnen der Ansicht aufgerufen. Sie gibt ein `Q promise`-Objekt zurück, wobei das DOM-Element, das die Ansicht darstellt, der aufgelöste Wert ist.

context
Enthält das Kontextobjekt.

options
Enthält die Optionen, die in der Datei `spec.json` enthalten sind.

void close()
Wird unmittelbar vor dem Schließen der Ansicht aufgerufen.

void onShow()
Wird unmittelbar vor dem Anzeigen der Ansicht aufgerufen.

void onHide()
Wird unmittelbar vor dem Ausblenden der Ansicht aufgerufen.

getDisplayInfo()
Gibt den Titel und das zugehörige Symbol der Ansicht zurück.

Erstellen einer Anmeldeansicht

Mit einer benutzerdefinierten Anmeldeansicht können Sie die Standardanmeldeseite von IBM Cognos Analytics ersetzen. Sie können ein eigenes Branding verwenden und weitere Änderungen an der Anmeldeseite vornehmen.

Nachfolgend finden Sie einen allgemeinen Überblick über die Struktur des JavaScript-Codes, der zum Durchführen einer Anmeldung erforderlich ist.

Das Beispiel `SampleLogin.zip` enthält eine Beispielansicht, mit der die integrierte Anmeldeansicht durch eine alternative Version ersetzt wird. Das Beispiel `SampleWelcome.zip` enthält eine `spec.json`-Datei zur Definition der Ansicht. Diese Datei ist hier dargestellt.

```
{
    "name": "Sample_Login",
    "schemaVersion": "2.0",
    "extensions": [{
        "perspective":"sampleLogin",
        "type": "login",
        "excludeCommon": true,
        "features": [{
            "id": "com.sample.login",
            "toolItems": [],
            "content": {
                "type":"v1/ext/Sample_Login/login/js/views/SampleLoginView",
                "options": {
                    "info":{
                            "title":"Sample login"
                            }
                }
            },
            "cssStyles": ["v1/ext/Sample_Login/login/css/SampleLoginCSS.css"]
        }]
    }]
}
```

Diese `spec.json`-Datei ähnelt der Datei mit demselben Namen im Beispiel `SampleWelcome.zip`; der Unterschied besteht darin, dass das Element `type` den Wert `login` aufweist und diese Ansicht keine Anwendungs- und Navigationsleiste enthält.

Nachfolgend finden Sie einen allgemeinen Überblick über die Struktur des JavaScript-Codes, der zum Durchführen einer Anmeldung erforderlich ist.

```
   /**
   * @typedef {Object} LoginError
   * @property {string} message - Fehlernachricht
   */
   /**
   * performs a login
   *
   * @public
   * @param {Object[]} loginPrompts - Objekt, das den Anmeldedialog enthält
   * @param {string} loginPrompts[].name - Name des Anmeldedialogs
   * @param {string} loginPrompts[].value - Wert des Anmeldedialogs
   * @return {Promise<undefined|LoginError} Promise ohne Objekt aufgelöst, wenn
   * die Anmeldung erfolgreich ist; wenn die Anmeldung fehlschlägt, wird das Promise mit einem
Fehler abgelehnt.
   *
   */
   signin: function(loginPrompts)
```

Die Datei SampleLoginView.js ist hier dargestellt.

```
/**
 * Licensed Materials - Property of IBM
 * IBM Cognos Products: BI Glass
 * Copyright IBM Corp. 2017
 * US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP
Schedule Contract with IBM Corp.
 */
define(['q',
    'text!./SampleLoginView.html',
    ], function(Q, html) {
    'use strict';

    var ContentView = function(){

        /**
         * Wird bei jeder Erstellung dieser Ansicht von AppController aufgerufen.
         *
         * @public
         * @returns {Promise} - Promise, das in das DOM-Stammelement für diese Ansicht aufge
löst wird.
         */
        this.open = function(context, options) {
            this.logger = context.logger;
            this.options = options;
            var deferred = Q.defer();

            var root = document.createElement('div');
            root.setAttribute('class','welcome');

            root.innerHTML = html;

            var loginBtn = root.getElementsByClassName('sample.loginBtn')[0];
            loginBtn.onclick = function() {
                document.getElementsByClassName('sampleIncorrectLoginText')[0].innerHTML='';
                var uid = document.getElementsByClassName('sample.username')[0].value;
                var pwd = document.getElementsByClassName('sample.password')[0].value;
                var loginPrompts = [
                    {name:'CAMNamespace',value:'CognosEx'},
                    {name:'h_CAM_action',value:'logonAs'},
                    {name:'CAMUsername',value:uid},
                    {name:'CAMPassword',value:pwd}
                ];
                this.signin(loginPrompts).catch(this._loginError.bind(this));
            }.bind(this);


            deferred.resolve(root);
            return deferred.promise;
        },

        /**
         * Wird bei jedem Löschen dieser Ansicht von AppController aufgerufen.
         *
         * @public
         */
        this.close = function() {
            this.logger.info('close');
        },

        /**
         * Wird bei jeder Anzeige dieser Ansicht von AppController aufgerufen.
         *
         * @public
         */
        this.onShow = function() {
            this.logger.info('onShow');
        },

        /**
         *
         * Der nachfolgend dargestellte Live-Code ruft die Fehlernachricht des Produkts ab.
         * Wenn Sie eine eigene Fehlernachricht verwenden möchten, verwenden Sie stattdessen
den folgenden Code dieses Kommentars:
         *
         * this._loginError = function() {
         *      document.getElementsByClassName('sampleIncorrectLoginText')[0].innerHTML='You
have entered an invalid username/password combination.';
         *     this.logger.error('loginError',arguments);
         *   },
```

```
         *
         *
         */
        this._loginError = function(error) {
            document.getElementsByClassName('sampleIncorrectLoginText')[0].innerHTML=error.mes
sage;
            this.logger.error('loginError',arguments);
        },

        /**
         * Wird bei jedem Ausblenden dieser Ansicht von AppController aufgerufen.
         *
         * @public
         */
        this.onHide = function() {
            this.logger.info('onHide');
        },

        /**
         * Wird von AppController aufgerufen, wenn Anzeigeinformationen für diese Ansicht erfor
derlich sind.
         *
         * @public
         * @returns {Object} displayInfo - displayInfo für diese Ansicht
         * @returns {string} displayInfo.title - Titel
         * @returns {string} displayInfo.icon - Symbol
         */
        this.getDisplayInfo = function() {
            this.logger.info('getDisplayInfo');
            return {
                'title':this.options.info.title,
                'icon': this.options.info.icon
            };
        }

    };

    return ContentView;

});
```

Bei einer Anmeldeansicht wird eine zusätzliche Methode verwendet.

promise login(credentials)
Mit dieser Methode wird eine Anmeldeanforderung übergeben und ein `promise`-Objekt zurückgegeben, das zurückgewiesen wird, falls der Anmeldeversuch fehlschlägt.

credentials
Enthält die Anmeldeinformationen.

```
[{name:'CAMNamespace',value:'<Namespace>'},
{name:'h_CAM_action',value:'logonAs'},
{name:'CAMUsername',value:<Benutzername>},
{name:'CAMPassword',value:<Kennwort>}]
```

Anmeldeansicht mit einer Namespace-Eingabeaufforderung erstellen

Mit einer benutzerdefinierten Anmeldeansicht mit Namespace-Eingabeaufforderung können Sie die Standardanmeldeseite von IBM Cognos Analytics ersetzen. Sie können angeben, dass der Benutzer aus einer Liste von Namespaces auswählen muss, wenn er sich anmeldet. Sie können auch ein eigenes Branding verwenden und weitere Änderungen an der Anmeldeseite vornehmen.

Nachfolgend finden Sie einen allgemeinen Überblick über die Struktur des JavaScript-Codes, der zum Durchführen einer Anmeldung erforderlich ist.

Das Beispiel `SampleLoginMultiple.zip` enthält eine Beispielansicht, mit der die integrierte Anmeldeansicht durch eine alternative Version ersetzt wird. Das Beispiel `SampleLoginMultiple.zip` enthält eine `spec.json`-Datei zur Definition der Ansicht. Diese Datei ist hier dargestellt.

```
{
    "name": "Sample_Login_Multiple",
    "schemaVersion": "2.0",
    "extensions": [{
        "perspective":"sampleLoginMultiple",
```

```
        "type": "login",
        "excludeCommon": true,
        "features": [{
            "id": "com.sample.login.multiple",
            "toolItems": [],
            "content": {
                "type":"v1/ext/Sample_Login_Multiple/login/js/views/SampleLoginView",
                "options": {
                    "info":{
                            "title":"Sample login namespaces"
                            }
                }
            },
            "cssStyles": ["v1/ext/Sample_Login_Multiple/login/css/SampleLoginCSS.css"]
        }]
    }]
}
```

Diese spec.json-Datei ähnelt derselben Datei für das Beispiel SampleLogin.zip insofern, als diese Ansicht keine Anwendungs- und Navigationsleiste enthält.

Beispielansichten

Die folgenden Beispiele veranschaulichen die Verwendung von Ansichten.

Bei einer einfachen Installation (Easy Install) werden diese Beispieldateien zusammen mit dem Produkt installiert, bei einer angepassten Installation können Sie als Option ausgewählt werden. Nach der Produktinstallation finden Sie die Dateien im Ordner *Installationsverzeichnis*/samples/extensions.

SampleLogin.zip
Eine Ansicht, die die Cognos Analytics-Anmeldeseite ersetzt.

SampleLoginMultiple.zip
Eine Ansicht als Ersatz für die Cognos Analytics-Anmeldeseite, die den Benutzer zur Angabe eines Namespace auffordert.

SampleWelcome.zip
Eine Ansicht, die die Cognos Analytics-Eingangsseite ersetzt.

Verwenden der benutzerdefinierten Eingangsansicht

Diese Aufgabe enthält eine Beschreibung der Installation und Verwendung der benutzerdefinierten Eingangsansicht.

Vorgehensweise

Laden Sie das Bereitstellungsarchiv **Samples_for_Install** hoch. (Falls dies bereits geschehen ist, können Sie diesen Schritt überspringen.)

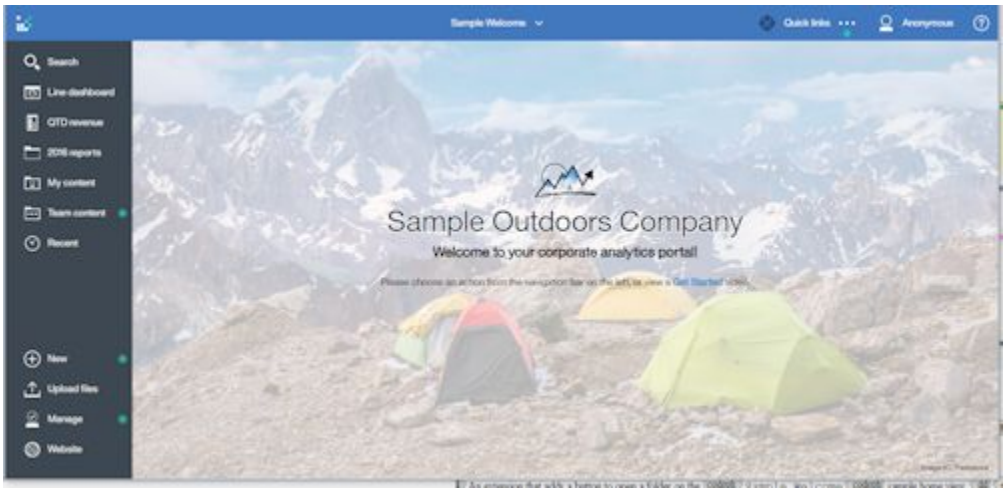
1. Öffnen Sie **IBM Cognos Administration** über **Verwalten** > **Administrationskonsole**.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Inhaltsadministration**.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neuer Import**.
4. Wählen Sie im ersten Schritt des Assistenten **Neuer Import** die Option **Samples_for_Install** aus und führen Sie die verbleibenden Schritte im Assistenten aus.

Laden Sie die Beispielerweiterungen hoch.

5. Wählen Sie im Slideout-Fenster **Verwalten** > **Anpassungen** die Registerkarte **Erweiterungen** aus, klicken Sie auf **Erweiterung hochladen** ( ), navigieren Sie zum Ordner <*Installationsverzeichnis*>/samples/extensions und wählen Sie SampleWelcome.zip aus.
6. Wiederholen Sie den vorherigen Schritt für SampleExtensionsAll.zip.
7. Geben Sie im Web-Browser <*Name des Web-Servers*>:<*Portnummer*>/bi/?perspective=sampleWelcome ein, um die benutzerdefinierte Eingangsansicht aufzurufen.

Ergebnisse

Die benutzerdefinierte Eingangsansicht ist hier dargestellt. Sie enthält ein neues Menü (**Quick Links**) in der Anwendungsleiste und neue Schaltflächen in der Navigationsleiste (**Dashboard für Produktreihe**, **Einnahmen Quartal bisher**, **2016 Berichte** und **Website**). Die Schaltfläche **Benachrichtigungen** in der Navigationsleiste wird entfernt. Die Hauptanzeige enthält ein neues Bild, neuen Text und einen Link zu einem Video.



Verwenden der benutzerdefinierten Anmeldeansicht

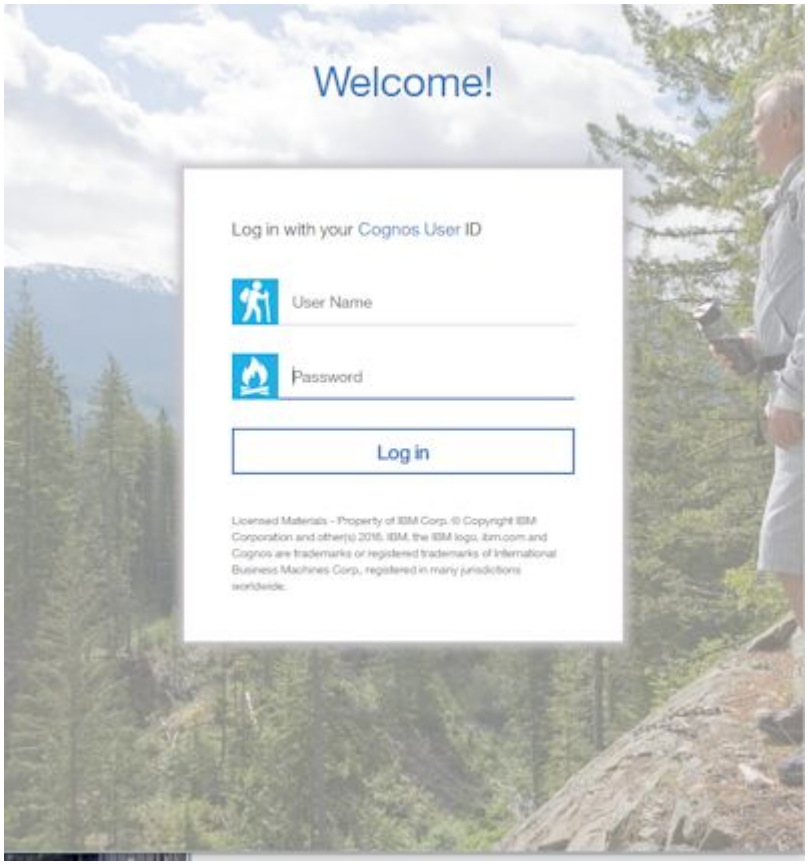
Diese Aufgabe enthält eine Beschreibung der Installation und Verwendung der benutzerdefinierten Anmeldeansicht.

Vorgehensweise

1. Extrahieren Sie die Dateien in `SampleLogin.zip`.
2. Öffnen Sie `login/js/views/SampleLoginView.js` zur Bearbeitung und suchen Sie die Zeile, die die Angabe `{name:'CAMNamespace',value:'CognosEx'}` enthält.
3. Ersetzen Sie `CognosEx` durch den Namen eines Ihrer Authentifizierungsnamespaces (wie in **IBM Cognos Configuration** definiert).
4. Speichern Sie `SampleLoginView.js` und erstellen Sie die .zip-Datei neu.
5. Wählen Sie im Slideout-Fenster **Verwalten** > **Anpassungen** die Registerkarte **Erweiterungen** aus, klicken Sie auf **Erweiterung hochladen** ( ), navigieren Sie zum Ordner *<Installationsverzeichnis>*`/samples/extensions` und wählen Sie `SampleLogin.zip` aus.
6. Klicken Sie auf der Registerkarte **Ansichten** neben der Standardanmeldeansicht auf . Wählen Sie die Ansicht **Beispielanmeldung** als die Standardansicht für die Anmeldung.
7. Melden Sie sich von IBM Cognos Analytics ab.
8. Greifen Sie auf den Cognos Analytics-Server zu.

Ergebnisse

Die benutzerdefinierte Anmeldeansicht ist hier dargestellt. Sie verfügt über einen benutzerdefinierten Hintergrund und neuen Text im Anmeldedialogfeld.



Anwenden von Motiven, Erweiterungen und Ansichten

Sie können Motive, Erweiterungen und Ansichten im Slideout-Fenster **Verwaltung** > **Anpassung** verwalten. Sie können Motive, Erweiterungen und Ansichten hochladen, löschen und ändern. Darüber hinaus können Sie ein Standardmotiv für alle Benutzer sowie eine Standardstartansicht und eine Standardanmeldeansicht festlegen.

Das Slideout-Fenster **Administration** > **Anpassung** enthält vier Registerkarten **Motive**, **Erweiterungn**, **Ansichten** und **Parameter**. Motive werden auf der Registerkarte **Motive** hochgeladen, Erweiterungen und Ansichten auf der Registerkarte **Erweiterungen**.

Hochladen von Motiven

Zum Hochladen eines Motivs klicken Sie auf der Registerkarte **Motive** auf **Motiv hochladen** ( ) und navigieren Sie im Dateisystem zum gewünschten Motiv. Das Motiv wird hochgeladen und validiert. Wenn das Motiv ungültig ist, wird eine Fehlernachricht angezeigt. Andernfalls wird das Motiv zur Liste der verfügbaren Motive hinzugefügt. Sie können auf **Mehr** ( ) neben einem Motiv klicken, um das Motiv zu aktualisieren, herunterzuladen oder zu löschen.

Tipp: Wenn Sie ein Motiv für eine verteilte Umgebung anwenden, müssen Sie mindestens 5 Minuten warten, bis die Änderung wirksam wird.

Festlegen eines Standardmotivs

Sie können ein Motiv auswählen, das als Standardmotiv für alle Benutzer verwendet werden soll. Wählen Sie auf der Registerkarte **Motive** des Slideout-Fensters **Administration** > **Anpassung** das Kontrollkästchen neben einem Motiv aus und klicken Sie dann auf **Anwenden**.

Über das Slideout-Fenster **Verwalten** > **Konten** können Sie auch Standardmotive für Rollen festlegen. Wenn einem Benutzer eine Rolle mit einem Standardmotiv zugewiesen ist, wird dieses Motiv anstelle des

für alle Benutzer ausgewählten Motivs verwendet. Weitere Informationen finden Sie unter „Anpassen von Rollen” auf Seite 7.

Hochladen von Erweiterungen und Ansichten

Zum Hochladen einer Erweiterung oder einer Ansicht klicken Sie auf der Registerkarte **Erweiterungen** auf **Erweiterung hochladen** ( ) und navigieren Sie im Dateisystem zur gewünschten Erweiterung bzw. Ansicht. Die Erweiterung oder Ansicht wird hochgeladen und validiert. Wenn die Erweiterung ungültig ist, wird eine Fehlernachricht angezeigt. Andernfalls wird die Erweiterung zur Liste der hochgeladenen Erweiterungen hinzugefügt. Sie können auf **Mehr** ( ) neben einer Erweiterung oder Ansicht klicken, um die Erweiterung bzw. Ansicht zu aktualisieren, herunterzuladen oder zu löschen.

Standardstartansicht festlegen

Klicken Sie auf der Registerkarte **Ansichten** des Slideout-Fensters **Verwaltung** > **Anpassung** auf neben der Standardstartansicht. Nun können Sie nach einem Dashboard oder Bericht suchen, das bzw. der als Standardstartansicht verwendet werden soll, oder Sie können eine Ansicht in der Liste der Startansichten auswählen, die als Standardstartansicht für alle Benutzer verwendet werden soll.

Über das Slideout-Fenster **Verwalten** > **Konten** können Sie auch Standardstartansichten für Rollen festlegen. Wenn einem Benutzer eine Rolle mit einer Standardstartansicht zugewiesen ist, wird diese Ansicht anstelle der für alle Benutzer ausgewählten Startansicht verwendet. Weitere Informationen finden Sie unter „Anpassen von Rollen” auf Seite 7.

Ein Benutzer kann auch eine persönliche Standardstartansicht von einer beliebigen Ansicht aus auswählen. In einer beliebigen Ansicht kann ein Benutzer auf **Mehr** ( ) und anschließend auf **Als Startansicht festlegen** klicken, um eine persönliche Standardstartansicht zu definieren. Diese Standardstartansicht hat Vorrang gegenüber den Standardstartansichten, die für Rollen oder für alle Benutzer erstellt wurden.

Festlegen einer Standardanmeldeansicht

Klicken Sie auf der Registerkarte **Ansichten** des Slideout-Fensters **Verwaltung** > **Anpassung** auf neben der Standardanmeldeansicht. Nun können Sie eine Ansicht in der Liste der Anmeldeansichten auswählen, die als Standardanmeldeansicht für alle Benutzer verwendet werden soll.

Ausführen von Cognos Analytics mit inaktivierten Erweiterungen und Ansichten

Wenn eine hochgeladene Erweiterung oder Ansicht Fehler enthält, kann dies dazu führen, dass IBM Cognos Analytics nicht mehr verwendet werden kann. In diesem Fall können Sie Cognos Analytics mit inaktivierten benutzerdefinierten Erweiterungen und Ansichten ausführen.

Vorgehensweise

Starten Sie Cognos Analytics, indem Sie die URL `<Name des Web-Servers>:<Portnummer>/bi/?factoryMode=true` eingeben.

Ergebnisse

Beim Start von Cognos Analytics sind alle Erweiterungen inaktiviert. Sie können nun die benutzerdefinierten Erweiterungen oder Ansichten korrigieren oder löschen und anschließend mit der Standard-URL einen Neustart von Cognos Analytics durchführen.

Beschreibung der Datei spec.json

Die Datei spec.json in einer Erweiterung definiert die Elemente, die durch die Erweiterung zur IBM Cognos Analytics-Standardbenutzerschnittstelle hinzugefügt bzw. aus dieser entfernt werden. Die Struktur und die Inhalte dieser Datei werden im Folgenden erläutert.

Die Struktur und die Inhalte, die hier beschrieben werden, weisen einen vorläufigen Status auf. Sie werden möglicherweise in zukünftigen Releases von Cognos Analytics geändert. Diese Änderungen sind möglicherweise nicht abwärtskompatibel.

name
Gibt den Namen der Erweiterung an. Der Name kann alphanumerische Zeichen, Unterstreichungszeichen (_) und Leerzeichen ( ) enthalten.

schemaVersion
Gibt einen numerischen Wert für die Schemaversion an. Der Wert kann 1.0 oder 2.0 lauten. Der Standardwert lautet 1.0.

extensions
Enthält ein Array von Objekten des Typs perspective.

perspective
Gibt die Ansicht an, die erweitert wird. Die Optionen sind nachfolgend aufgeführt.

common
Wird für alle Ansichten angewendet.

<Ansichtsname>
Wird für die Ansicht *<Ansichtsname>* angewendet. Hierbei kann es sich um eine integrierte Ansicht (home, authoring, dashboard oder modeller) oder um eine hochgeladene Ansicht handeln.

type
Gibt den Typ an, wenn es sich bei der Erweiterung um eine Ansicht handelt. Die möglichen Werte sind login für eine Anmeldeansicht und home für eine Startansicht. Dieses Element wird nur in der Schemaversion 2.0 verwendet. Wenn dieses Element weggelassen wird und die Schemaversion 2.0 angegeben ist, wird die Ansicht nicht in der Liste möglicher Standardstartansichten oder Standardanmeldeansichten aufgeführt.

excludeCommon
Gibt an, ob Ansichtsbeiträge aus dem Ordner /common empfangen werden. Die möglichen Werte sind false zum Empfang aller Beiträge und true zum Empfang keiner Beiträge. Alle fehlenden Beiträge können der Erweiterung hinzugefügt werden.

lensable
Bei der Angabe false wird diese Ansicht nicht in der Liste der Ansichten aufgeführt, für die Features weggelassen werden können. Weitere Informationen finden Sie unter „Anpassen von Rollen" auf Seite 7.

Der Standardwert lautet true.

comment
Optionaler Kommentar.

features
Enthält ein Array mit Featuregruppierungen.

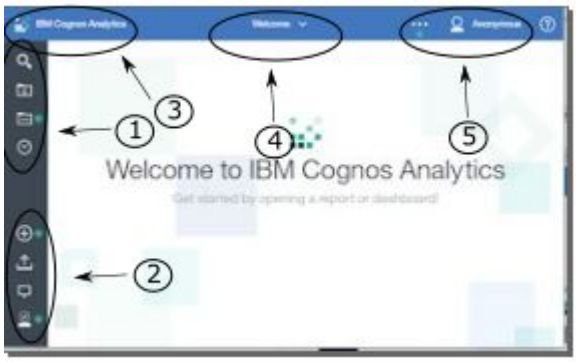
id
Gibt die eindeutige ID des Features an.

toolItems
Enthält ein Array mit Benutzerschnittstellenelementen, die hinzugefügt werden.

id
Die eindeutige ID für das neue Benutzerschnittstellenelement.

containerId
Gibt die Position des Benutzerschnittstellenelements an.

- Wenn es sich bei dem Benutzerschnittstellenelement um ein Menü oder eine Schaltfläche handelt, befindet sich das Element in der Anwendungs- oder Navigationsleiste, wie in der folgenden Abbildung dargestellt.



  Die Werte für `containerId`, die der Positionierung der Schaltfläche oder des Menüs entsprechen, werden in der folgenden Liste angezeigt.

  1. `com.ibm.bi.glass.navbarLeadingGroup`
  2. `com.ibm.bi.glass.navbarTrailingGroup`
  3. `com.ibm.bi.glass.appbarLeadingGroup`
  4. `com.ibm.bi.glass.appbarCenterGroup`
  5. `com.ibm.bi.glass.appbarTrailingGroup`

- Wenn es sich bei dem Benutzerschnittstellenelement um ein Menüelement handelt, ist der Wert für `containerId` die `id` des Menüs, das das Menüelement enthält. Informationen zur Bestimmung einer `id` finden Sie in „Bestimmen der ID eines Benutzerschnittstellenobjekts” auf Seite 235.

`label`
Gibt die Textbeschriftung für das Benutzerschnittstellenelement an. Dieser Text kann nicht lokalisiert werden.

`type`
Gibt den Typ des Benutzerschnittstellenelements an. Die möglichen Werte sind nachfolgend aufgeführt.

- `Button`
- `Menu`
- `MenuItem`

`icon`
Gibt das Bild an, das für das Benutzerschnittstellenelement angezeigt werden soll. Die Pfadangabe ist relativ zu der Bilddatei im ZIP-Archiv der Erweiterung.

`weight`
Gibt einen numerischen Wert an, der die Position des Benutzerschnittstellenelements im Container bestimmt. Durch einen höheren Wert wird das Element im Container nach oben verschoben.

`push`
Gibt an, ob die Aktion der ersten Auswahl bei erneutem Auswählen derselben Schaltfläche rückgängig gemacht wird. Beispiel: das Öffnen und anschließende Schließen eines Ordners. Der Wert kann `true` oder `false` sein. Für eine Schaltfläche zum Öffnen eines Ordners muss der Wert `true` sein.

`coachMark`
Gibt eine Coachmarkierung an.

`title`
Gibt den Titel der Coachmarkierung an.

contents
Gibt die Inhalte der Coachmarkierung an.

actionController
Gibt die Aktion an, die ausgeführt werden soll, wenn auf das Benutzerschnittstellenelement geklickt wird. Die verfügbaren Aktionen sind hier aufgeführt.

bi/glass/api/IFrameOpener
Öffnet eine Webseite.

bi/glass/api/ReportOpener
Öffnet einen bestimmten Bericht.

bi/glass/api/DashboardOpener
Öffnet ein bestimmtes Dashboard.

bi/glass/api/FolderOpener
Öffnet einen bestimmten Ordner.

v1/ext/*<Name>*/js/controllers/*Controllername*
Führt den im Erweiterungspackage enthaltenen benutzerdefinierten Controller aus. Beim Controller handelt es sich um die Datei `js/controllers/`*`Controllername`*`.js`.

options
Enthält ein Array mit Optionen, die an den Aktionscontroller übergeben werden sollen. Die verfügbaren Option hängen vom verwendeten Aktionscontroller ab. Informationen zu den von den integrierten Aktionscontrollern verwendeten Optionen finden Sie in „Verwenden integrierter Aktionscontroller" auf Seite 206.

collectionItems
Enthält ein Array mit Benutzerschnittstellenelementen, die hinzugefügt werden.

containerId
Gibt an, wo das Benutzerschnittstellenelement lokalisiert ist.

id
Gibt die eindeutige ID des Benutzerschnittstellenelements an.

content
Enthält Definitionen für eine Ansicht.

type
Enthält einen Link zu der JavaScript-Datei, die ausgeführt werden soll, wenn diese Ansicht aufgerufen wird.

options
Enthält Parameter, die an die JavaScript-Datei übergeben werden sollen.

cssStyles
Enthält ein Array mit Links zu .css-Dateien, die für diese Ansicht verwendet werden sollen.

excludeFeatures
Enthält ein Array mit IDs der Benutzerschnittstellenfeatures, die ausgeschlossen werden sollen. Dieses Feature kann für die Ansicht `common` nicht angewendet werden.

Informationen zur Bestimmung einer `id` finden Sie in „Bestimmen der ID eines Benutzerschnittstellenobjekts" auf Seite 235.

excludeItems
Enthält ein Array mit IDs der Benutzerschnittstellenelementen, die ausgeschlossen werden sollen. Dieses Feature kann für die Ansicht `common` nicht angewendet werden.

Informationen zur Bestimmung einer `id` finden Sie in „Bestimmen der ID eines Benutzerschnittstellenobjekts" auf Seite 235.

JSON-Schemaprüfung

Wenn Sie eine Datei `spec.json` hochladen, wird sie anhand des folgenden Schemas geprüft.

```
{
  "type": "object",
  "definitions": {
    "extType": {
      "type": "string",
      "minLength": 1,
      "pattern": "^v1/ext/.+$"
    },
    "noEmptyString": {
      "type": "string",
      "minLength": 1
    },
    "toolItem": {
      "type": "object",
      "properties": {
        "id": {
          "$ref": "#/definitions/noEmptyString"
        },
        "title": {
          "type": "string"
        },
        "type": {
          "$ref": "#/definitions/noEmptyString"
        },
        "actionController": {
          "$ref": "#/definitions/noEmptyString"
        },
        "label": {
          "$ref": "#/definitions/noEmptyString"
        },
        "containerId": {
          "$ref": "#/definitions/noEmptyString"
        },
        "icon": {
          "type": "string"
        },
        "weight": {
          "type": "number"
        },
        "class": {
          "type": "string"
        },
        "comment": {
          "type": "string"
        },
        "options": {
          "type": "object"
        },
        "push": {
          "type": "string",
          "enum": [
            "true",
            "false"
          ]
        },
        "coachMark": {
          "type": "object",
          "properties": {
            "title": {
              "type": "string"
            },
            "contents": {
              "type": "string"
            }
          },
          "additionalProperties": false,
          "required": [
            "title"
          ]
        },
        "lensable": {
          "type": "boolean"
        }
      },
      "required": [
        "id"
      ]
    },
    "collectionItem": {
      "type": "object",
      "properties": {
```

```
        "id": {
          "$ref": "#/definitions/noEmptyString"
        },
        "containerId": {
          "$ref": "#/definitions/noEmptyString"
        },
        "label": {
          "$ref": "#/definitions/noEmptyString"
        },
        "lensable": {
          "type": "boolean"
        }
      },
      "required": [
        "id",
        "containerId"
      ]
    },
    "collectionContainerItem": {
      "type": "object",
      "properties": {
        "id": {
          "$ref": "#/definitions/noEmptyString"
        },
        "label": {
          "$ref": "#/definitions/noEmptyString"
        },
        "lensable": {
          "type": "boolean"
        }
      },
      "required": [
        "id"
      ]
    },
    "collectionContainer": {
      "type": "object",
      "properties": {
        "id": {
          "$ref": "#/definitions/noEmptyString"
        },
        "items": {
          "type": "array",
          "items": {
            "$ref": "#/definitions/collectionContainerItem"
          }
        },
        "lensable": {
          "type": "boolean"
        }
      },
      "additionalProperties": false,
      "required": [
        "id"
      ]
    },
    "feature": {
      "type": "object",
      "properties": {
        "id": {
          "$ref": "#/definitions/noEmptyString"
        },
        "excludeItems": {
          "type": "array",
          "items": {
            "$ref": "#/definitions/noEmptyString"
          }
        },
        "excludeFeatures": {
          "type": "array",
          "items": {
            "$ref": "#/definitions/noEmptyString"
          }
        },
        "toolItems": {
          "type": "array",
          "items": {
            "$ref": "#/definitions/toolItem"
          }
        },
        "content": {
          "type": "object",
```

```
        "properties": {
          "type": {
            "$ref": "#/definitions/extType"
          },
          "options": {
            "type": "object"
          }
        },
        "additionalProperties": false,
        "required": [
          "type"
        ]
      },
      "cssStyles": {
        "type": "array",
        "items": {
          "$ref": "#/definitions/extType"
        }
      },
      "collectionItems": {
        "type": "array",
        "items": {
          "$ref": "#/definitions/collectionItem"
        }
      },
      "collectionContainers": {
        "type": "array",
        "items": {
          "$ref": "#/definitions/collectionContainer"
        }
      },
      "comment": {
        "type": "string"
      },
      "lensable": {
        "type": "boolean"
      }
    },
    "additionalProperties": false,
    "required": [
      "id"
    ]
  },
  "extension": {
    "type": "object",
    "properties": {
      "perspective": {
        "$ref": "#/definitions/noEmptyString"
      },
      "features": {
        "type": "array",
        "minItems": 1,
        "items": {
          "$ref": "#/definitions/feature"
        }
      },
      "type": {
        "type": "string",
        "enum": [
          "home",
          "login"
        ]
      },
      "excludeCommon": {
        "type": "string",
        "enum": [
          "true",
          "false"
        ]
      },
      "lensable": {
        "type": "boolean",
        "default": true
      },
      "comment": {
        "type": "string"
      }
    },
    "additionalProperties": false
  }
},
"properties": {
```

```
    "schemaVersion": {
      "type": "string",
      "enum": [
        "1.0",
        "2.0"
      ]
    },
    "name": {
      "type": "string",
      "pattern": "[a-zA-Z0-9_ ]+$"
    },
    "extensions": {
      "type": "array",
      "minItems": 1,
      "items": {
        "$ref": "#/definitions/extension"
      }
    },
    "comment": {
      "type": "string"
    }
  },
  "additionalProperties": false,
  "required": [
    "name",
    "extensions"
  ]
}
```

Bestimmen der ID eines Benutzerschnittstellenobjekts

Sie müssen die `id` eines vorhandenen Benutzerschnittstellenelements bestimmen, wenn Sie Erweiterungen erstellen, die Features oder Elemente ausschließen oder die Menüelemente zu einem vorhandenen Menü hinzufügen.

Vorgehensweise

1. Wenn Sie Cognos Analytics 11.0.7 oder höher ausführen, führen Sie die folgenden Schritte aus:
   a) Öffnen Sie das Fenster für Windows-Dienste und stoppen Sie den Service **IBM Cognos**.
   b) Öffnen Sie die Datei *Installationsverzeichnis*`\wlp\usr\servers\cognosserver\bootstrap.properties`.
   c) Fügen Sie die folgende Zeile hinzu:

      ```
      disableXSRFCheck=true
      ```

   d) Speichern Sie die Datei.
   e) Starten Sie den Service **IBM Cognos** erneut.
2. Melden Sie sich bei Ihrem IBM Cognos Analytics-Server an.
3. Geben Sie die folgende URL in einem Web-Browser ein: `http://<`*Servername*`>:<`*Port*`>/bi/v1/perspectives/<`*Ansicht*`>`. Dabei ist *<Ansicht>* die Ansicht (`home`, `authoring`, `dashboard` oder `modeller`), die das Benutzerschnittstellenobjekt enthält.

   Eine JSON-Datei wird zurückgegeben, die eine Beschreibung aller Benutzerschnittstellenelemente in der Ansicht enthält.
4. Suchen Sie nach dem Kurzinfotext für das Benutzerschnittstellenelement.

   Die Angaben für `id` und `featureId` der Benutzerschnittstellenelemente werden nach dem Kurzinfotext angezeigt.

Beispiel

Wenn Sie in der für die Startansicht zurückgegebenen JSON-Datei nach **Delete** suchen, wird der folgende Teil der Datei angezeigt.

```
"label": "Delete",
"id": "com.ibm.bi.contentApps.deleteAction.DeleteAction",
"featureId": "com.ibm.bi.contentApps.deleteAction"
```

Die Werte für `id` und `featureId` können in der Erweiterung verwendet werden, um bei Bedarf diese Schaltfläche oder dieses Feature auszuschließen.

Erstellen einer globalen Farbpalette

11.1.0 -Administratoren können globale Farbpaletten erstellen, die für Berichte, Dashboards und Story-Autoren verfügbar sind.

Informationen zu diesem Vorgang

Sie können die folgenden Typen von Farbpaletten erstellen:

Kategorien
Wird für Visualisierungen verwendet, die diskrete Farben unterstützen, wie z. B. ein Balken-oder Kreisdiagramm.

Kontinuierlich
Wird für Visualisierungen verwendet, die Farbübergänge unterstützen, wie z. B. eine Karte oder eine Heat-Map.

Einige Visualisierungen unterstützen beide Arten von Farbpaletten. Wenn Sie zum Beispiel eine Kennzahl auf den Farbschlitz eines Balkendiagramms ablegen, können Sie den Balken für diese Kennzahl einen Farbverlauf hinzufügen. Die folgenden Visualisierungen unterstützen beide Arten von Farbpaletten:

- Bar, schwebende Leiste, gestapeltes Balken
- Variable Spalte, gestapelte Spalte
- Blase, gepackte Blase, hierarchische verpackte
- Marimekko
- Radial
- Streudiagramm
- Baumstrukturzuordnung

Farbpaletten sind in die folgenden Kategorien eingeteilt:

Angepasst
Erstellt von einem Benutzer (Bericht, Dashboard oder Story-Autor). Nur für den Benutzer verfügbar, der sie erstellt hat. Weitere Informationen zu angepassten Paletten finden Sie unter *Farbpalette erstellen* in der *Dashboards und Stories-Handbuch*.

Global
Erstellt durch den Systemadministrator. Für alle Benutzer steht eine globale Palette zur Verfügung, aber nur ein Administrator kann sie ändern. Ein Benutzer kann eine globale Palette duplizieren und anschließend die duplizierte Version ändern.

System
Standardpaletten, die in IBMCognos Analyticsverfügbar sind. Eine Systempalette kann nicht geändert werden, aber ein Benutzer kann ihn duplizieren und anschließend die duplizierte Version ändern.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Anpassung**, und wählen Sie dann die Registerkarte **Paletten** aus.
2. Klicken Sie auf **Angepasste Palette erstellen** .

Das Fenster **Kategorische Farbpalette erstellen** wird geöffnet.

3. Um eine kontinuierliche Farbpalette zu erstellen, klicken Sie auf **Kontinuierliche Palette**  .
4. Geben Sie einen Namen für Ihre Palette ein.
5. Klicken Sie auf die Registerkarte **Raster** oder **Rad** .

   Auf der Registerkarte **Raster** können Sie Farben aus einem Raster von Farbsuhren auswählen. Auf der Registerkarte **Rad** können Sie eine Farbe auswählen, indem Sie eine der folgenden Aktionen ausführen:

   - Anklicken des Farbrads
   - Eingabe der Farbe in HSB (Farbton, Sättigung, Helligkeit) oder RGB-Notation (rot, grün, blau)
   - Farbe im Hexadezimalcode eingeben
6. Klicken Sie unter **Farbführung**auf **Automatisch** oder **Angepasst**.

   Kategorische Farbpalette
   Enthält eine Reihe von Uhren. Wenn Sie in **Automatisch**eine Farbe aus dem Raster oder dem Rad auswählen, werden alle Uhren in der Palette mit Farben gefüllt, die sich auf die von Ihnen ausgewählte Farbe beziehen, ausgehend von der aktuell ausgewählten Uhr. In **Angepasst**müssen Sie jede Swatch auswählen und anschließend eine Farbe für sie auswählen.

   Kontinuierliche Farbpalette
   Enthält eine fortlaufende Armbanduhr. Wenn Sie in **Angepasst**eine Farbe aus dem Gitter oder dem Rad auswählen, wird die Uhr mit der ausgewählten Farbe gefüllt. Die Farbe steigt allmählich in der Intensität von einem Ende der Swatch auf das andere. **Automatisch** ist für eine kontinuierliche Farbpalette nicht verfügbar.
7. Um eine Auswahl rückgängig zu machen, klicken Sie auf **Swatch entfernen**  .
8. Wenn Sie der Palette weitere Uhren hinzufügen möchten, klicken Sie auf **Swatch hinzufügen**  .
9. Wenn Sie die Farben in der Palette umkehren möchten, klicken Sie auf **Umgekehrte Palette**  .
10. Klicken Sie auf **Speichern** , wenn Sie fertig sind.

Ergebnisse

Die Farbpalette wird unter **Global** angezeigt und ist für alle Berichte, Dashboards und Story-Autoren verfügbar.

Verwalten von Benutzerprofilen

Ein Benutzerprofil definiert die Portalregisterkarten, auf die der Benutzer zugreifen kann, und gibt Benutzervorgaben an, z. B. die Produktsprache, das bevorzugte Ausgabeformat von Berichten und den Stil, der in der Benutzerschnittstelle verwendet wird.

Ein Benutzerprofil wird erstellt, wenn sich der Benutzer zum ersten Mal bei der IBM Cognos-Software anmeldet. Es kann auch von einem Administrator erstellt werden. Ursprünglich basiert das Profil auf dem Standardbenutzerprofil.

Benutzer können die dem Profil zugeordneten Vorgaben anzeigen oder ändern.

Zum Kopieren, Bearbeiten oder Löschen von Benutzerprofilen muss ein Administrator über Schreibberechtigungen für den Namespace verfügen, der die entsprechenden Benutzer enthält. Die in IBM Cognos vordefinierte Rolle, **Verzeichnisadministratoren**, hat nur für den Namespace **Cognos** Schreibberechtigungen. **Systemadministratoren** müssen **Verzeichnisadministratoren** Schreibberechtigungen erteilen, damit diese Benutzerprofile für den Namespace verwalten können.

Weitere Informationen finden Sie unter Kapitel 1, „Verwalten von Personen”, auf Seite 1.

Bearbeiten des Standardbenutzerprofils

Das Standardbenutzerprofil wird im Namespace **Cognos** definiert. Es enthält Einstellungen, die auf alle neuen Benutzer angewendet werden. Sie können das Standardbenutzerprofil für ihre Benutzer bearbeiten, um die Anzahl von Änderungen zu minimieren, die Sie an einzelnen Benutzerprofilen vornehmen müssen.

Nachdem Sie das Standardbenutzerprofil geändert haben, wird es nur auf Benutzer angewendet, die sich zum ersten Mal bei der IBM Cognos-Software anmelden. Die Änderung wirkt sich nicht auf die vorhandenen Benutzerprofile von anderen Benutzern aus.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Anpassung** und wählen Sie dann die Registerkarte **Profile** aus.
2. Aktualisieren Sie alle Einstellungen im Abschnitt **Regionale Optionen**, die Sie ändern möchten.
3. 11.1.5 Zum Ändern der Standardposition für hochgeladene Dateien klicken Sie auf neben **Standardposition für Upload**.

   Tipp: Hochgeladene Dateien werden standardmäßig in **Eigener Inhalt** gespeichert. Wenn das Hochladen aus einem bestimmten Ordner in **Teaminhalt** oder **Eigener Inhalt** heraus eingeleitet wurde, können die Dateien in diesem Ordner gespeichert werden.

   Wenn Sie eine neue gemeinsam genutzte Position in **Teaminhalt** für hochgeladene Dateien auf Rollen-, Tenant- oder globaler Ebene angeben, können Benutzer die hochgeladenen Dateien an dieser neuen Standardposition speichern.
4. Gehen Sie wie folgt vor, wenn Sie die Berechtigungen des Standardbenutzerprofils ändern möchten:
   a) Klicken Sie auf **Berechtigungen** > **Bearbeiten**.
   b) Klicken Sie auf oder , um Benutzer, Gruppen oder Rollen zum Standardbenutzerprofil hinzuzufügen oder daraus zu entfernen.
   c) Klicken Sie auf für einen Benutzer, eine Gruppe oder eine Rolle und wählen Sie dann nach Bedarf **Lesen**, **Ausführen**, **Schreiben** oder **Vollständig** aus.
5. Klicken Sie auf **Anwenden**.

Ergebnisse

Jeder Benutzer, der sich zum ersten Mal bei IBM Cognos-Software anmeldet, übernimmt diese Einstellungen automatisch, kann sie jedoch später ändern.

Anzeigen oder Ändern von Benutzerprofilen

Sie können ein Benutzerprofil anzeigen oder ändern.

Informationen zu diesem Vorgang

Sie können bestimmte Elemente im Profil des Benutzers löschen. Dies kann in den folgenden Situationen nützlich sein:

- Der Inhalt des Benutzers belegt so viel Speicherplatz, dass die Leistung beeinträchtigt ist. Sie sollten den gesamten Inhalt oder Teile davon löschen.
- Sie sollten ein Benutzerprofil anzeigen, bevor Sie es löschen, um sicherzustellen, dass Sie nichts Wichtiges löschen.

Wenn ein Benutzer in Ihrem Authentifizierungsprovider gelöscht wurde, wird er nicht mehr in der IBM Cognos-Software angezeigt und Sie können das Benutzerprofil nicht mehr ändern.

Sie können nur die Profile von Benutzern sehen, die sich mindestens einmal angemeldet haben. Wenn sich Benutzer anmelden, wird in der Spalte **Geändert** ein Datum angezeigt.

Um ein Benutzerprofil anzuzeigen, Inhalt zu löschen oder zu ändern, müssen Sie über Transitberechtigungen für das Benutzerkonto und für alle Ordner mit Inhalten verfügen, deren Eigentümer der Benutzer ist. Sie müssen über Schreibberechtigungen für den Eintrag, den Sie löschen möchten, und sein übergeordnetes Element verfügen.

Sie können das Benutzerprofil für einzelne Benutzer ändern, aber nicht für Gruppen oder Rollen.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Personen** und wählen Sie dann **Konten** aus.
2. Klicken Sie auf den Namespace, der den Benutzer enthält.
3. Klicken Sie auf den Namen des Benutzers, dessen Vorgaben angezeigt oder geändert werden sollen.
4. Klicken Sie auf die Registerkarten **Allgemein**, **Persönlich** oder **Berechtigungen**, um die Einstellungen anzuzeigen oder zu ändern.
5. Klicken Sie außerhalb des Slideout-Fensters, um es zu schließen.

   Das Slideout-Fenster wird geschlossen. Wenn Sie Änderungen vorgenommen haben, wird die Nachricht ***benutzername* wurde bearbeitet.** angezeigt.

Löschen von Benutzerprofilen

Sie können Benutzerprofile aus dem Content Store löschen.

Wenn Sie einen Benutzer in Ihrem Authentifizierungsprovider löschen, sollten Sie zuerst das Benutzerprofil aus dem Content Store löschen, damit es nicht länger Speicherplatz belegt.

Sie sollten das Benutzerprofil aus der IBM Cognos-Software löschen, bevor Sie den Benutzer im zugeordneten Namespace löschen. Nachdem Sie den Benutzer gelöscht haben, werden die Benutzerinformationen nicht länger in der IBM Cognos-Software angezeigt und Sie können das Benutzerprofil nicht mehr in IBM Cognos Analytics verwalten.

Wenn das Benutzerkonto bereits aus dem zugeordneten Namespace gelöscht wurde, können Sie die Content Store-Verwaltung verwenden, um alle zugeordneten Benutzerkontoinformationen in der IBM Cognos-Software zu finden und optional daraus zu entfernen.

Wenn sich ein Benutzer mit einem gelöschten Benutzerprofil anmeldet, wird ein Konto mit Standardwerten erstellt. Wenn ein Benutzer angemeldet ist, während das zugehörige Benutzerprofil gelöscht wird, läuft der Passport des Benutzers ab und die Anmeldeseite wird geöffnet.

Bevor Sie ein Benutzerprofil löschen, sollten Sie dessen Inhalt 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 Onjekt verfügen.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Personen** und wählen Sie dann **Konten** aus.
2. Klicken Sie auf den Namespace, der den Benutzer enthält.
3. Suchen Sie nach dem Benutzer, dessen Benutzerprofil Sie löschen möchten. Sie können die Suchfunktion verwenden, um einen Benutzer zu finden. Weitere Informationen finden Sie unter „Suchen von Benutzern, Gruppen und Rollen” auf Seite 18.
4. Klicken Sie auf das Symbol 'Mehr' ··· neben dem Benutzernamen und wählen Sie dann  **Profil löschen** aus.
5. Klicken Sie auf **OK**, um zu bestätigen, dass das Benutzerprofil gelöscht werden soll.

Ergebnisse

Wenn sich der Benutzer das nächste Mal anmeldet, wird ihm das aktuelle Standardbenutzerprofil zugeordnet. Er kann das Profil später ändern, wenn er möchte.

Kopieren von Benutzerprofilen

Unter Umständen möchten Sie ein Benutzerprofil kopieren.

Das Kopieren von Benutzerprofilen kann in den folgenden Situationen nützlich sein:

- Ein Benutzer ändert seinen Namen und Sie richten ein Konto unter dem neuen Namen ein.
- Ein Benutzer zieht in einen anderen Namespace um oder Ihre Organisation ändert Namespaces und Sie müssen neue Konten einrichten.
- Sie erstellen viele neue ähnliche Benutzerkonten.

Wenn Sie beabsichtigen, den Quellenbenutzer in Ihrem Authentifizierungsprovider zu löschen, kopieren Sie vorher die Benutzerkontoinformationen. Nachdem Sie den Benutzer gelöscht haben, wird er nicht mehr in der IBM Cognos-Software angezeigt, und Sie können seine Kontoinformationen nicht mehr kopieren.

Sie können nur mit Profilen von Benutzern arbeiten, die sich mindestens einmal angemeldet haben. Wenn sich Benutzer anmelden, wird in der Spalte **Geändert** ein Datum angezeigt und der Benutzername ändert sich in einen Link.

Vorbereitende Schritte

Um Benutzerprofile zu kopieren, müssen Sie über Schreibberechtigungen für die Namespaces sowohl der Quellen- als auch der Zielbenutzer verfügen.

Tipp: Wenn Sie ein Benutzerprofil kopieren, werden keine vertrauenswürdigen Berechtigungsnachweise kopiert.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Personen** und wählen Sie dann **Konten** aus.
2. Klicken Sie auf den Namespace, der den Benutzer enthält.
3. Suchen Sie nach dem Quellenbenutzer, dessen Benutzerprofil Sie kopieren möchten. Sie können die Suchfunktion verwenden, um einen Benutzer zu finden. Weitere Informationen finden Sie unter „Suchen von Benutzern, Gruppen und Rollen” auf Seite 18.
4. Klicken Sie auf das Symbol 'Mehr'  neben dem Benutzernamen und wählen Sie dann  **Benutzerprofil kopieren** aus.
5. Wählen Sie die Einstellungen aus, die Sie kopieren möchten:
   - Regionale Einstellungen und Anzeigeoptionen
   - Der gesamte Inhalt des Benutzerordners **Eigener Inhalt**
   - Alle Portalseiten, die der Benutzer unter Umständen von einer alten Version von Cognos Business Intelligence migriert hat.

     Tipp: Informationen zur Aktivierung von eigenen Portalseiten finden Sie unter „Konfigurieren der Darstellung” auf Seite 81.
6. Geben Sie an, ob das Benutzerprofil des Quellenbenutzers gelöscht werden soll, nachdem Sie es zu anderen Benutzern kopiert haben.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie einen oder mehrere Zielbenutzer aus, die das kopierte Benutzerprofil erhalten sollen, und klicken Sie dann auf **Hinzufügen**.

Tipp: Um mehrere Benutzer auszuwählen, halten Sie die Steuertaste gedrückt, während Sie auf die einzelnen Benutzernamen klicken.

9. Ändern Sie bei Bedarf auf der Seite **Zusammenfassung** alle Einstellungen, einschließlich der Quellen- und Zielbenutzer.
10. Klicken Sie auf **Anwenden**.

Festlegen globaler Parameter

Administratoren können globale Parameter definieren, die in allen Berichten von allen Rollen verwendet werden können.

Anmerkung: Über das Slideout-Fenster **Verwalten** > **Konten** können Sie auch Standardberichtsparameter für bestimmte Rollen festlegen. Wenn ein Benutzer über eine Rolle mit benutzerdefinierten Parametern verfügt und mit diesen Parametern einen Bericht ausführt, werden ihm die von Ihnen festgelegten Standardwerte angezeigt. Weitere Informationen finden Sie unter „Anpassen von Rollen" auf Seite 7.

Vorgehensweise

1. Rufen Sie **Verwalten** > **Anpassung** auf und wählen Sie die Registerkarte **Parameter** aus.
2. Führen Sie abhängig von der Version von Cognos Analytics einen der folgenden Schritte aus:
   - In Version 11.1.4 und höher klicken Sie auf den Link **Neu** und geben den Parameternamen in den bereitgestellten Bereich ein. Drücken Sie die **Eingabetaste** auf der Tastatur.
   - In Version 11.1.3 und früher klicken Sie auf den Link **Importieren** und importieren den Parameter aus Ihrem Bericht, der sich entweder in **Eigener Inhalt** oder **Teaminhalt** befindet.
3. Klicken Sie im Parameterkontextmenü  auf die Option **Eigenschaften**.
4. Geben Sie eine angepasste Bezeichnung für den Parameter an. Zum Angeben einer sprachspezifischen Bezeichnung klicken Sie auf die Schaltfläche **Festlegen** neben **Sprachen**. Sie können auch eine Beschreibung des Parameters hinzufügen oder ihn inaktivieren.
5. 11.1.4 Aktivieren Sie das Kontrollkästchen **Für alle Rollen angewendet**.

   Wenn Sie diese Eigenschaft auswählen, können alle System- und Tenantbenutzerrollen diesen Parameter verwenden.

   Tipp: Wenn Sie ein lokaler Cognos Analytics-Benutzer sind und diesen Parameter für bestimmte Rollen anpassen wollen, wählen Sie das Kontrollkästchen **Für alle Rollen angewendet** nicht aus. Fahren Sie stattdessen mit Schritt 6 fort.
6. Passen Sie den Parameter für bestimmte Rollen wie folgt an:
   a) Wählen Sie unter **Verwalten** > **Personen** die Registerkarte **Konten** aus.
   b) Lokalisieren Sie die Rolle, für die Sie diesen Parameter anpassen möchten, und wählen Sie in der Anzeige **Eigenschaften** der Rolle die Registerkarte **Anpassung** aus.
   c) Klicken Sie neben **Parameter** auf **Einstellungen**.
   d) Wählen Sie das Kontrollkästchen neben dem Parameter aus, den Sie in Schritt 2 angegeben haben.

      Klicken Sie auf **OK**, um das Festlegen dieses Parameters abzuschließen, ohne den Standardwert zu ändern. Wenn Sie einen bestimmten Wert festlegen wollen, wählen Sie den Link **Werte festlegen** aus, ändern den Wert und klicken auf **Anwenden**.
   e) Wiederholen Sie bei Bedarf die Schritte b bis d für weitere Rollen. Die von Ihnen ausgewählten Parameterwerte können für verschiedene Rollen unterschiedlich sein.
7. Melden Sie sich ab und wieder an.

Ergebnisse

Berichtsersteller können im Fenster **Eigene Parameter**  Berichte entsprechend ihrer Rolle anpassen und berichtsübergreifende Konsistenz gewährleisten.

Globalen Parameter _as_of_date festlegen

Sie können den globalen Parameter **_as_of_date** konfigurieren und für alle System- und Tenantrollen verfügbar machen. Die lokalen Administratoren können diesen Parameter für bestimmte Benutzerrollen anpassen.

Vorgehensweise

1. Wechseln Sie zu **Verwalten** > **Anpassung** und wählen Sie die Registerkarte **Parameter** aus.
2. Führen Sie je nach Version von Cognos Analytics einen der folgenden Schritte aus:
   - In Version 11.1.4 und höher: Klicken Sie auf den Link **Neu** und geben Sie **_as_of_date** in den bereitgestellten Bereich ein. Drücken Sie die **Eingabetaste** auf der Tastatur.
   - In Version 11.1.3 und früher: Klicken Sie auf den Link für **Importieren** und importieren Sie den Parameter **_as_of_date** aus dem Beispielbericht "Datumsauswahlfeld für globale Parameter". Dieser Bericht befindet sich in **Teaminhalt** > **Beispiele** > **Relative Datumsangaben** > **Tools**.
3. Klicken Sie im Kontextmenü des Parameters **_as_of_date** ⋯ auf **Eigenschaften**.
4. Geben Sie eine benutzerdefinierte Beschriftung für den Parameter an. Wenn Sie eine sprachspezifische Beschriftung angeben möchten, klicken Sie neben **Sprachen** auf **Festlegen**. Sie können auch eine Beschreibung des Parameters hinzufügen oder ihn inaktivieren.
5. 11.1.4 Wählen Sie das Kontrollkästchen **Für alle Rollen angewendet** aus.

   Wenn Sie diese Eigenschaft auswählen, können alle System -und Tenantbenutzerrollen diesen Parameter verwenden.

   Wenn Sie ein lokaler Cognos Analytics-Benutzer sind und diesen Parameter für bestimmte Rollen anpassen wollen, wählen Sie das Kontrollkästchen **Für alle Rollen angewendet** nicht aus. Fahren Sie stattdessen mit Schritt 6 fort.
6. Gehen Sie wie folgt vor, um den Parameter **as_of_date** für bestimmte Rollen anzupassen:
   a) Wählen Sie unter **Verwalten** > **Personen** die Registerkarte **Konten** aus.
   b) Suchen Sie die Rolle, für die Sie diesen Parameter anpassen wollen, und wählen Sie in der Anzeige **Eigenschaften** der betreffenden Rolle die Registerkarte **Anpassung** aus.
   c) Klicken Sie neben **Parameter** auf **Einstellungen**.
   d) Wählen Sie das Kontrollkästchen neben dem Parameter **_as_of_date** aus, den Sie in Schritt 2 angegeben haben.

      Klicken Sie auf **OK**, um die Konfiguration dieses Parameters fertigzustellen, ohne das Standarddatum zu ändern, bei dem es sich um das aktuelle Datum handelt. Wenn Sie ein bestimmtes Datum festlegen wollen, wählen Sie den Link **Werte festlegen** aus, wählen Sie das gewünschte Datum aus und klicken Sie dann auf **Anwenden**.
   e) Wiederholen Sie bei Bedarf die Schritte b bis d für andere Rollen. Das von Ihnen ausgewählte Datum kann für verschiedene Rollen unterschiedlich sein.
7. Melden Sie sich ab und melden Sie sich anschließend erneut an.

Ergebnisse

Alle Benutzer im System oder Tenants können jetzt das Dialogfenster **Eigene Parameter** anzeigen, und der Parameter **_as_of_date** steht den Benutzern zur Verfügung, wenn sie Berichte oder Dashboards ausführen, die die Filter und Kennzahlen für relative Datumsangaben enthalten. Die Benutzer können diesen Parameter ihren Anforderungen entsprechend anpassen. Weitere Informationen finden Sie im Thema "Anpassen des Referenzdatums" im Handbuch *Cognos Analytics Datenmodellierung*.

Kapitel 10. Verwalten des Cloud-Speichers

11.1.5 Sie können Cognos Analytics für die Verbindung zu einem Cloud-Speicherservice konfigurieren, der von einem anderen Anbieter angeboten wird. Cognos Analytics-Benutzer können ihre Berichte anschließend in der Cloud speichern.

Zur Verwaltung des Cloud-Speichers muss Ihnen die geschützte Funktion **Verbindungen verwalten** zugewiesen sein, die der Funktion 'In Cloud speichern' zugeordnet ist. Weitere Informationen finden Sie unter „In Cloud speichern" auf Seite 133.

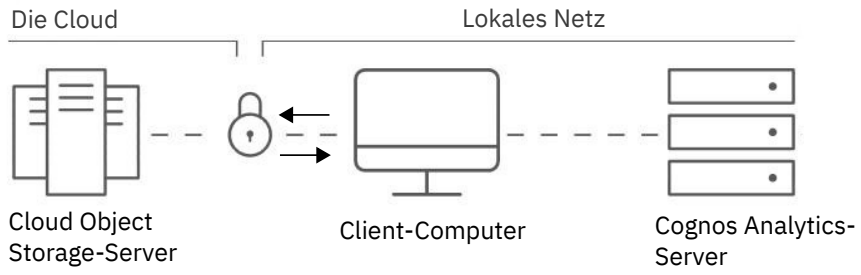
Cloud-Speicher auf einen Blick

Cloud-Speicher, der auch als Cloud-Objektspeicher (Cloud Object Storage - COS) bezeichnet wird, ist eine Technologie, die Unternehmen anderen Unternehmen oder Anwendungen als Service anbieten.

Erster Schritt: Sie als Administrator erstellen eine Instanz eines Speicherservice mit einem Cloud-Objektspeicherprovider.

Zweiter Schritt: Sie konfigurieren eine Speicherverbindung in Cognos Analytics, die in den Cloud-Objektspeicherservice integriert wird.

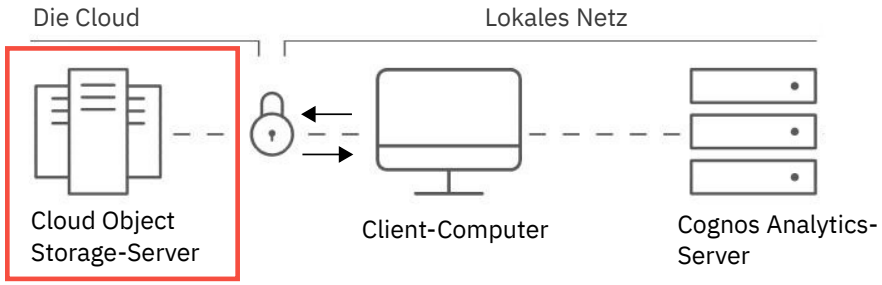
Die Integration von Cognos Analytics-Servern und eines Cloud-Objektspeicherservers ist im folgenden Diagramm dargestellt:



Erstellen einer Verbindung mit einem Cloud-Objektspeicherprovider

Erstellen Sie eine Verbindung mit einem Cloud-Objektspeicherprovider, um einen Speicherservice einzurichten, den Sie anschließend in Cognos Analytics integrieren können.

Dies ist die erste Phase bei der Einrichtung der Speicherung im Cloud-Feature von Cognos Analytics.



Wählen Sie ein Unternehmen als Cloud-Objektspeicherprovider aus:

- IBM
- Amazon
- MinIO

- Google

Erstellen einer IBM Speicherverbindung

Erstellen Sie eine Verbindung zu einem IBM Cloud Object Storage-Service (COS-Service), damit Cognos Analytics-Benutzer ihre Berichte in der Cloud speichern können.

Eine Übersicht über den IBM COS-Service finden Sie in den Informationen zu IBM Cloud Object Storage (https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-about-ibm-cloud-object-storage).

Schritt 1: IBM Cloud Platform-Konto erstellen

Erstellen Sie ein IBM Cloud Platform-Konto (https://cloud.ibm.com/docs/services/cloud-object-storage/basics?topic=cloud-object-storage-provision#provision-account).

Schritt 2: COS-Serviceinstanz erstellen

Erstellen Sie eine Serviceinstanz (https://cloud.ibm.com/docs/services/cloud-object-storage/basics?topic=cloud-object-storage-provision#provision-instance).

Tipps für Cognos Analytics-Administratoren:

- Zu Anfang hat eine COS-Serviceinstanz keine Serviceberechtigungsnachweise. Bevor Sie Cognos Analytics für die Verbindung zu Ihrem Cloud-Objektspeicherservice konfigurieren können, müssen Sie ihm einen Serviceberechtigungsnachweis zuweisen.

Schritt 3: Serviceberechtigungsnachweise erstellen

Erstellen Sie Ihre COS-Serviceberechtigungsnachweise (https://cloud.ibm.com/docs/services/cloud-object-storage?topic=cloud-object-storage-service-credentials).

Tipps für Cognos Analytics-Administratoren:

- Notieren Sie sich die Werte der COS-Eigenschaften, die in der folgenden Tabelle aufgeführt sind. Sie benötigen diese Werte später, wenn Sie Cognos Analytics konfigurieren, um eine Verbindung zu dieser IBM Cloud Object Storage-Verbindung herzustellen.

Tabelle 77. IBM COS-Zugriffsschlüssel und geheimer Zugriffsschlüssel

Eigenschaft in den IBM COS-Serviceberechtigungsnachweisen	**Zugehörige Eigenschaft bei der Konfiguration von Cognos Analytics**
`apikey`	**Zugriffsschlüssel-ID**
`resource_instance_id`	**Geheimer Zugriffsschlüssel**

Schritt 4: Bucket erstellen

Erstellen Sie einige Buckets zum Speichern Ihrer Daten (https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-getting-started#gs-create-buckets) .

Tipps für Cognos Analytics-Administratoren:

- Wählen Sie ein vordefiniertes Standardbucket aus.
- Wenn Sie ein Bucket erstellen, wählen Sie einen Resilienzwert (**Resiliency**) aus. Beispiel: `Regional`. Dann wählen Sie einen Positionswert (**Location**) aus. Beispiel: `eu-gb`.

  Wichtig:

  Notieren Sie den Wert für **Position**. Sie müssen denselben Wert später auswählen, wenn Sie Cognos Analytics konfigurieren, um Ihrer Verbindung eine Position hinzuzufügen.

Erstellen einer Amazon-Speicherverbindung

Erstellen Sie eine Verbindung zu einem Amazon Simple Storage Service (S3), damit Cognos Analytics-Benutzer ihre Berichte in der Cloud speichern können.

Eine Übersicht über Amazon Simple Storage Service (S3) finden Sie unter Amazon S3 Basics auf der Website von Amazon Web Services (AWS) (https://docs.aws.amazon.com/AmazonS3/latest/gsg/AmazonS3Basics.html).

Schritt 1: AWS-Konto erstellen

Erstellen Sie ein Amazon Web Services-Konto (AWS-Konto) auf der AWS-Website (https://portal.aws.amazon.com/billing/signup#/start).

Schritt 2: Amazon S3-Service erstellen

Erstellen Sie einen Amazon Simple Storage Service (S3) auf der AWS-Website (https://docs.aws.amazon.com/AmazonS3/latest/gsg/SigningUpforS3.html).

Schritt 3: Serviceberechtigungsnachweise erstellen

Erstellen Sie einen neuen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel (https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html#create-aws-access-key) als Teil Ihrer Serviceberechtigungsnachweise.

Tipps für Cognos Analytics-Administratoren:

- Auch wenn Sie bereits einen Zugriffsschlüssel haben, müssen Sie einen neuen Schlüssel erstellen, sodass Sie auch Ihren geheimen Zugriffsschlüssel erfassen können.
- Notieren Sie sich die Werte der AWS-Eigenschaften, die in der folgenden Tabelle aufgeführt sind. Sie benötigen diese Werte später, wenn Sie Cognos Analytics konfigurieren, um eine Verbindung zu dieser IBM Cloud Object Storage-Verbindung herzustellen.

Tabelle 78. AWS-Zugriffsschlüssel und geheimer Zugriffsschlüssel

Eigenschaft in der Managementkonsole von Amazon Web Services (AWS)	**Zugehörige Eigenschaft bei der Konfiguration von Cognos Analytics**
`AWSAccessKeyId`	**Zugriffsschlüssel-ID**
`AWSSecretKey`	**Geheimer Zugriffsschlüssel**

Schritt 4: Bucket erstellen

Erstellen Sie ein Bucket auf der AWS-Website (https://docs.aws.amazon.com/AmazonS3/latest/gsg/CreatingABucket.html).

Tipps für Cognos Analytics-Administratoren:

- Wählen Sie ein vordefiniertes Standardbucket aus.
- Wenn Sie ein Bucket erstellen, wählen Sie eine Region aus. Beispiel für Asien/Pazifik: `Asia Pacific (Tokyo)`.

  Wichtig:

  Notieren Sie die Region. Sie müssen denselben Wert später auswählen, wenn Sie Cognos Analytics konfigurieren, um Ihrer Verbindung eine Position hinzuzufügen.

Erstellen einer MinIO-Speicherverbindung

Erstellen Sie eine Verbindung zu einer MinIO-Speicherumgebung, damit Cognos Analytics-Benutzer ihre Berichte in der Cloud speichern können.

Eine Übersicht über den MinIO-Objektspeicherserver finden Sie unter MinIO (https://www.ibm.com/support/knowledgecenter/SSBS6K_3.1.2/manage_cluster/minio.html).

Schritt 1: MinIO installieren

Installieren Sie MinIO (https://docs.min.io/docs/minio-quickstart-guide).

Schritt 2: MinIO ausführen

Anmerkung: Ausführliche Informationen finden Sie in der Veröffentlichung MinIO Quickstart Guide (https://docs.min.io/docs/minio-quickstart-guide.html).

Beispiel für das Abrufen von MinIO-Parametern

In diesem Beispiel wird MinIO unter Windows installiert. Notieren Sie die Werte, die für die Konfiguration von Cognos Analytics erforderlich sind:

1. Installieren Sie den MinIO-Server auf einem Windows-Computer.
2. Erstellen Sie einen Ordner `C:\my_data_folder`.
3. Wechseln Sie in einem Befehlszeilenfenster in das Verzeichnis, in dem Sie den MinIO-Server installiert haben.
4. Geben Sie den folgenden Befehl ein: `minio.exe server C:\my_data_folder`.

   Eine Liste der Parameter für Ihre MinIO-Instanz wird im Befehlsfenster angezeigt.
5. Notieren Sie sich für die Konfiguration von Cognos Analytics die folgenden Parameter:
   - Zugriffsschlüssel (`Access key`)
   - Geheimer Zugriffsschlüssel (`Secret access key`)
   - Endpunkt (`Endpoint`)

   Tipp: Sie verwenden diese Werte zum Erstellen einer MinIO-Speicherverbindung in Cognos Analytics.

Schritt 3: Bucket erstellen

Beispiel

1. Geben Sie die MinIO-Endpunkt-URL, die Sie zuvor notiert haben, in einem Browserfenster ein.

   Das MinIO-Browserfenster wird angezeigt.
2. Geben Sie den Zugriffsschlüssel und den geheimen Zugriffsschlüssel ein, die Sie zuvor notiert haben.
3. Befolgen Sie die Anweisungen zum Erstellen eines Buckets.

Google Cloud Platform-Speicherverbindung erstellen

Erstellen Sie eine Verbindung zu einer GCP-Speicherverbindung (GCP, Google Cloud Platform), damit Cognos Analytics-Benutzer ihre Berichte in der Cloud speichern können.

Weitere Informationen zu GCP-Speicherverbindungen finden Sie unter Cloud Storage Overview (https://cloud.google.com/storage/docs).

Schritt 1: Google Cloud Platform-Konto erstellen

1. Rufen Sie die Seite Google Cloud Platform (https://console.cloud.google.com) auf.
2. Befolgen Sie die Anweisungen, um ein GCP-Konto zu erstellen.

Schritt 2: Projekt erstellen

1. Rufen Sie die Projektauswahlseite (https://console.cloud.google.com/projectselector2) auf.
2. Klicken Sie auf **PROJEKT ERSTELLEN**.

3. Geben Sie einen Projektnamen ein und klicken Sie anschließend auf **ERSTELLEN**.

Schritt 3: Speicher-Service-Account erstellen

1. Wählen Sie im Navigationsmenü die Option **Speicher** aus, um auf Ihre Speicherbrowserseite (https: // console.cloud.google.com/storage/browser) zu wechseln.
2. . Klicken Sie auf **Rechnungsstellung aktivieren**, wenn Sie die Rechnungsstellung noch nicht aktiviert haben.
3. Klicken Sie auf **SERVICEKONTO ERSTELLEN**.
   a. Geben Sie einen Servicekontonamen und eine Beschreibung ein.

      Anmerkung: Das Feld **Service-Account-ID** wird automatisch gefüllt.
   b. Klicken Sie auf **ERSTELLEN**.
   c. Erteilen Sie dem Service-Account Zugriff auf Ihr Projekt.
   d. Erteilen Sie Benutzern Zugriff auf das Service-Konto.
   e. Klicken Sie auf **FERTIG**.

Schritt 4: Serviceberechtigungsnachweise erstellen

Weitere Informationen finden Sie unter Service-Account-Schlüssel erstellen und verwalten (https: // cloud.google.com/iam/docs/creating-management-service-account-keys).

1. Wechseln Sie in der Cloudkonsole auf die Seite für Service-Accounts (https://console.cloud.google.com/projectselector2/iam-admin/serviceaccounts).
2. Klicken Sie auf **Projekt auswählen**, wählen Sie ein Projekt aus und klicken Sie auf **Öffnen**.
3. Suchen Sie die Zeile des Service-Accounts, für den Sie einen Schlüssel erstellen möchten. Klicken Sie in dieser Zeile auf die Schaltfläche **Mehr**, und klicken Sie anschließend auf **Schlüssel erstellen**.
4. Wählen Sie einen **Schlüsseltyp** aus und klicken Sie auf **Erstellen**.

   Anmerkung:

   Wenn Sie auf **Erstellen** klicken, wird eine Servicekontoschlüsseldatei heruntergeladen. Nachdem Sie die Schlüsseldatei heruntergeladen haben, können Sie sie nicht erneut herunterladen.

   Stellen Sie sicher, dass Sie die Schlüsseldatei sicher speichern, da sie für die Authentifizierung als Ihr Service-Account verwendet werden kann. Sie können diese Datei verschieben und umbenennen, wie Sie möchten.
5. Öffnen Sie die Schlüsseldatei, die Sie heruntergeladen haben. Suchen Sie nach den beiden Zeilen, die mit "private_key_id" und "private_key" beginnen, wie folgt:

   ```
   "private_key_id": "key-id",
   "private_key": "----- BEGIN PRIVATE KEY ----- \nprivater Schlüssel\n ----- END PRIVATE KEY
   ----- \n",
   ```
6. Notieren Sie die Werte ***key-id*** und ***private-key*** , die in der vorhergehenden Tabelle hervorgehoben sind. Sie benötigen diese Werte später, wenn Sie Cognos Analytics konfigurieren, um eine Verbindung zu dieser IBM Cloud Object Storage-Verbindung herzustellen. In der folgenden Tabelle ist beschrieben, wie die Werte für ***key-id*** und ***private-key*** in Cognos Analytics verwendet werden müssen.

Tabelle 79. Service-Berechtigungsnachweise von GCP zu Cognos Analytics zuordnen

Eigenschaft in GCP-Service-Berechtigungsnachweisen	**Zugehörige Eigenschaft bei der Konfiguration von Cognos Analytics**
`key-id`	**Zugriffsschlüssel-ID**
`privater Schlüssel`	**Geheimer Zugriffsschlüssel**

Tabelle 79. Service-Berechtigungsnachweise von GCP zu Cognos Analytics zuordnen (Forts.)	
Eigenschaft in GCP-Service-Berechtigungsnachweisen	**Zugehörige Eigenschaft bei der Konfiguration von Cognos Analytics**
Roh-Endpunkt	**Serviceendpunkt** Geben Sie Folgendes ein: https://www.google-apis.com/service_accounts/v1/metadata/raw/***sa-name***@***projekt-id***.iam.gserviceaccount.com

Schritt 5: Bucket erstellen

Führen Sie die Schritte im Abschnitt Speicherbuckets erstellenaus.

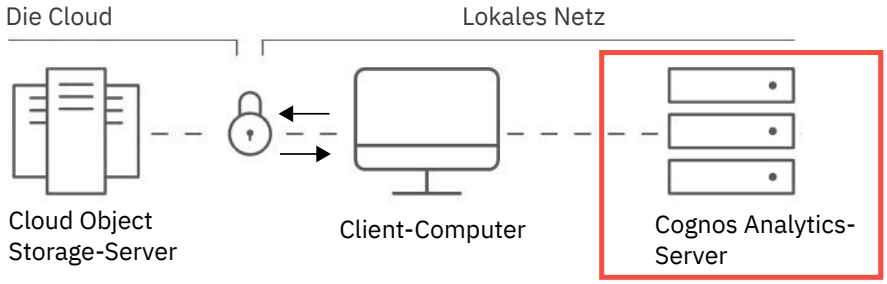
Tipps für Cognos Analytics-Administratoren:

- Wenn Sie aus der Liste **Position** auswählen, notieren Sie sich die Region. Sie müssen denselben Wert später auswählen, wenn Sie Cognos Analytics konfigurieren, um Ihrer Verbindung eine Position hinzuzufügen.
- Wählen Sie im Feld **Zugriffssteuerung** die Option **Uniform**aus, sodass alle Inhalte im Bucket die gleichen Berechtigungen haben.
- Wählen Sie im Feld **Erweiterte Einstellungen (optional)** > **Verschlüsselung** die Option **Google-verwalteter Schlüssel**aus und klicken Sie anschließend auf **CREATE**.

Erstellen einer Speicherverbindung in Cognos Analytics

Erstellen Sie eine Speicherverbindung in Cognos Analytics, um einen bestehenden Cloud-Speicherservice in Cognos Analytics zu integrieren.

Dies ist die zweite Phase der Konfiguration von Cognos Analytics für die Speicherung in der Cloud.



Vorbereitende Schritte

Sie müssen einen Speicherservice mit einem Cloud-Objektspeicherprovider einrichten, bevor Sie Cognos Analytics für die Verbindung mit diesem Service konfigurieren können.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Speicher**.

   Die Seite **Cloud-Speicher** wird angezeigt. Wenn Verbindungen vorhanden sind, werden sie in der **Verbindungsliste** angezeigt.

2. Klicken Sie auf das Symbol 'Verbindung erstellen' .
3. Geben Sie einen Namen für Ihre Verbindung ein.
4. Wählen Sie im Feld **Typ** den Cloud-Objektspeicherprovider aus, mit dem Sie eine Verbindung erstellt haben.
5. Geben Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel ein.

Tipp: Diese Werte wurden generiert, als Sie Ihre Berechtigungsnachweise in Ihrem Konto für den Cloud-Objektspeicher erstellt haben. Weitere Informationen finden Sie unter „Bestimmen der ID des Zugriffsschlüssels und der ID des geheimen Zugriffsschlüssels" auf Seite 249.

6. Wenn Sie die Option **Sonstige** im Feld **Typ** ausgewählt haben, geben Sie den MinIo-Serviceendpunkt ein.

   Tipp: Weitere Informationen finden Sie unter „Bestimmen des Serviceendpunkts (nur MinIO)" auf Seite 250

7. Klicken Sie auf **Testen**.

   - **Test erfolgreich** gibt an, dass die Verbindung ordnungsgemäß konfiguriert ist.
   - **Test fehlgeschlagen** gibt an, dass die Verbindung nicht ordnungsgemäß konfiguriert ist. Versuchen Sie diese Lösung.

8. Klicken Sie auf **Erstellen und fortsetzen**.

   Die Verbindung wird erstellt und der Assistent wechselt zur nächsten Seite **Position hinzufügen**.

Nächste Schritte

Im nächsten Schritt fügen Sie der soeben erstellten Verbindung eine Position hinzu.

Bestimmen der ID des Zugriffsschlüssels und der ID des geheimen Zugriffsschlüssels

Sie müssen die ID des Zugriffsschlüssels und die ID des geheimen Zugriffsschlüssels für Ihren Speicherprovider ermitteln, bevor Sie Cognos Analytics für die Verbindung mit dem Speicherservice konfigurieren können.

Wählen Sie die Vorgehensweise für Ihren Speicherobjektprovider aus:

- IBM
- Amazon
- MinIO

Vorgehensweise für IBM Cloud Object Storage

1. Wenn nicht bereits geschehen, erstellen Sie Ihre Serviceberechtigungsnachweise.
2. Führen Sie andernfalls die folgenden Schritte aus:
   a. Wechseln Sie zur IBM Cloud-Ressourcenliste.
   b. Erweitern Sie **Speicher** und klicken Sie auf die IBM COS-Serviceinstanz, die Sie erstellt haben.
   c. Klicken Sie auf **Serviceberechtigungsnachweise**.
   d. Erweitern Sie **Berechtigungsnachweise anzeigen** in der Zeile für einen vorhandenen Berechtigungsnachweis.
3. Notieren Sie sich die Werte der COS-Eigenschaften, die in der folgenden Tabelle aufgeführt sind. Sie benötigen diese Werte später, wenn Sie Cognos Analytics konfigurieren, um eine Verbindung zu dieser IBM Cloud Object Storage-Verbindung herzustellen.

Tabelle 80. IBM COS-Zugriffsschlüssel und geheimer Zugriffsschlüssel

Eigenschaft in den IBM COS-Serviceberechtigungsnachweisen	**Zugehörige Eigenschaft bei der Konfiguration von Cognos Analytics**
`apikey`	**Zugriffsschlüssel-ID**
`resource_instance_id`	**Geheimer Zugriffsschlüssel**

Vorgehensweise für Amazon Simple Storage Service

1. Erstellen Sie einen neuen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel (https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html#create-aws-access-key) als Teil Ihrer Serviceberechtigungsnachweise.

   Tipp: Wenn Sie zuvor einen Zugriffsschlüssel erstellt, jedoch den geheimen Zugriffsschlüssel nicht erfasst haben, müssen Sie einen neuen Zugriffsschlüssel erstellen und den neuen geheimen Zugriffsschlüssel erfassen.
2. Notieren Sie sich die Werte der AWS-Eigenschaften, die in der folgenden Tabelle aufgeführt sind. Sie benötigen diese Werte später, wenn Sie Cognos Analytics konfigurieren, um eine Verbindung zu dieser IBM Cloud Object Storage-Verbindung herzustellen.

Tabelle 81. AWS-Zugriffsschlüssel und geheimer Zugriffsschlüssel

Eigenschaft in der Managementkonsole von Amazon Web Services (AWS)	**Zugehörige Eigenschaft bei der Konfiguration von Cognos Analytics**
`AWSAccessKeyId`	**Zugriffsschlüssel-ID**
`AWSSecretKey`	**Geheimer Zugriffsschlüssel**

Vorgehensweise für MinIO

In diesem Beispiel wird MinIO unter Windows installiert. Notieren Sie die Werte, die für die Konfiguration von Cognos Analytics erforderlich sind:

1. Installieren Sie den MinIO-Server auf einem Windows-Computer.
2. Erstellen Sie einen Ordner `C:\my_data_folder`.
3. Wechseln Sie in einem Befehlszeilenfenster in das Verzeichnis, in dem Sie den MinIO-Server installiert haben.
4. Geben Sie den folgenden Befehl ein: `minio.exe server C:\my_data_folder`.

   Eine Liste der Parameter für Ihre MinIO-Instanz wird im Befehlsfenster angezeigt.
5. Notieren Sie sich für die Konfiguration von Cognos Analytics die folgenden Parameter:
   - Zugriffsschlüssel (`Access key`)
   - Geheimer Zugriffsschlüssel (`Secret access key`)
   - Endpunkt (`Endpoint`)

Bestimmen des Serviceendpunkts (nur MinIO)

Der Serviceendpunkt ist eine URL, die erforderlich ist, wenn Sie Cognos Analytics für die Verbindung zu einer MinIO-Speicherumgebung konfigurieren.

Im folgenden Beispiel wird MinIO unter Windows installiert. Notieren Sie den Endpunktwert.

Vorgehensweise

1. Installieren Sie den MinIO-Server auf einem Windows-Computer.
2. Erstellen Sie einen Ordner `C:\my_data_folder`.
3. Wechseln Sie in einem Befehlszeilenfenster in das Verzeichnis, in dem Sie den MinIO-Server installiert haben.
4. Geben Sie den folgenden Befehl ein: `minio.exe server C:\my_data_folder`.

   Eine Liste der Parameter für Ihre MinIO-Instanz wird im Befehlsfenster angezeigt.
5. Notieren Sie den Wert für den Endpunkt (`Endpoint`).

Nächste Schritte

Sie geben den Endpunktwert in das Feld **Serviceendpunkt** ein, wenn Sie eine MinIO-Verbindung in Cognos Analytics erstellen.

Verwalten der Verbindungsliste

Zeigen Sie nach der Erstellung einer oder mehrerer Verbindungen die Verbindungsliste an, um die Eigenschaften und den Status der einzelnen Verbindungen zu prüfen.

Vorbereitende Schritte

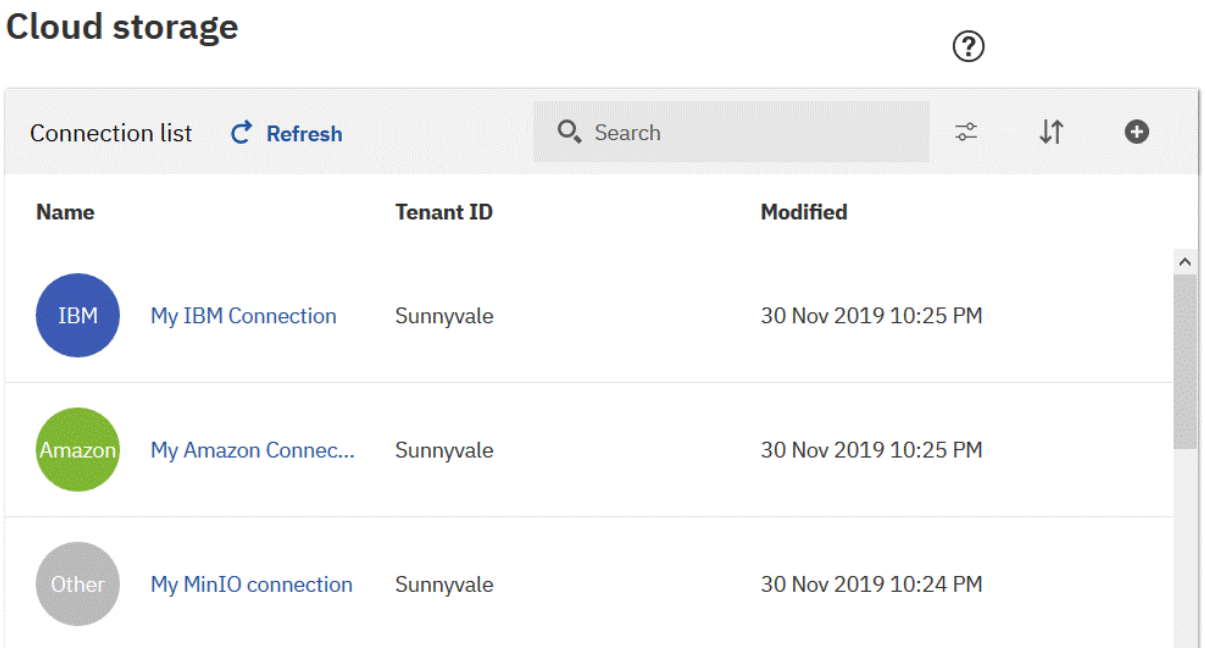
Sie müssen mindestens eine Verbindung erstellt haben.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Speicher**.

   Die **Verbindungsliste** wird angezeigt.

   Die folgende Abbildung zeigt ein Beispiel:



   Wichtig: Sie müssen möglicherweise den Cache Ihres Browsers leeren, falls die Anzeige des Datums und der Uhrzeit für **Geändert** nicht richtig aktualisiert wird, wenn Sie auf **Aktualisieren** klicken.

   Öffnen Sie in Firefox ein privates Fenster. Öffnen Sie in Chrome ein Incognito-Fenster.

2. Klicken Sie am Ende der Zeile für Ihre Verbindung auf das Symbol mit den Auslassungspunkten und anschließend auf **Eigenschaften**.

   Es wird eine Anzeige für die Verbindung mit der Registerkarte **Allgemein** geöffnet.

   - Wenn Sie den Verbindungsnamen in der Liste abblenden und die Verbindung vorübergehend nicht verfügbar machen wollen, klicken Sie auf **Erweitert** und wählen dann das Kontrollkästchen **Diesen Eintrag inaktivieren** aus.

     Tipp: Die Verbindung zwischen dem Cognos Analytics-Server und dem Cloud-Speicherservice wird unterbrochen. Wenn Sie das Kontrollkästchen abwählen, können Benutzer die Verbindung wieder verwenden.

- Wenn Sie den Namen Ihrer Verbindung ändern wollen, klicken Sie auf das Symbol 'Bearbeiten' oben auf der Anzeige. Geben Sie dann einen neuen Namen ein.

3. Klicken Sie auf die Registerkarte **Verbindung**.
   - Zum Ändern der Felder **Zugriffsschlüssel-ID** und **Geheimer Zugriffsschlüssel** aktualisieren Sie zunächst die Sicherheitsberechtigungsnachweise für Ihren Cloud-Speicherservice. Bestimmen Sie anschließend die Schlüsselwerte, die Sie eingeben müssen.

     Wichtig: Nur für MinIO-Speicherumgebungen müssen Sie außerdem das Feld für den Serviceendpunkt in Ihrer MinIO-Cloud-Speicherumgebung aktualisieren. Weitere Informationen finden Sie unter „Bestimmen des Serviceendpunkts (nur MinIO)" auf Seite 250.

   - Klicken Sie auf **Testen** und anschließend auf **Speichern**, um sicherzustellen, dass alle von Ihnen vorgenommenen Änderungen die Betriebsbereitschaft der Verbindung aufrechterhalten.
4. Wenn Sie die Verbindung aus der Liste entfernen wollen, klicken Sie auf das Symbol mit den Auslassungspunkten am Ende der Zeile. Klicken Sie anschließend auf **Löschen**.

   Anmerkung: Auf den Speicherservice, den Sie in der Cloud-Speicherumgebung erstellt haben, hat das Entfernen der Cognos Analytics-Speicherverbindung keine Auswirkungen.

Hinzufügen einer Position zu einer Verbindung

Sie können Ihrer Verbindung eine Position hinzufügen, die als Container für Berichte genutzt wird, die in der Cloud gespeichert werden. Die Position in Cognos Analytics wird einem Bucket zugeordnet, das Sie in Ihrer Cloud-Objektspeicherumgebung erstellt haben.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Speicher**.

   Die Seite **Cloud-Speicher** wird angezeigt.
2. Klicken Sie auf die Verbindung, der Sie eine Position hinzufügen wollen.

   Die Seite **Positionsliste** wird angezeigt.

   Tipp: Falls die Nachricht Fehler beim Zugriff auf die Cloud-Speicherverbindung '*verbindungsname*' angezeigt wird, versuchen Sie diese Lösung.
3. Klicken Sie auf das Symbol 'Position erstellen' oder klicken Sie auf **Position hinzufügen**, falls noch keine Positionen vorhanden sind.

   Die Seite **Position hinzufügen** wird angezeigt.
4. Geben Sie einen Namen für Ihre Position ein.
5. Wählen Sie im Feld **Bucket auswählen** ein Bucket aus, das Sie mithilfe Ihres Cloud-Objektspeicherservice erstellt haben.
6. Wenn gewünscht, geben Sie ein Schlüsselpräfix ein.

   Tipp: Das optionale Feld **Schlüsselpräfix** hat in etwa die Funktion eines Ordners in Ihrer Cloud-Objektspeicherumgebung. Wenn Sie keinen Schlüsselpräfixwert eingeben, werden Ihre Objekte im Stammordner Ihres Buckets gespeichert.

   - **Wenn Sie ein Schlüsselpräfix für ein Amazon S3-Bucket eingeben und ein Benutzer einen Bericht in diesem Bucket speichert, gilt Folgendes:**
     - Der Bericht wird in einen Ordner im Bucket in der Amazon S3-Umgebung kopiert.
     - Der Ordnername stimmt mit dem Wert des Schlüsselpräfix überein.
     - **Beispiel**

Ein Cognos Analytics-Benutzer speichert den Bericht `Product line revenue` (Produktreihe - Einnahmen) in der Cloud und wählt einen AWS-Service (AWS - Amazon Web Services) und ein Bucket aus, dem der Präfixwert `Revenue` (Einnahmen) zugeordnet wurde. Der Benutzer wählt die Formate **PDF** und **Excel** sowie als Sprache **Englisch (Neuseeland)** aus.

Ergebnis

Die Berichtsausgabedateien `Product line revenue-en-nz.xlsx` und `Product line revenue-en-nz.pdf` werden in der Amazon-Managementkonsole an der Position ***aws-servicename*/*aws-bucketname*/Revenue** angezeigt.

- **Wenn Sie ein Schlüsselpräfix für ein IBM COS-Bucket eingeben und ein Benutzer einen Bericht in diesem Bucket speichert, gilt Folgendes:**
  - **Anmerkung:** Es wird **kein** Ordner im Bucket in der IBM COS-Konsole erstellt. Stattdessen wird der Bericht in der Liste der Bucketobjekte angezeigt, wobei *`schlüsselpräfixwert/`* dem Berichtsnamen vorangestellt wird.
  - **Beispiel**

    Ein Cognos Analytics-Benutzer speichert den Bericht `Product line revenue` (Produktreihe - Einnahmen) in der Cloud und wählt einen IBM COS-Service und ein Bucket aus, dem der Präfixwert `Revenue` (Einnahmen) zugeordnet wurde. Der Benutzer wählt die Formate **PDF** und **Excel** sowie als Sprache **Englisch (Neuseeland)** aus.

    Ergebnis

    Die Berichtsausgabedateien `Revenue/Product line revenue-en-nz.xlsx` und `Revenue/Product line revenue-en-nz.pdf` werden in der IBM COS-Konsole an der Position ***ibm_cos-servicename/ibm_cos-bucketname*** angezeigt.
- **Wenn Sie ein Schlüsselpräfix für ein MinIO-Bucket eingeben und ein Benutzer einen Bericht in diesem Bucket speichert, gilt Folgendes:**
  - Der Bericht wird in einen Ordner im Bucket im MinIO-Browser kopiert.
  - Der Ordnername stimmt mit dem Wert des Schlüsselpräfix überein.

7. Wählen Sie die Region aus.

   Wichtig: Sie müssen dieselbe Region auswählen, die auch beim Erstellen Ihres Buckets in Ihrer Cloud-Objektspeicherumgebung verwendet wurde. Weitere Informationen finden Sie unter „Bestimmen der Region für das Cognos Analytics-Bucket" auf Seite 253.

8. Klicken Sie auf **Testen**.

   - **Test erfolgreich** gibt an, dass die Position ordnungsgemäß konfiguriert ist.
   - **Test fehlgeschlagen** gibt an, dass die Position nicht ordnungsgemäß konfiguriert ist. Versuchen Sie diese Lösung.

Nächste Schritte

Nach dem erfolgreichen Hinzufügen einer Position können Cognos Analytics-Benutzer ihre Berichtsausgaben an dieser Cloud-Position speichern. Weitere Informationen finden Sie unter „Speichern von Ausgaben in der Cloud" auf Seite 256.

Bestimmen der Region für das Cognos Analytics-Bucket

Für AWS- oder IBM Speichertypen müssen Sie sicherstellen, dass die Region, die Sie an Ihrer Cognos Analytics-Position auswählen, der Region bzw. Position entspricht, die Sie bei der Erstellung eines Buckets in Ihrer Cloud-Speicherumgebung ausgewählt haben.

Wählen Sie die Vorgehensweise für Ihren Speicherobjektprovider aus:

- IBM
- Amazon

Anmerkung: Die MinIO-Speicherkonfiguration enthält keinen Wert für Region.

Schritte für IBM Cloud Object Storage

1. Wechseln Sie zu Ihrer IBM Cloud-Ressourcenliste (https://cloud.ibm.com/resources).
2. Erweitern Sie **Speicher** und klicken Sie auf Ihren Cloud Object Storage-Service (COS-Service).

   Es wird eine Liste der Buckets für Ihren COS-Service angezeigt.
3. Suchen Sie in der Zeile für das gewünschte Bucket den Wert in der Spalte **Position** heraus.
4. Notieren Sie den Wert für **Position**.

   Tipp: Sie geben diesen Wert später in das Feld **Region** ein, wenn Sie eine IBM Position in Cognos Analytics hinzufügen.

Schritte für Amazon Simple Storage Service

1. Wechseln Sie zu Ihrer Liste der S3-Buckets in der AWS-Managementkonsole (https://s3.console.aws.amazon.com/s3/home).
2. Suchen Sie in der Zeile für das gewünschte Bucket den Wert in der Spalte **Region** heraus.
3. Notieren Sie den Wert für **Region**.

   Tipp: Sie geben diesen Wert später in das Feld **Region** ein, wenn Sie eine Amazon-Position in Cognos Analytics hinzufügen.

Verwenden eines Schlüsselpräfix

Wenn Sie dies wollen, können Sie ein Schlüsselpräfix angeben, wenn Sie ein Bucket in Cognos Analytics konfigurieren. Wenn Sie planen, eine hohe Anzahl von Berichten in der Cloud zu speichern, bietet ein Schlüsselpräfix eine Möglichkeit, viele Berichtsobjekte unter verschiedene Kategorien zu sortieren.

Ein Schlüsselpräfix kann je nach verwendeter Speicherlösung zu verschiedenen Dateistrukturen für gespeicherte Berichtsausgaben führen:

- **Wenn Sie ein Schlüsselpräfix für ein Amazon S3-Bucket eingeben und ein Benutzer einen Bericht in diesem Bucket speichert, gilt Folgendes:**
  - Der Bericht wird in einen Ordner im Bucket in der Amazon S3-Umgebung kopiert.
  - Der Ordnername stimmt mit dem Wert des Schlüsselpräfix überein.
  - **Beispiel**

    Ein Cognos Analytics-Benutzer speichert den Bericht `Product line revenue` (Produktreihe - Einnahmen) in der Cloud und wählt einen AWS-Service (AWS - Amazon Web Services) und ein Bucket aus, dem der Präfixwert `Revenue` (Einnahmen) zugeordnet wurde. Der Benutzer wählt die Formate **PDF** und **Excel** sowie als Sprache **Englisch (Neuseeland)** aus.

    Ergebnis

    Die Berichtsausgabedateien `Product line revenue-en-nz.xlsx` und `Product line revenue-en-nz.pdf` werden in der Amazon-Managementkonsole an der Position ***aws-servicename*/*aws-bucketname*/Revenue** angezeigt.
- **Wenn Sie ein Schlüsselpräfix für ein IBM COS-Bucket eingeben und ein Benutzer einen Bericht in diesem Bucket speichert, gilt Folgendes:**
  - **Anmerkung:** Es wird **kein** Ordner im Bucket in der IBM COS-Konsole erstellt. Stattdessen wird der Bericht in der Liste der Bucketobjekte angezeigt, wobei *`schlüsselpräfixwert/`* dem Berichtsnamen vorangestellt wird.
  - **Beispiel**

    Ein Cognos Analytics-Benutzer speichert den Bericht `Product line revenue` (Produktreihe - Einnahmen) in der Cloud und wählt einen IBM COS-Service und ein Bucket aus, dem der Präfixwert

Revenue (Einnahmen) zugeordnet wurde. Der Benutzer wählt die Formate **PDF** und **Excel** sowie als Sprache **Englisch (Neuseeland)** aus.

Ergebnis

Die Berichtsausgabedateien `Revenue/Product line revenue-en-nz.xlsx` und `Revenue/Product line revenue-en-nz.pdf` werden in der IBM COS-Konsole an der Position ***ibm_cos-servicename/ibm_cos-bucketname*** angezeigt.

- **Wenn Sie ein Schlüsselpräfix für ein MinIO-Bucket eingeben und ein Benutzer einen Bericht in diesem Bucket speichert, gilt Folgendes:**
  - Der Bericht wird in einen Ordner im Bucket im MinIO-Browser kopiert.
  - Der Ordnername stimmt mit dem Wert des Schlüsselpräfix überein.

Verwalten der Positionsliste

Zeigen Sie nach der Erstellung einer oder mehrerer Positionen die Positionsliste an, um die Eigenschaften und den Status der einzelnen Positionen zu prüfen.

Vorbereitende Schritte

Sie müssen mindestens eine Position erstellt haben.

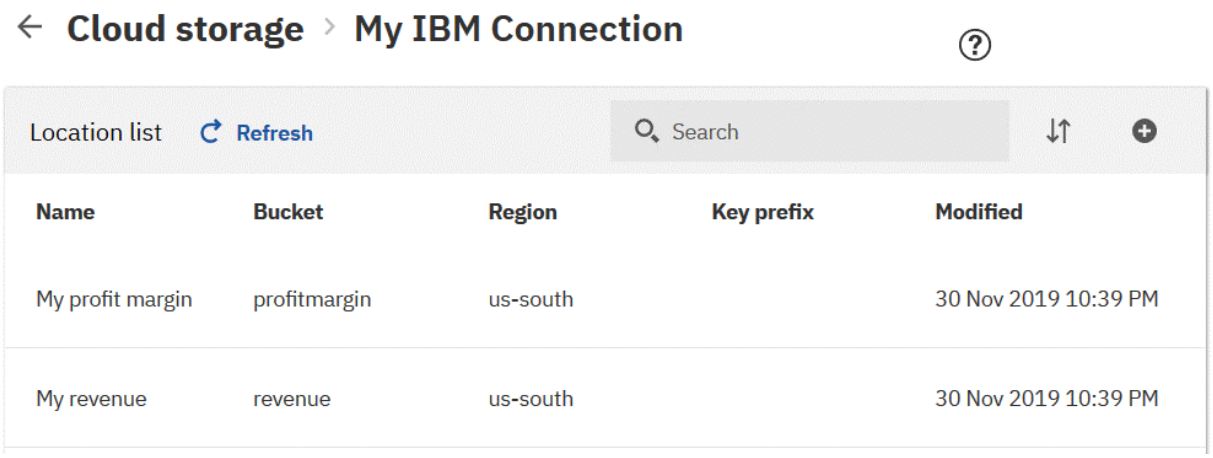
Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Speicher**.

   Die **Verbindungsliste** wird angezeigt.
2. Klicken Sie auf eine Verbindung.

   Die **Positionsliste** wird angezeigt.

   Die folgende Abbildung zeigt ein Beispiel:



3. Klicken Sie auf eine Position.
4. Klicken Sie am Ende der Zeile für Ihre Position auf das Symbol mit den Auslassungspunkten  und anschließend auf **Eigenschaften**.

   Es wird eine Anzeige für die Position mit der Registerkarte **Allgemein** geöffnet.

   - Wenn Sie den Positionsnamen in der Liste abblenden und die Position vorübergehend nicht verfügbar machen wollen, klicken Sie auf **Erweitert** und wählen dann das Kontrollkästchen **Diesen Eintrag inaktivieren** aus.

Tipp: Die Verbindung zwischen dem Cognos Analytics-Server und dem Cloud-Speicherservice wird unterbrochen. Wenn Sie das Kontrollkästchen abwählen, können Benutzer die Position wieder verwenden.

- Wenn Sie den Namen Ihrer Position ändern wollen, klicken Sie auf das Symbol 'Bearbeiten' oben auf der Anzeige. Geben Sie dann einen neuen Namen ein.

5. Klicken Sie auf die Registerkarte **Position**.
   - Wenn Sie zu einem anderen Bucket wechseln wollen, wählen Sie es im Pulldown-Menü aus.

     Wichtig: Nur bei IBM und Amazon-Speicherumgebungen müssen Sie anschließend die Region auswählen, die Sie bei der Erstellung des Buckets in Ihrer Cloud-Speicherumgebung ausgewählt haben. Weitere Informationen finden Sie unter „Bestimmen der Region für das Cognos Analytics-Bucket" auf Seite 253.
   - Wenn Sie ein Schlüsselpräfix hinzufügen oder ändern wollen, geben Sie den Wert in das Feld **Schlüsselpräfix** ein. Weitere Informationen finden Sie unter „Verwenden eines Schlüsselpräfix" auf Seite 254.
   - Klicken Sie auf **Testen** und anschließend auf **Speichern**, um sicherzustellen, dass alle von Ihnen vorgenommenen Änderungen die Betriebsbereitschaft der Position aufrechterhalten.
6. Wenn Sie die Position aus der Liste entfernen wollen, klicken Sie auf das Symbol mit den Auslassungspunkten am Ende der Zeile. Klicken Sie anschließend auf **Löschen**.

   Anmerkung: Auf den Speicherservice, den Sie in der Cloud-Speicherumgebung erstellt haben, hat das Entfernen der Cognos Analytics-Speicherverbindung keine Auswirkungen.

Testen gespeicherter Ausgaben in der Cloud

Führen Sie die folgenden Aufgaben aus, um zu testen, ob Sie den Cloud-Speicher ordnungsgemäß aktiviert haben.

1. Speichern Sie einen Bericht in der Cloud.
2. Bestätigen Sie, dass die Ausgabe in der Cloud gespeichert wurde.

Speichern von Ausgaben in der Cloud

Das Speichern eines Berichts in der Cloud ist der **erste** Schritt beim Testen, ob der Cloud-Speicher ordnungsgemäß aktiviert wurde.

Vorbereitende Schritte

Bevor Sie Berichtsausgaben in der Cloud speichern können, müssen Sie zunächst eine Verbindung zu einem Cloud-Objektspeicherprovider erstellen und anschließend eine Speicherverbindung in Cognos Analytics erstellen.

Vorgehensweise

1. Klicken Sie für den Bericht, den Sie ausführen wollen, in einem Ordner auf die Schaltfläche 'Mehr' und klicken Sie dann auf **Ausführen als**.
2. Wählen Sie ein Ausgabeformat aus.
3. Wählen Sie **Im Hintergrund ausführen** aus, klicken Sie dann auf **Erweitert** und führen Sie die folgenden Schritte aus:
   a) Wählen Sie **Jetzt** für den Zeitpunkt aus, zu dem der Bericht ausgeführt werden soll.
   b) Wählen Sie im Feld **Sprachen** eine oder mehrere Ausgabesprachen aus.

c) Wählen Sie im Feld **Zustellung** das Kontrollkästchen **In Cloud speichern** aus und klicken Sie auf **Fertig**.

d) Ändern Sie den Berichtsnamen, wenn Sie dies wünschen.

Sie könnten zum Beispiel das aktuelle Datum und die aktuelle Uhrzeit an den Namen anhängen.

e) Klicken Sie auf das Feld **Verbindungsname** und wählen Sie eine Verbindung aus, die Sie in Cognos Analytics konfiguriert haben.

f) Klicken Sie auf das Feld **Positionsname** und wählen Sie eine Position aus, die Sie in der Verbindung konfiguriert haben.

g) Klicken Sie auf **Fertig**.

4. Klicken Sie auf **Ausführen**.

Ergebnisse

Der Bericht wird an der Cloud-Position gespeichert.

Nächste Schritte

Im nächsten Schritt bestätigen Sie, dass die Ausgabe in der Cloud gespeichert wurde.

Bestätigen, dass die Ausgabe in der Cloud gespeichert wurde

Das Bestätigen, dass die Ausgabe in der Cloud gespeichert wurde, ist der **zweite** Schritt beim Testen, ob der Cloud-Speicher ordnungsgemäß aktiviert wurde.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie einen Bericht in der Cloud gespeichert haben.

Vorgehensweise

1. Klicken Sie in der Anwendungsleiste auf das Symbol 'Persönliches Menü' und klicken Sie auf die Option **Eigene Zeitpläne und Abonnements**.
2. Klicken Sie auf **Zeitplan**, dann auf das Symbol 'Typ' und schließlich auf **Vergangen**.

   Der Status (**Erfolgreich** oder **Fehlgeschlagen**) der Berichtsausführung wird in einer Liste oder in einem Diagramm angezeigt.
3. Zum Anzeigen weiterer Details zur Berichtsausführung klicken Sie auf das Symbol 'Mehr' neben der Liste und klicken Sie dann auf **Versionen anzeigen**.
4. Klicken Sie auf das Symbol für 'Detailanzeige öffnen' für die Berichtsversion.

   Es werden weitere Informationen angezeigt, wie zum Beispiel die folgenden:

   - **Startzeit** der Berichtsausführung
   - **Endzeit** der Berichtsausführung
   - Nachricht über **gestarteten Upload** für jede Version
   - Nachricht über **beendeten Upload** für jede Version
5. Zum Anzeigen der Ausgabe wechseln Sie zu Ihrer Cloud-Speicherposition und navigieren zu dem Bucket oder Ordner, in dem Sie Ihre Cognos Analytics-Ausgabe gespeichert haben.

   Tipp: Wenn Benutzer ihre gespeicherten Ausgaben in der Cloud anzeigen können sollen, müssen Sie ihnen die entsprechenden Berechtigungen für den Zugriff auf die Cloud-Speicherposition zuweisen.

Nächste Schritte

Wenn Sie sich vergewissert haben, dass Cognos Analytics-Ausgaben an Ihrer Cloud-Position erfolgreich gespeichert werden können, informieren Sie andere Cognos Analytics-Benutzer, dass sie dieses Feature verwenden können.

Fehlerbehebung für Cloud-Speicher

Bei der Verwaltung des Cloud-Speichers in Cognos Analytics können möglicherweise Probleme auftreten.

In diesem Abschnitt werden einige häufiger auftretende Probleme und ihre möglichen Lösungen beschrieben.

Fehler beim Zugriff auf eine Cloud-Speicherverbindung

Sie versuchen, eine Position zu erstellen, jedoch wird die folgende Fehlernachricht angezeigt:

Fehler beim Zugriff auf die Cloud-Speicherverbindung '*verbindungsname*'.

Lösung

Versuchen Sie die folgenden Schritte:

- Prüfen Sie, ob Ihr Zugriffsschlüssel und Ihr geheimer Zugriffsschlüssel den aktuellen Werten Ihrer Cloud-Objektspeicherverbindung entsprechen.
- Klicken Sie auf **Testen**, um Ihre Verbindung zu testen.
- Leeren Sie Ihren Browser-Cache oder öffnen Sie ein privates Fenster (in Firefox) oder ein Incognito-Fenster (in Chrome). Starten Sie Cognos Analytics neu und versuchen Sie erneut, eine Position hinzuzufügen.
- Prüfen Sie, ob Ihre Cloud-Speicherumgebung ordnungsgemäß funktioniert.

Test fehlgeschlagen

Sie klicken auf **Testen**, um Ihre Verbindung bzw. Position zu testen, jedoch wird die folgende Nachricht angezeigt:

Test fehlgeschlagen

Lösung

Versuchen Sie die folgenden Schritte:

- Wenn sich der fehlgeschlagene Test auf eine neue Position bezog, stellen Sie sicher, dass Sie die richtige Region ausgewählt haben. Die Region muss mit der Region übereinstimmen, die Sie beim Erstellen eines Buckets in Ihrer Cloud-Objektspeicherumgebung ausgewählt haben. Weitere Informationen finden Sie unter „Bestimmen der Region für das Cognos Analytics-Bucket” auf Seite 253.

  Tipp: Wenn Sie sich sicher sind, die richtige Region zu kennen, wählen Sie diese Region aus. Wiederholen Sie anschließend den Test.
- Wenn sich der fehlgeschlagene Test auf eine neue Verbindung bezog, stellen Sie sicher, dass die Verbindungsparameter korrekt eingegeben wurden.
- Leeren Sie Ihren Browser-Cache oder öffnen Sie ein privates Fenster (in Firefox) oder ein Incognito-Fenster (in Chrome). Starten Sie Cognos Analytics neu und versuchen Sie erneut, eine Position bzw. eine Verbindung hinzuzufügen.
- Prüfen Sie, ob Ihre Cloud-Speicherumgebung ordnungsgemäß funktioniert.

Datei kann nicht in die Cloud hochgeladen werden

Bei dem Versuch, eine Datei in eine Cloudspeicherposition hochzuladen, wird die Nachricht `Fehler beim Hochladen von` *`berichtsname`* angezeigt.

Sie versuchen beispielsweise, eine Datei für einen Amazon S3-Speicherservice hochzuladen. Dabei wird die folgende Nachricht angezeigt:

`Fehler beim Hochladen von` *`berichtsname`*`. Die Teilenummer muss eine Ganzzahl zwischen 1 und 10000 einschließlich sein (Service: Amazon S3; Statuscode: 400; Fehlercode: InvalidArgument; Anforderungs-ID:` *`anforderungs-id`*`)`

Diese Nachricht kann auftreten, wenn die Standardgröße von Datenblöcken, die beim Hochladen von Dateien an die Cloud übergeben werden, zu klein ist.

Lösung

Um dieses Problem zu vermeiden, können Sie die Datenblockgröße hochgeladener Dateien anpassen.

Kapitel 11. Cognos Analytics on Demand

Cognos Analytics on Demand ist eine Version von Cognos Analytics on Cloud, die Ihnen digital über den Self-Service zur Verfügung steht. Das Produkt wird bei Verfügbarkeit auf die neueste Version aktualisiert. Dieses Angebot hat drei Preisstufen: Standard, Plus und Premium.

Wer sollte Cognos Analytics on Demand verwenden?

Wenn Sie diese Kriterien erfüllen, können Sie sich für Cognos Analytics on Demand registrieren:

- ☐ Sie sind bereit, nur dann eine Verbindung zu Datenquellen herzustellen, wenn sie über ein Secure Gateway oder eine der unterstützten on Cloud-Datenbankenverbunden sind.
- ☐ Ihre Organisation verwendet nur einen Namespace.
- ☐ Sie sind bereit, sich mit IBMid oder mit einem Identitätsprovider zu authentifizieren, der in IBMid eingebunden ist.
- ☐ Sie sind kein vorhandener On Demand-Kunde.
- ☐ Sie sind bereit, alle Ihre Inhalte in einem Schritt zu migrieren. Partielle Importe können nicht ausgeführt werden.

Funktionalität

Eine vollständige Liste der Funktionen und unabhängig davon, ob sie von Cognos Analytics on Demand unterstützt werden, finden Sie unter Cognos Analytics-Angebote.

Begrenzungen

Sie sollten sich darüber im Klaren sein, dass das Angebot von Cognos Analytics on Demand die folgenden Einschränkungen aufweist:

- Wenn Sie von Cognos Analytics on Cloud Hosted migrieren:
  - Ihre Funktionseinstellungen werden nicht übertragen.
  - Die Cognos-Standardgruppen und -Rollen werden migriert. Sie verlieren jedoch alle Fähigkeiten, die ihnen zugewiesen wurden.
  - Wenn Ihre Cognos-Standardgruppen und -Rollen für den Inhalt von Inhalten verwendet wurden, wird diese Sicherheit beibehalten.
- Zertifikate können nicht gesichert werden.
- Cognos Analytics on Demand unterstützt die folgenden Informationen nicht:
  - Jobs
  - IBM Cognos Administration Console
  - Cognos-Standardgruppen und -Rollen. Sie können neue angepasste Rollen erstellen. Sie können sie jedoch nur für den sicheren Inhalt verwenden. Sie können die Funktionalität eines Benutzers, einer Gruppe oder einer Rolle nicht ändern.
  - Grafiken und Schriftarten
  - Secure File Transfer Protocol (SFTP)
  - Framework Manager
  - Datenquellen, für die eine SSL-Zertifizierung erforderlich ist
  - Power-Cubes und Transformer
  - Kompatibler Abfragemodus (CQM)

Migration auf Cognos Analytics on Demand

Wenn Sie der Administrator einer Cognos Analytics on Cloud Hosted-Umgebung sind, möchten Sie möglicherweise auf eine Cognos Analytics on Demand-Umgebung migrieren.

Vorbereitende Schritte

Informieren Sie sich über die Zielgruppe, den Funktionsumfang und die Einschränkungen von Cognos Analytics on Demand.

Wichtig: Sie müssen Mitglied der Rolle "Verzeichnisadministratoren" sein, um diese Aufgabe ausführen zu können.

Informationen zu diesem Vorgang

Einige Cognos-Daten werden während der Migration nicht übertragen:

- Ihre Funktionseinstellungen werden nicht übertragen.
- Die Cognos-Standardgruppen und -Rollen werden migriert. Sie verlieren jedoch alle Fähigkeiten, die ihnen zugewiesen wurden.
- Wenn Ihre Cognos-Standardgruppen und -Rollen für den Inhalt von Inhalten verwendet wurden, wird diese Sicherheit beibehalten.

Vorgehensweise

1. Wenden Sie sich an Ihren IBM Vertriebsmitarbeiter, um zu besprechen, ob ein Cognos Analytics on Demand-Subscription für Ihr Unternehmen in Frage kommt.

   Tipp: Wenn Sie sich entscheiden, mit der Migration fortzufahren, denken Sie daran, dass Sie eng mit Ihrem Vertriebsmitarbeiter zusammenarbeiten werden. Sie werden informiert, wann immer es etwas gibt, was Sie tun müssen. Wenn Sie eine Frage haben, ist Ihr Vertriebsmitarbeiter Ihre erste Anlaufstelle!
2. Wenn sich Ihr Unternehmen nicht bereits mit IBMid authentifiziert, müssen Sie Ihren Identitätsanbieter mit IBMid föderieren, bevor die Migration beginnt.

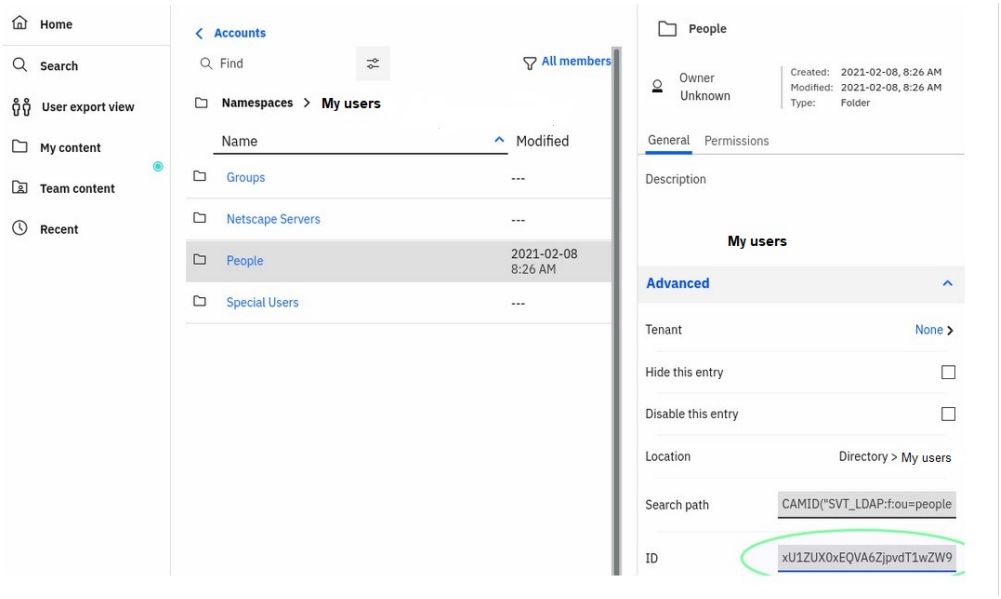
   Weitere Informationen finden Sie in der Veröffentlichung IBMid Enterprise Federation Adoption Guide (https: //ibm.ent.box.com/notes/78040808400?v=IBMid-Federation-Guide).
3. Vergewissern Sie sich, dass Sie eine Einladung zu Ihrer On Demand Subskription erhalten und dass Sie diese Aufgaben erledigen:
   - Akzeptieren Sie Ihre Einladung als On Demand-Subskriptionsadministrator.
   - Laden Sie alle Ihre Benutzer ein, der On-Demand-Subscription beizutreten.

     Anmerkung: Die Benutzer müssen die Einladungen nicht sofort akzeptieren. Sie müssen jedoch alle eingeladen werden, damit das IBM Team ihre IBMIDs validieren kann.
4. Entfernen Sie in Ihrer Cognos Analytics-Hosted-Umgebung alle Inhalte und Benutzerprofile, die Sie nicht in Ihre On-Demand-Umgebung exportiert haben möchten.
5. Wenn Sie Ihre Beispiele auf "On Demand" importieren möchten, benennen Sie den Ordner `Samples` um.
6. Erstellen Sie eine `.csv` -Datei, die Informationen zu jedem Benutzer in Ihrem Namespace enthält.
   a) Rufen Sie die Datei `user-export-extension.zip` von Ihrem Verkaufsrep ab, und kopieren Sie sie auf Ihren Computer.
   b) Wählen Sie **Verwalten** > **Anpassung** aus und klicken Sie dann auf die Registerkarte **Erweiterungen** .
   c) Klicken Sie auf das Symbol 'Erweiterung hochladen'  , navigieren Sie zu der Datei `user-export-extension.zip`und klicken Sie dann auf **Öffnen**.

      Der Name wird in der Liste der Erweiterungen angezeigt.

d) Melden Sie sich ab und dann wieder bei Cognos Analytics an, damit die Erweiterung wirksam wird.

Die Kategorie **Benutzerexportsicht** wird in der Navigationsleiste angezeigt.



e) Klicken Sie auf **Benutzerexportsicht**und navigieren Sie dann zu **Konten** > **Namensbereiche** > ***your_namespace_folder*** > **Personen** .

f) Kopieren Sie in der Anzeige "Personen" unter ***your_namespace_folder***den Wert in das Feld **ID** .

g) Fügen Sie den Wert **ID** in das Feld **Namespace-ObjectID** ein.

Die Kategorie **Benutzerexportsicht** wird in der Navigationsleiste angezeigt.

h) Klicken Sie auf **Benutzer abfragen** , um die Liste der Benutzer zu überprüfen.

Tipp: Entfernen oder ändern Sie bei Bedarf alle Benutzer.

i) Klicken Sie auf **CSV herunterladen** und speichern Sie die `.csv` -Datei auf Ihrem Computer.

j) Senden Sie die `.csv` -Datei an das IBM Team.

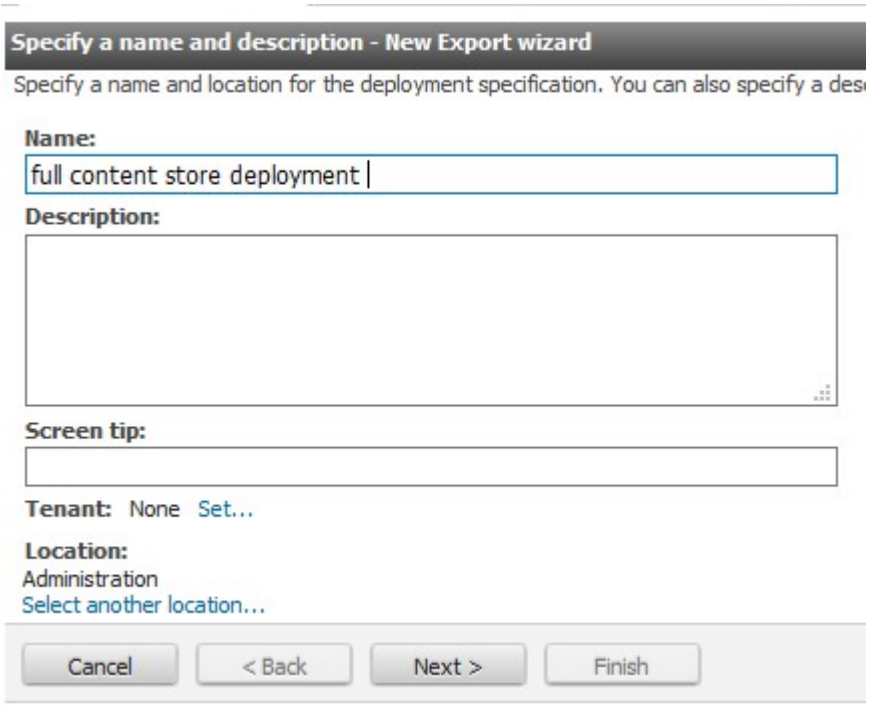
k) Entfernen Sie die Erweiterung **Benutzerexportsicht** , nachdem Sie sie mit der Erweiterung abgeschlossen haben.

7. Erstellen Sie eine Implementierung Ihrer aktuellen Umgebung:

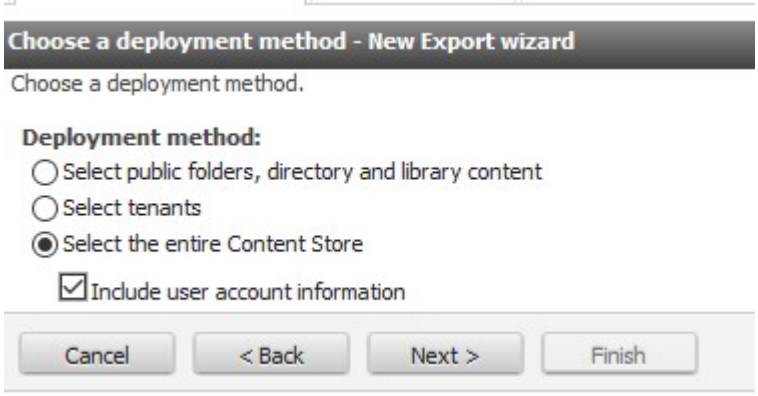
a) Klicken Sie in **IBM Cognos Administration** auf der Registerkarte **Konfiguration** auf **Inhaltsadministration**.

b) Klicken Sie in der Symbolleiste auf das Symbol **Neuer Export**  .

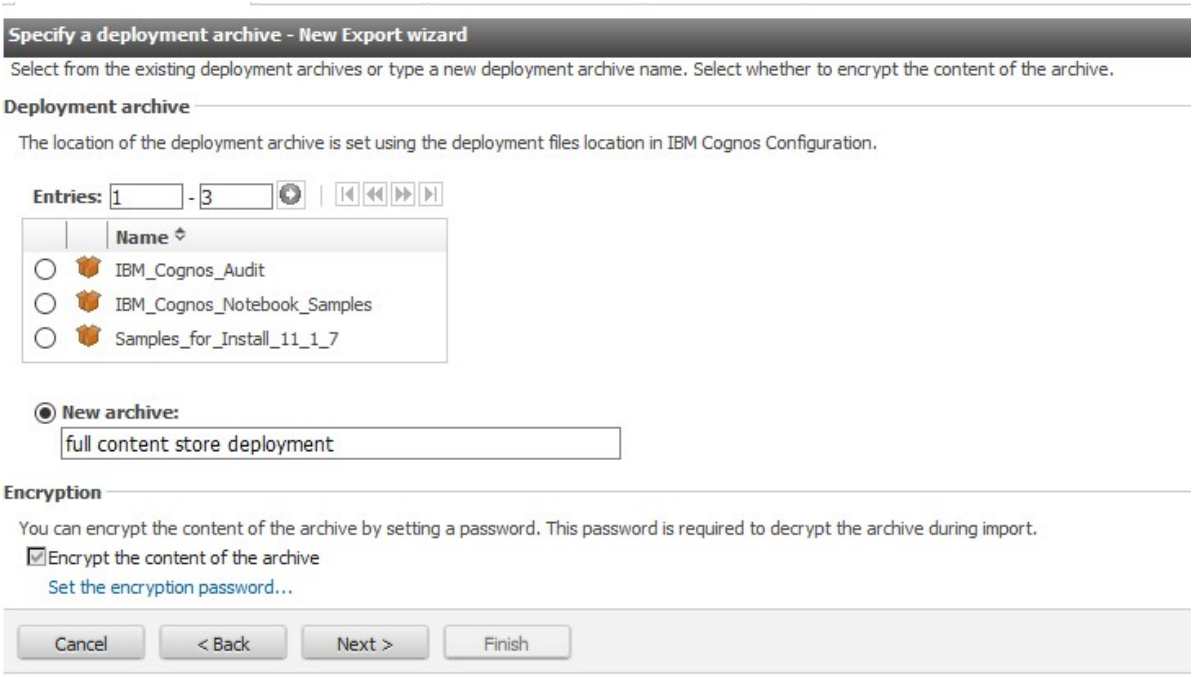
c) Benennen Sie das Archiv.



d) Wählen Sie sowohl **Den gesamten Content-Store auswählen** als auch **Benutzerkontoinformationen einschließen** aus und klicken Sie anschließend auf **Weiter**.

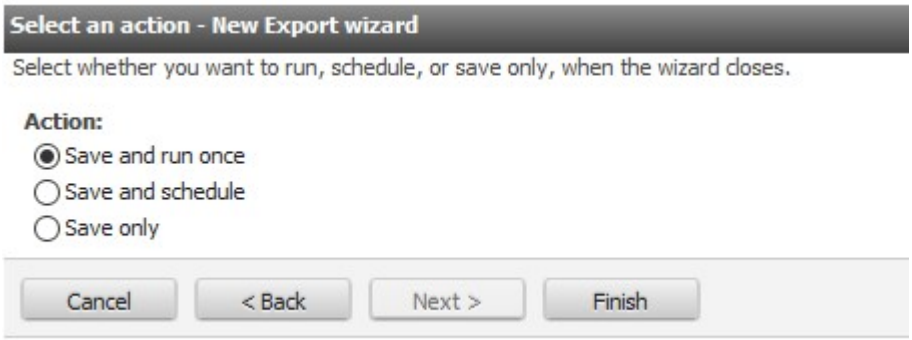


e) Legen Sie ein Verschlüsselungskennwort fest, das Sie dem IBM Team geben, damit sie den Inhalt importieren können, und klicken Sie anschließend auf **Weiter**.



f) Prüfen Sie die Zusammenfassung und klicken Sie auf **Weiter**.

g) Wählen Sie unter **Aktion**die Option **Speichern und einmal ausführen** aus und klicken Sie dann auf **Fertigstellen**.



Eine `.zip` Implementierungsdatei wird in *`installation_location`*`/deployment`erstellt.

h) Kopieren Sie die `.zip` Implementierungsdatei und senden Sie sie an das IBM Team.

Tipp: Das IBM Team importiert diese Implementierung in Ihre On-Demand-Umgebung.

8. Wenn das IBM Team in Ihrem **Team Inhaltsordner** Assets ohne gültige Eigentümer entdeckt, sendet es Ihnen eine Liste der ungültigen Eigentümer und fragt Sie, wie Sie vorgehen sollen.

   Wenn dies geschieht, gehen Sie wie folgt vor:

   a) Öffnen Sie die Liste in einem Editor.

   b) Geben Sie neben jedem ungültigen Benutzernamen den Namen eines gültigen Benutzers ein, dem der Inhalt des ungültigen Benutzers neu zugewiesen werden kann.

   c) Senden Sie die Liste zurück an das IBM Team.

9. Nachdem das IBM Team Sie darüber informiert hat, dass die Migration abgeschlossen ist, stellen Sie Ihre Datenquellenverbindungen wieder her, indem Sie ein Secure Gateway erstellen oder eine Verbindung zu einer unterstützten Datenbank in der Cloud herstellen.

Verwalten Ihres On Demand-Abonnements (für Subscription-Administratoren)

Wenn Sie als Subskriptionsadministrator für IBM Cognos Analytics on Demand bezeichnet werden, erhalten Sie eine E-Mail-Einladung zur Verwendung der on-Demand-Version. Anschließend können Sie Benutzer zur Subskription hinzufügen und entfernen, Benutzer zuordnen, Ihr Abonnement aktualisieren und andere Subskriptionsdetails verwalten.

Annehmen einer Einladung zu einem Abonnement von Cognos Analytics on Demand

Nachdem Sie eine E-Mail-Einladung zur Teilnahme an einem IBM Cognos Analytics on Demand-Abonnement akzeptiert haben, können Sie sich bei dem Abonnement anmelden.

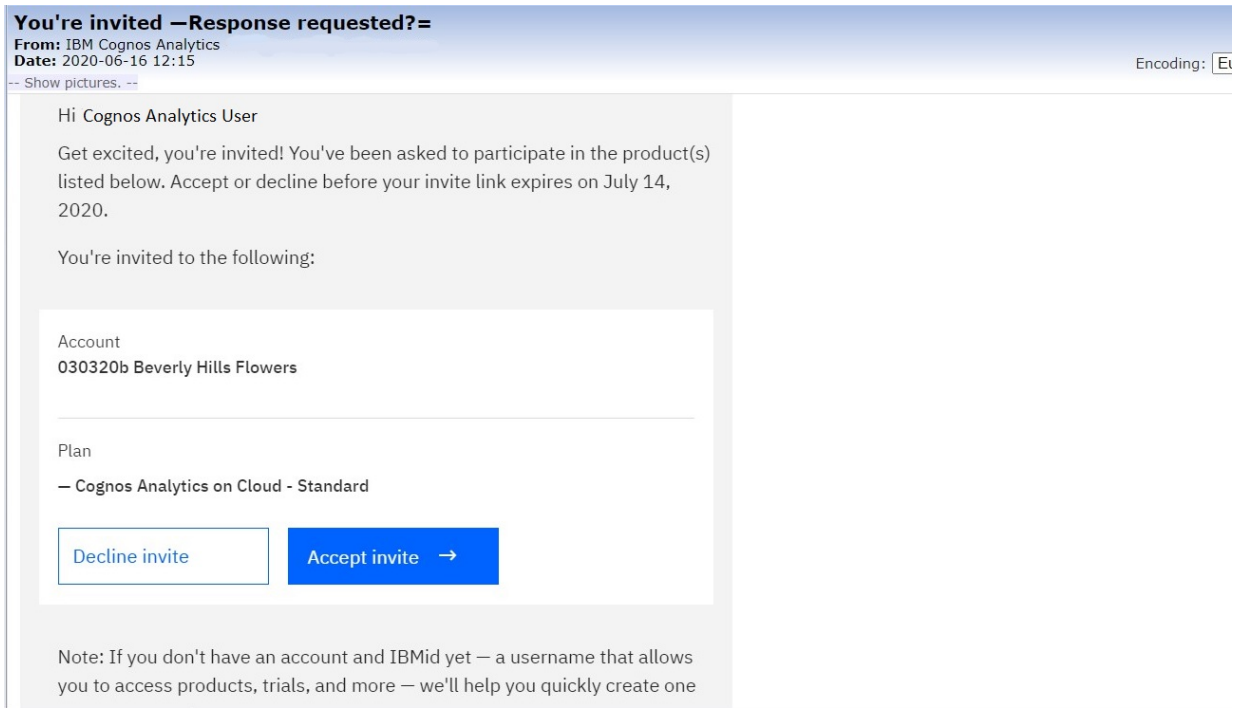
Anmerkung: Die Schritte in dieser Aufgabe sind für die beiden on Demand-Abonnementrollen *weitgehend* identisch:

- Abonnementadministratoren
- Lizenzierte Benutzer

Wenn Sie eine E-Mail von **IBM Cognos Analytics <noreply@us.ibm.com>** erhalten, in der Sie eingeladen werden, IBM Cognos Analytics on Demand zu verwenden, führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Öffnen Sie die Einladungs-E-Mail und klicken Sie auf **Einladung akzeptieren**.



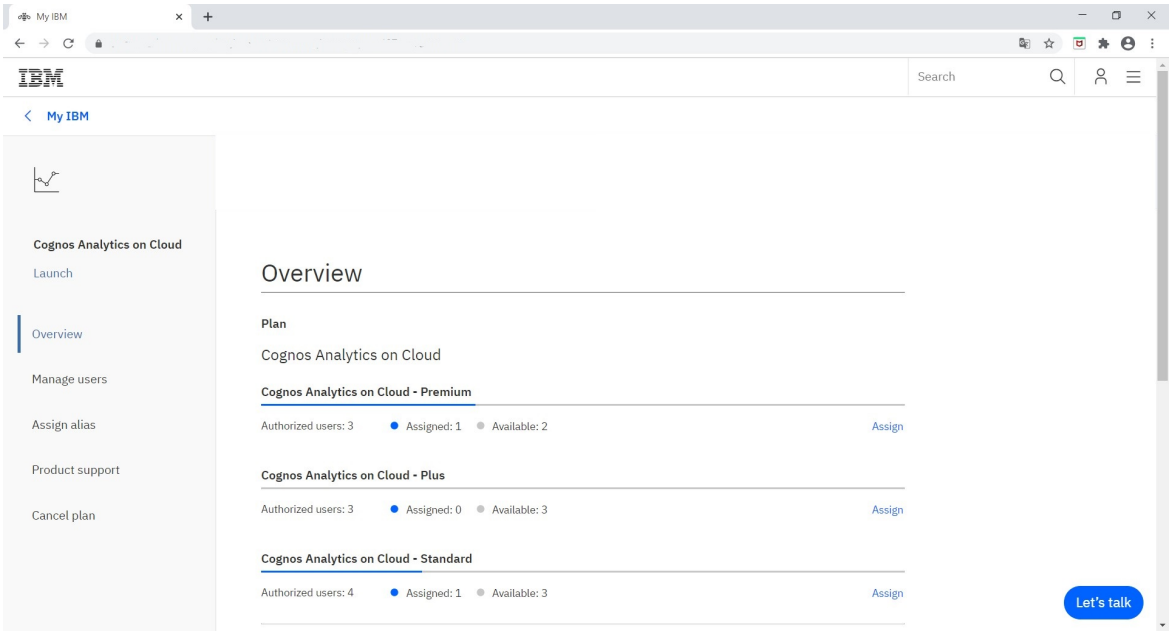
2. Melden Sie sich mit Ihrer IBMid an, falls Sie bereits über eine solche verfügen. Falls nicht, erstellen Sie Ihr IBM Konto jetzt (https://www.ibm.com/account/profile).

   Die **Begrüßungsseite** von IBM Cognos Analytics wird angezeigt.
3. Wenn Sie eine Lizenz haben, können Sie sofort mit Cognos Analytics arbeiten. Weitere Informationen finden Sie im *Einführungshandbuch*.
4. Wenn Sie Details zu Ihrem Abonnement anzeigen wollen (wenn Sie Lizenzbenutzer sind) oder das Abonnement verwalten wollen (wenn Sie Abonnementadministrator sind), gehen Sie wie folgt vor:
   a) Klicken Sie in der Anwendungsleiste auf das Symbol für das persönliche Menü .

b) Klicken Sie auf **Produktabonnement verwalten**.

Die **Übersichtsseite** für Ihr IBM Cognos Analytics-Abonnement wird angezeigt.

- Wenn Sie Abonnementadministrator sind, sieht die **Übersichtsseite** wie folgt aus:

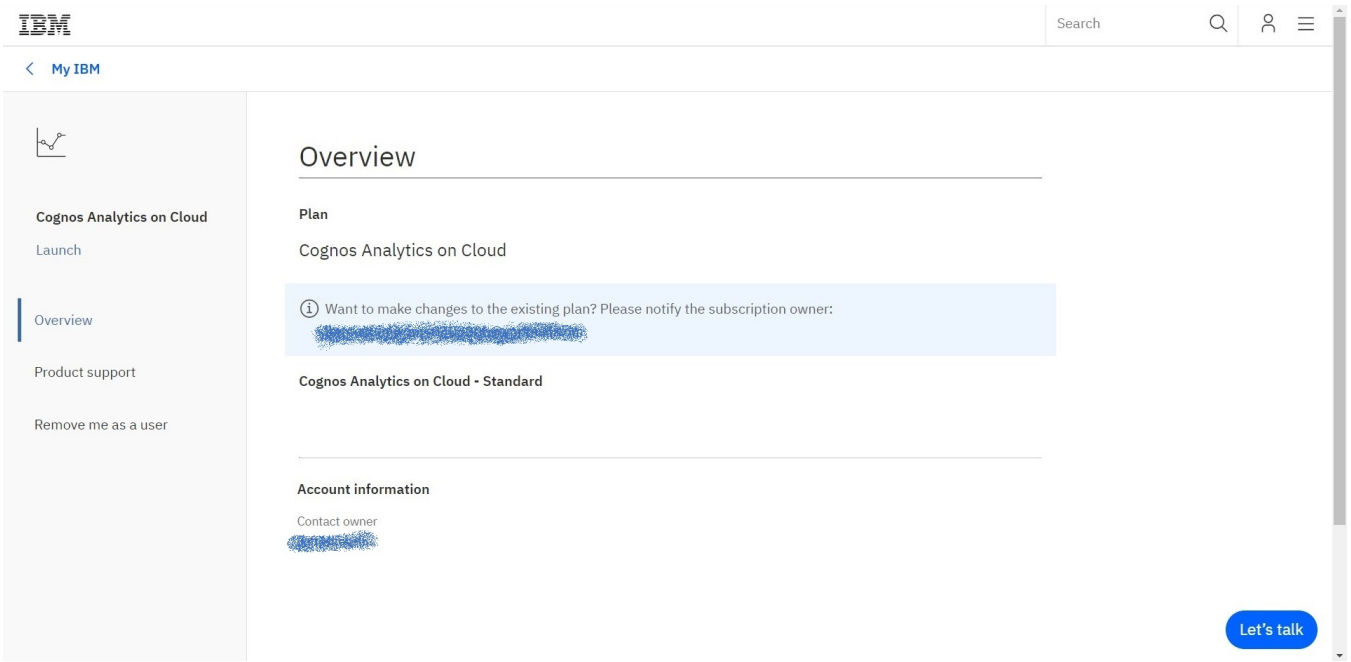


Es werden drei Abonnementebenen angezeigt:

- **Cognos Analytics on Cloud - Premium**
- **Cognos Analytics on Cloud - Plus**
- **Cognos Analytics on Cloud - Standard**

Anmerkung: Notieren Sie sich zur Vereinfachung der Planung Ihrer Benutzerzuweisungen die Anzahl der bereits **zugewiesenen** Lizenzplätze sowie die Anzahl der noch **verfügbaren** Lizenzplätze, die für das ausgewählte Abonnement angezeigt werden.

- Wenn Sie Lizenzbenutzer sind, sieht die **Übersichtsseite** wie folgt aus:



Anmerkung: Lizenzbenutzer bekommen keine Informationen zu Abonnementebenen angezeigt. Da es sich bei Lizenzbenutzern nicht um Abonnementadministratoren handelt, können sie keine Änderungen am Abonnement vornehmen und auch keine weiteren Benutzer einladen.

Anmeldung beim eigenen Abonnement

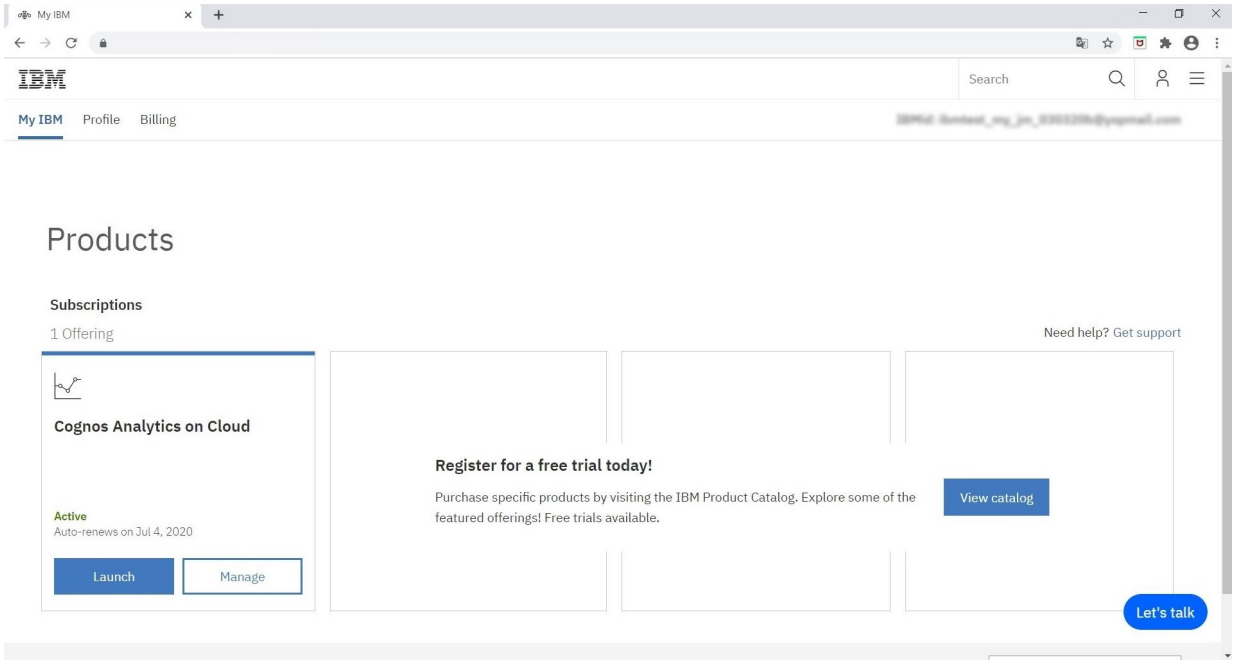
Wenn Sie zuvor die an Sie gerichtete E-Mail-Einladung akzeptiert haben und Änderungen an Ihrem Abonnement vornehmen wollen, können Sie sich über Ihr IBM Dashboard bei der **Übersichtsseite** Ihres Abonnements anmelden.

Führen Sie die folgenden Schritte aus:

Vorgehensweise

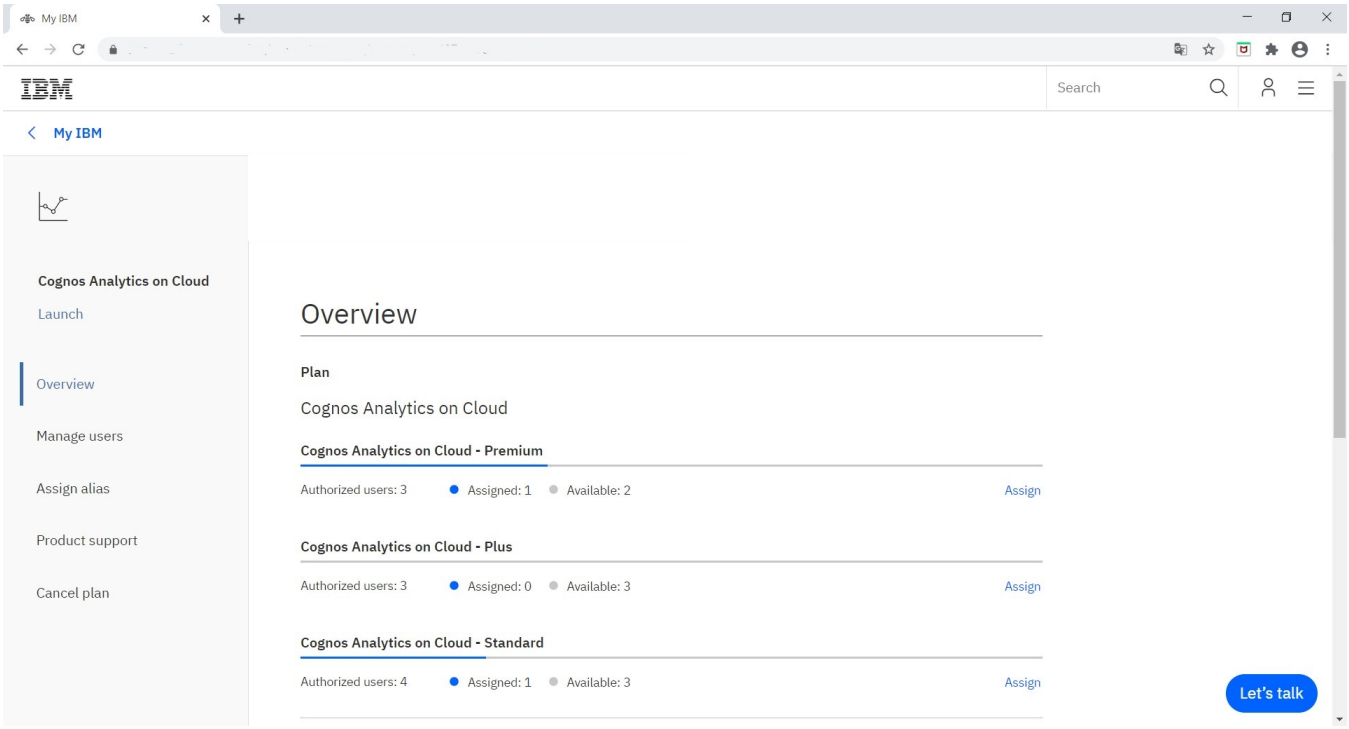
1. Navigieren Sie zu Ihrem IBM Dashboard (https://myibm.ibm.com/dashboard).
2. Melden Sie sich bei Ihrem IBM Konto an, falls Sie bereits über ein solches verfügen. Falls nicht, erstellen Sie Ihr IBM Konto jetzt (https://www.ibm.com/account/profile).

   Ihr IBM Dashboard wird angezeigt. Es enthält eine Kachel für Ihr Cognos Analytics on Cloud-Abonnement:



3. Klicken Sie in der Kachel für Ihr IBM Cognos Analytics on Cloud-Produkt auf **Verwalten**.

   Die **Übersichtsseite** für Ihr IBM Cognos Analytics-Abonnement wird angezeigt:



Es werden drei Abonnementebenen angezeigt:

- **Cognos Analytics on Cloud - Premium**
- **Cognos Analytics on Cloud - Plus**
- **Cognos Analytics on Cloud - Standard**

Anmerkung: Notieren Sie sich zur Vereinfachung der Planung Ihrer Benutzerzuweisungen die Anzahl der bereits **zugewiesenen** Lizenzplätze sowie die Anzahl der noch **verfügbaren** Lizenzplätze, die für das ausgewählte Abonnement angezeigt werden.

Abonnementrollen für on Demand

Es gibt zwei Typen von Abonnementrollen in Cognos Analytics on Demand: **1.** Abonnementadministratoren und **2.** Lizenzbenutzer.

Abonnementadministratorrolle

Als Abonnementadministrator können Sie die folgenden Änderungen an Ihrem registrierten IBM Cognos Analytics on Demand-Plan vornehmen:

- Benutzer zum Abonnement der Ebene **Standard**, **Plus** oder **Premium** hinzufügen oder aus dem entsprechenden Abonnement entfernen.

  Anmerkung: Eine Liste der Features, die für die einzelnen on Demand-Abonnementebenen verfügbar sind, finden Sie unter Cognos Analytics-Angebote.
- Benutzern eine der folgenden Rollenoptionen zuweisen:
  - Abonnementadministratorrolle
  - Lizenzbenutzerrolle
  - Abonnementadministratorrolle und Lizenzbenutzerrolle
- E-Mail an Benutzer senden, die Sie zur Verwendung von Cognos Analytics on Demand einladen
- Cognos Analytics on Demand-Plan stornieren

Lizenzbenutzerrolle

Ein Lizenzbenutzer kann IBM Cognos Analytics on Demand mit den Funktionen verwenden, die für ihre Subskriptionsebenedefiniert sind. Wenn Sie Lizenzbenutzer beispielsweise für ein Standardabonnement registriert haben, dann sind sie nicht in der Lage, Berichte zu erstellen. Sollen diese Benutzer Berichte erstellen können, müssen Sie ihr Abonnement auf die Ebene 'Premium' hochstufen.

Lizenzbenutzer können die folgenden Tasks ausführen:

- Sich selbst als Benutzer aus dem Abonnement entfernen.
- Starten und Verwenden von IBM Cognos Analytics on Demand
- in Cognos Analytics on Demand, erstellen Sie angepasste Gruppen und Rollen in dem Cognos-Namespace, für den Inhalt gesichert werden kann.

  Wichtige Hinweise zu Gruppen und Rollen in Cognos-Namespaces:

  – Die beiden *On Demand-Subskriptionsrollen* (Subskriptionsadministratoren und Lizenzbenutzer) dienen einem anderen Zweck als *Cognos-Namespace-Rollen*.

  – In Cognos Analytics on Demand sind die standardmäßigen integrierten Gruppen und Rollen im Cognos-Namespace nicht vorhanden.

Hinzufügen von Benutzern zu Ihrer On Demand Subscription

Wenn Sie ein Abonnementadministrator für IBM Cognos Analytics on Demand sind, können Sie Benutzer zu Ihrem Abonnement hinzufügen. Bei diesem Task weisen Sie jeden Benutzer der Subscription-Administratorrolle, der Lizenzbenutzerrolle oder beiden zu.

Wichtige Hinweise zu Gruppen und Rollen in Cognos-Namespaces:

- Die beiden *On Demand-Subskriptionsrollen* (Subskriptionsadministratoren und Lizenzbenutzer) dienen einem anderen Zweck als *Cognos-Namespace-Rollen*.
- In Cognos Analytics on Demand sind die standardmäßigen integrierten Gruppen und Rollen im Cognos-Namespace nicht vorhanden.

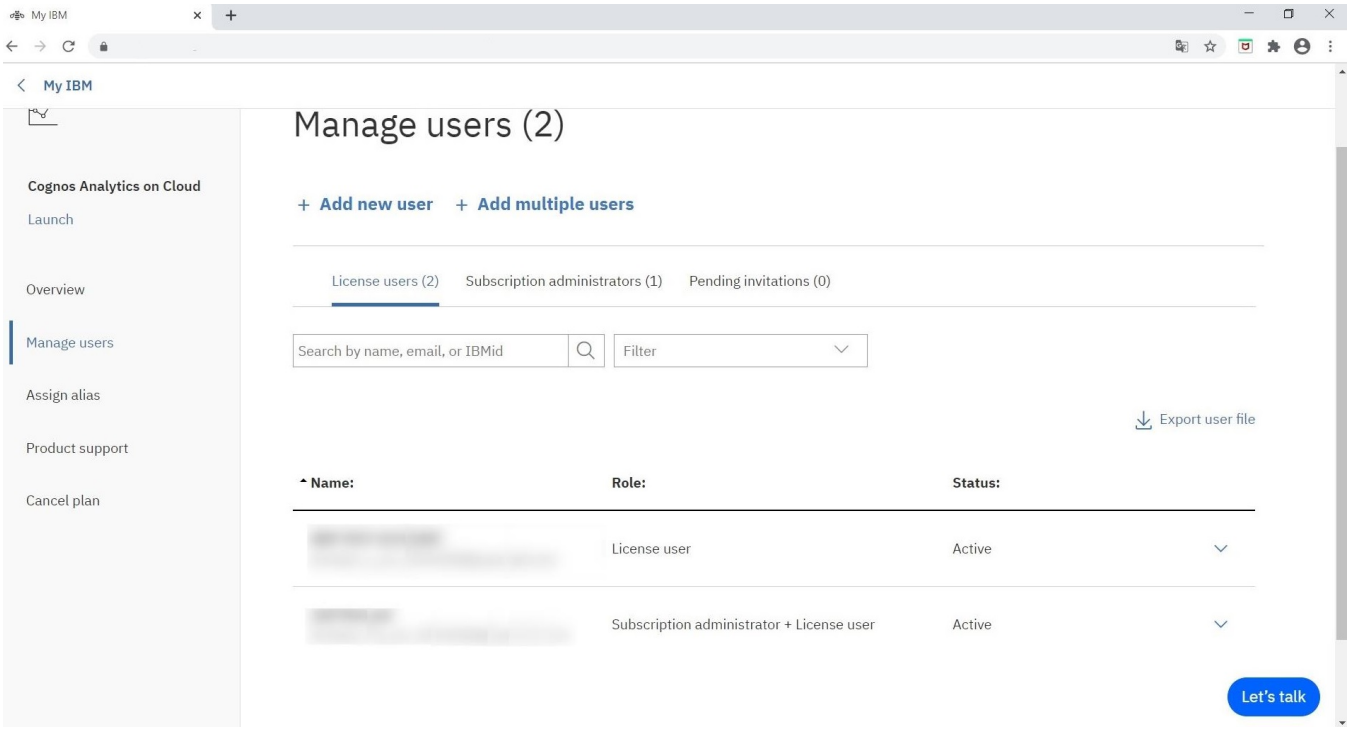
Informationen zu diesem Vorgang

Nachdem Sie diese Task ausgeführt haben, wird eine E-Mail an den/die Benutzer (en) gesendet, in dem sie aufgefordert werden, IBM Cognos Analytics on Demand zu verwenden.

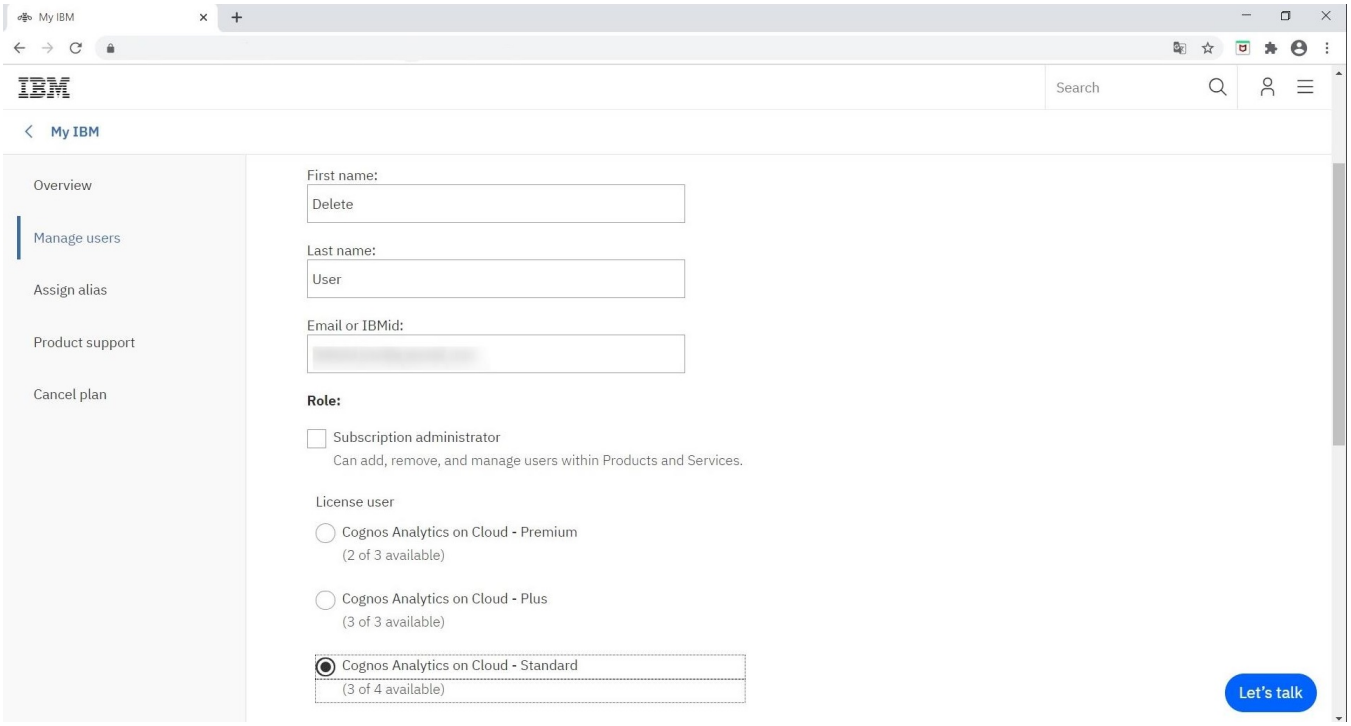
Vorgehensweise

1. Melden Sie sich bei Ihrem Abonnement an.
2. Klicken Sie im Navigationsfenster auf **Benutzer verwalten**.

   Die Seite 'Benutzer verwalten' wird angezeigt:



3. Wenn Sie einen einzelnen Benutzer hinzufügen wollen, führen Sie die folgenden Schritte aus:
   a) Klicken Sie auf **Neuen Benutzer hinzufügen**.



   b) Geben Sie den Vornamen, den Nachnamen und die E-Mail-Adresse des Benutzers ein.
   c) Wählen Sie eines oder beide der folgenden Kontrollkästchen aus:

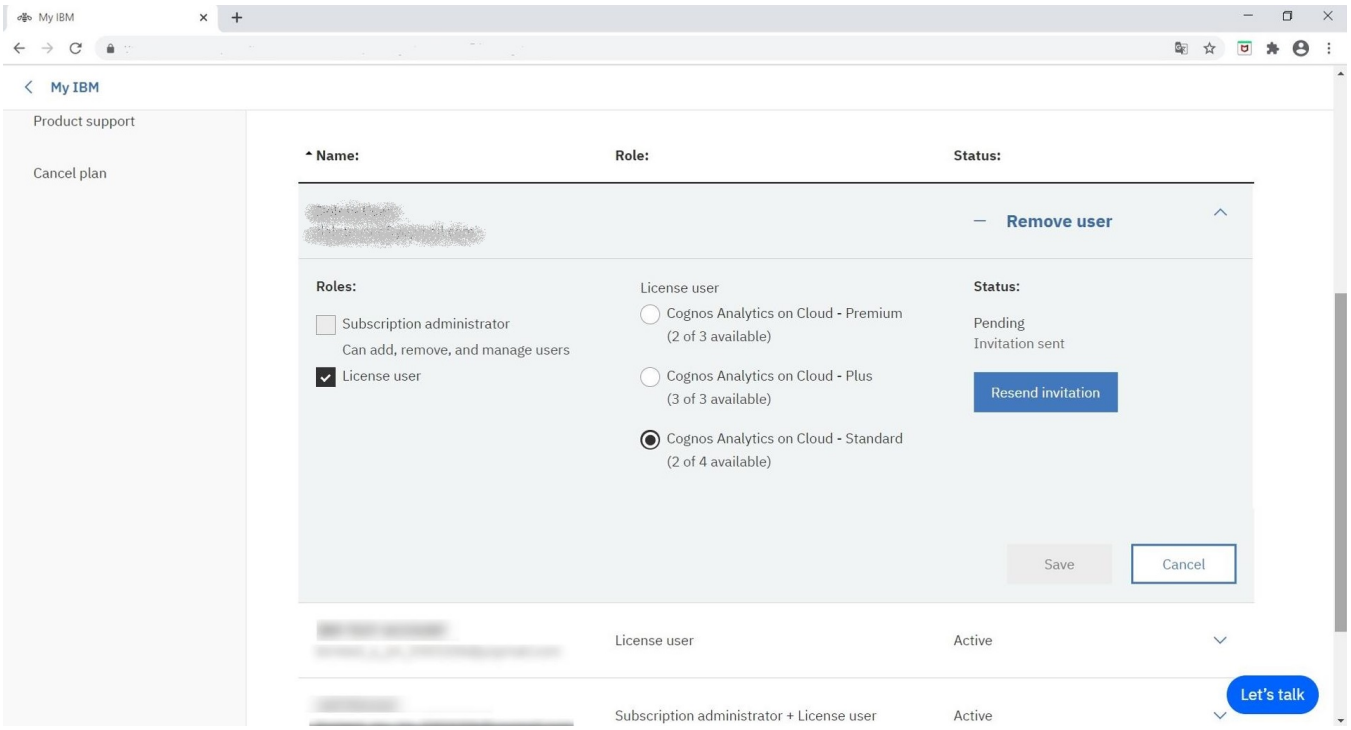
   - **Abonnementadministrator**

     Tipp: Es hat sich als bewährtes Verfahren erwiesen, mindestens zwei Benutzern die Rolle eines Abonnementadministrators zuzuweisen.
   - **Lizenzbenutzer** für eine der folgenden Abonnements:

- **Cognos Analytics on Cloud - Premium**
- **Cognos Analytics on Cloud - Plus**
- **Cognos Analytics on Cloud - Standard**

d) Klicken Sie auf **Übergabe**.

e) Klicken Sie auf das nach unten zeigende Winkelsymbol ⌄ am Ende der Zeile mit dem Namen des Benutzers, um die Benutzerinformationen einzublenden.



Beachten Sie in der vorstehenden Abbildung, dass der **Status** des Benutzers jetzt als **Anstehend** angegeben ist, da die Einladung noch nicht akzeptiert worden ist. Darüber hinaus gibt es die Option, die Einladung erneut zu senden, falls sie nicht angekommen oder bereits abgelaufen ist.

4. Wenn Sie mehrere Benutzer auf einmal hinzufügen wollen, führen Sie die folgenden Schritte aus:

a) Klicken Sie auf **Mehrere Benutzer hinzufügen**.

b) Klicken Sie auf **Diese CSV-Datei zum Hochladen mehrerer Benutzer verwenden**.

c) Bearbeiten Sie die Vorlage `add-multi-users.csv`, um den Namen, die E-Mail-Adresse und die Lizenzrolle(n) jedes einzelnen Benutzers aufzulisten.

d) Speichern Sie die Datei.

e) Klicken Sie auf **Datei auswählen** und navigieren Sie dann zu der Datei, die Sie soeben bearbeitet haben.

f) Klicken Sie auf **Hochladen**.

Tipp: Es kann ein paar Minuten dauern, bis das Abonnement mit den neuen Benutzern aktualisiert worden ist.

Ergebnisse

Wenn Sie fertig sind, wird die Liste der Benutzer auf der Seite **Benutzer verwalten** aktualisiert.

Es wird an alle Benutzer eine E-Mail gesendet, in der sie zur Verwendung von IBM Cognos Analytics on Cloud eingeladen werden. Ein Lizenzbenutzer erhält die gleiche E-Mail-Einladung, die Sie als Abonnementadministrator erhalten und akzeptiert haben.

Nachdem die Benutzer die Einladung akzeptiert haben, werden die Anzahl der **zugeordneten Lizenzplätze** und die Anzahl der **verfügbaren Lizenzplätze** auf der Seite **Übersicht** entsprechend aktualisiert.

Benutzer aus Abonnement entfernen

Wenn Sie ein Abonnementadministrator für IBM Cognos Analytics on Demand sind, können Sie Benutzer zu Ihrem Abonnement hinzufügen.

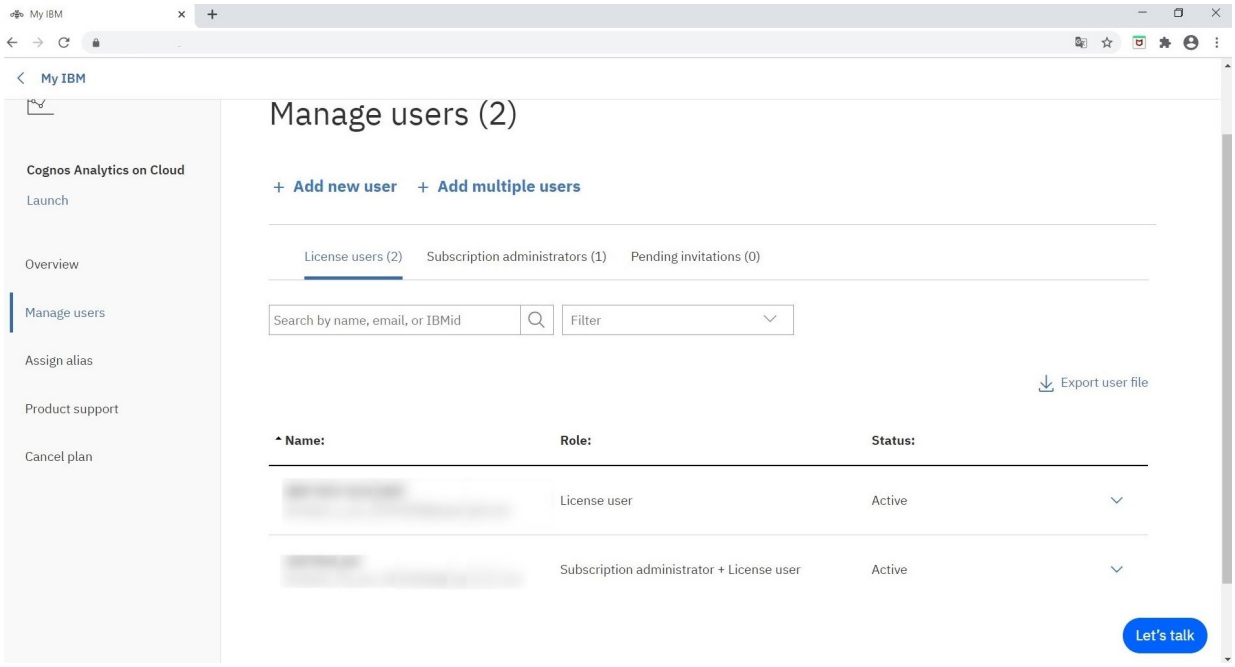
Wenn Benutzer entfernt werden, dann bleiben alle von ihnen erstellten öffentlichen Inhalte bestehen. Alle Inhalte im Ordner **Eigener Inhalt** gehen jedoch verloren. Werden Benutzer dem Abonnement anschließend wieder hinzugefügt, werden die Inhalte unter **Eigener Inhalt** nicht wiederhergestellt.

Führen Sie für jeden Benutzer, der entfernt werden soll, die folgenden Schritte aus:

Vorgehensweise

1. Melden Sie sich bei Ihrem Abonnement an.
2. Klicken Sie im Navigationsfenster auf **Benutzer verwalten**.

   Die Seite 'Benutzer verwalten' wird angezeigt:

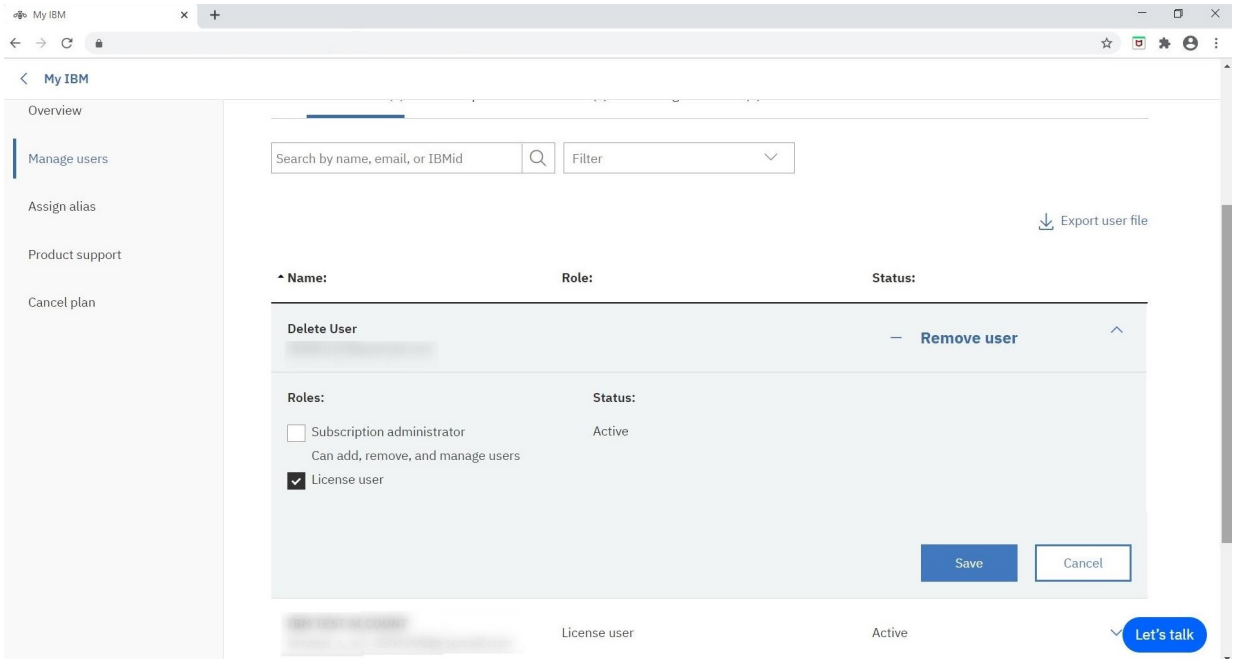


3. Suchen Sie nach dem betreffenden Benutzer.

   Tipps:

   - Suchen Sie nach Textteilen im Namen, in der E-Mail-Adresse oder in der IBMid des betreffenden Benutzers.
   - Klicken Sie auf **Lizenzbenutzer**, **Abonnementadministratoren** oder **Anstehende Einladungen**, um die Benutzereinträge nach der jeweiligen Kategorie zu filtern.
   - Klicken Sie auf **Filter**, um nach dem Status des Benutzers zu filtern.

4. Klicken Sie auf das nach unten zeigende Winkelsymbol ⌄ am Ende der Zeile mit dem Namen des Benutzers, um die Benutzerinformationen einzublenden.



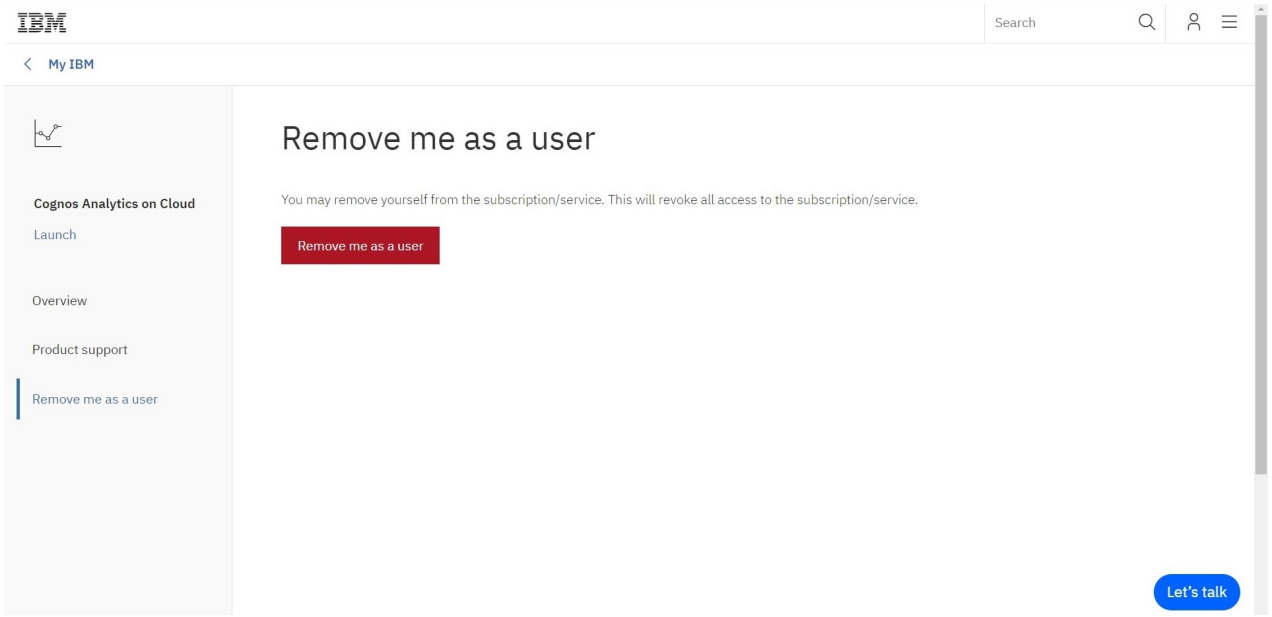
5. Wenn Sie den Benutzer aus Ihrem Abonnement entfernen wollen, klicken Sie auf **Benutzer entfernen**.
6. Wenn Sie die Rolle des Benutzers ändern wollen, ändern Sie dementsprechend die Auswahl der Kontrollkästchen im Abschnitt **Rollen**.

   Anmerkung: Wenn Sie weder das Kontrollkästchen **Abonnementadministrator** noch das Kontrollkästchen **Lizenzbenutzer** auswählen, wird der betreffende Benutzer aus dem Abonnement entfernt.
7. Klicken Sie auf **Speichern**.

Ergebnisse

Je nach der von Ihnen getroffenen Auswahl wird der Benutzer entweder aus dem Abonnement entfernt oder seine Rolle aktualisiert.

Anmerkung: Benutzer können sich auch selbst aus dem Abonnement entfernen, indem Sie im Navigationsmenü ihres eigenes Dashboards die entsprechende Option für **Mich als Benutzer entfernen** auswählen. Dies wird in der folgenden Abbildung gezeigt:



Upgrade für Testabonnement durchführen

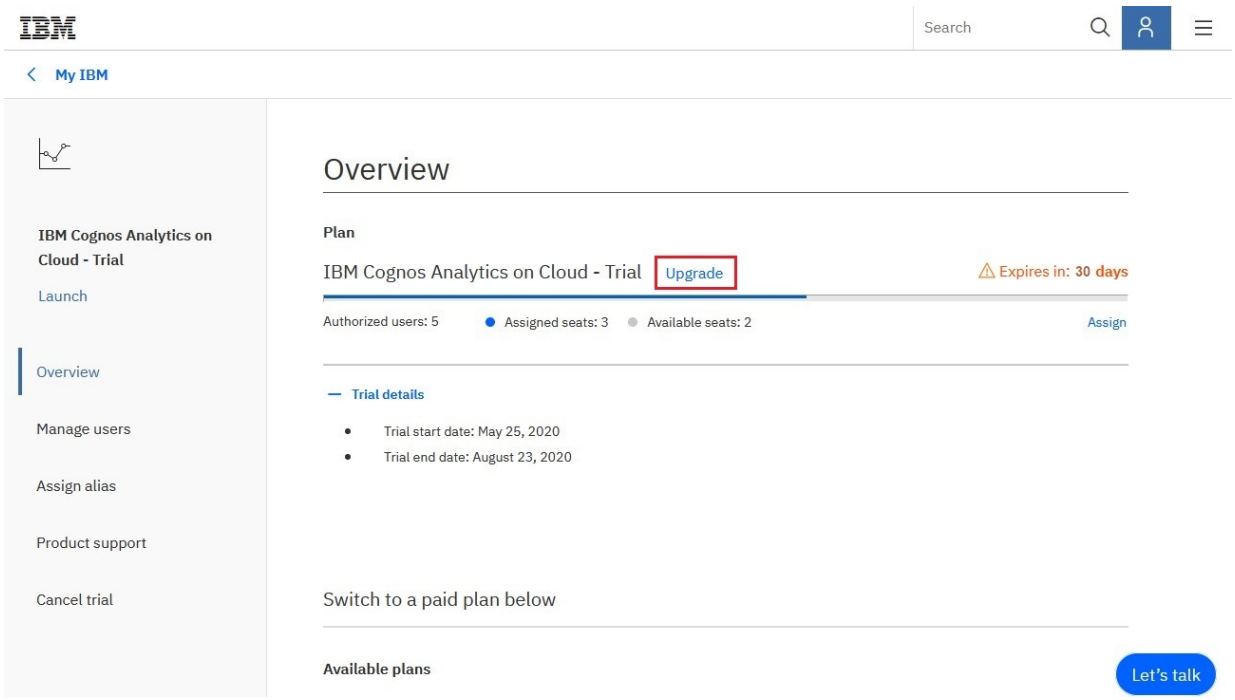
Wenn Sie über ein Testabonnement für IBM Cognos Analytics Cloud verfügen, können Sie jederzeit ein Upgrade auf einen Plan durchführen, der Ihnen eine umfassendere Benutzererfahrung bietet.

Anmerkung: Das Testabonnement bietet die gleiche Funktionalität wie das Premium-Angebot. Dies sollten Sie bei der Entscheidung für ein Upgrade berücksichtigen.

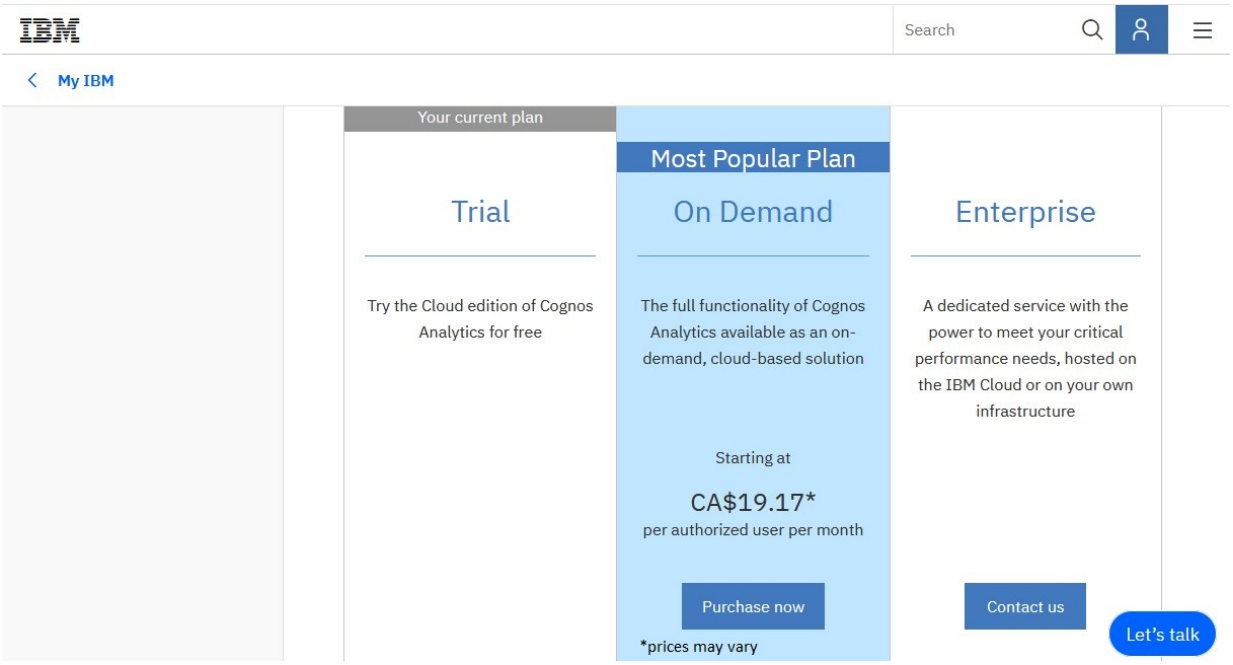
Vorgehensweise

1. Navigieren Sie zu Ihrem IBM Dashboard (https://myibm.ibm.com/dashboard).
2. Melden Sie sich bei Ihrem IBM Konto an.
3. Klicken Sie in der Kachel für IBM Cognos Analytics on Cloud auf **Verwalten**.

   Die **Übersichtsseite** für Ihr **IBM Cognos Analytics-Testabonnement** wird angezeigt:



4. Klicken Sie auf **Upgrade** oder blättern Sie abwärts, um Details zu verfügbaren IBM Cognos Analytics **On Demand**- oder **Enterprise**-Lösungen anzuzeigen.



5. Klicken Sie auf die Option für **Jetzt kaufen** oder **Kontaktieren Sie uns**, um mit Ihrem Upgrade fortzufahren.

Sichern Ihres Inhalts (für on Demand-Lizenzbenutzer)

Wenn Sie ein designierter Lizenzbenutzer für IBM Cognos Analytics on Demand sind, können Sie Ihren Cognos Analtyics-Inhalt sichern. Sie können dies in Cognos Analytics on Demand durchführen, indem Sie Berechtigungen für angepasste Gruppen und Rollen zuweisen, die Sie im Ordner für den Cognos-Namespace erstellt haben.

Angepasste Gruppen und Rollen im Cognos-Namespace

Gruppen und Rollen im Ordner 'Cognos-Namespace' stellen Sammlungen von Benutzern dar, die ähnliche Funktionen ausführen oder einen ähnlichen Status in einer Organisation haben. Beispiele für Gruppen sind Mitarbeiter, Entwickler und Vertriebspersonal. Mitglieder von Gruppen können Benutzer und andere Gruppen sein. Wenn ein Benutzer sich anmeldet, kann er keine Gruppe für eine Sitzung auswählen. Er wird immer mit allen Berechtigungen angemeldet, die der Gruppe zugewiesen sind, der er angehört.

Rollen in IBM Cognos haben eine ähnliche Funktion wie Gruppen. Mitglieder von Rollen können Benutzer, Gruppen und andere Rollen sein.

Die folgende Abbildung zeigt die Struktur von Gruppen und Rollen.

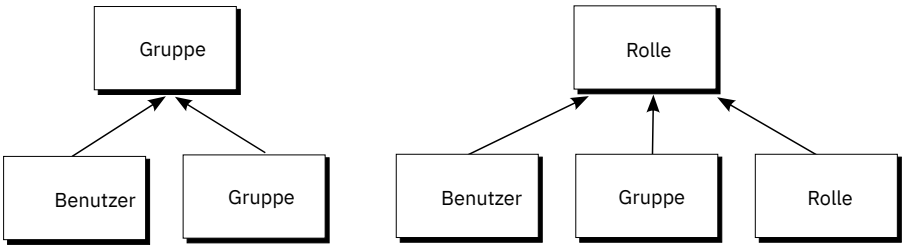


Abbildung 6. Struktur von Gruppen und Rollen

Benutzer können Mitglieder von Gruppen und Rollen werden, die in der IBM Cognos Software definiert wurden, sowie von Gruppen und Rollen, die von Authentifizierungsprovidern definiert wurden. Ein Benutzer kann einer oder mehreren Gruppen oder Rollen angehören. Wenn Benutzer mehreren Gruppen angehören, werden ihre Zugriffsberechtigungen zusammengeführt.

Vorgehensweise

1. Erstellen Sie angepasste Gruppen und Rollen im Cognos-Namespace-Ordner.

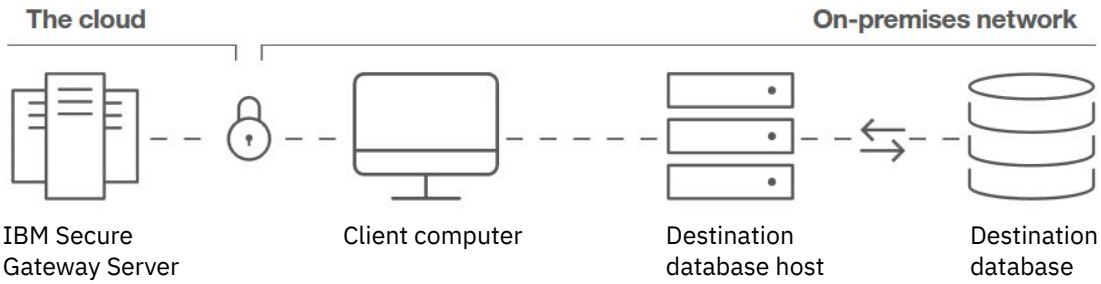
   Tipp: Sie können die Funktionalitäten eines Benutzers, einer Gruppe oder einer Rolle nicht ändern. Funktionalitäten werden durch die on Demand-Abonnementenebene des Benutzers bestimmt.
2. Legen Sie fest, welche Gruppen oder Rollen Zugriff auf Ihren Inhalt haben sollen.
3. Zuweisen von Gruppen-oder Rollenberechtigungen zu Ihrem ausgewählten Inhalt.

IBM Secure Gateway (nur on Demand)

Verwenden Sie IBM Secure Gateway, um eine verschlüsselte Verbindung zwischen einem lokalen Secure Gateway-Client und den Secure Gateway-Servern zu verwalten, die IBM in Cloud verwaltet. Auf diese Weise können Sie IBM Cognos Analytics on Demand verwenden, um Ihre On-Premises-Daten sicher zu verarbeiten.

Secure Gateway auf einen Blick

Zunächst installieren Sie den Secure Gateway Client in Ihrem On-Premises-Netzwerk und konfigurieren eine verschlüsselte bidirektionale Verbindung (TLS v1.2) mit dem on Cloud Secure Gateway-Server. Als Nächstes stellen Sie eine sichere Verbindung zwischen dem Secure Gateway-Client und einer lokalen Datenbank her. Diese lokale Datenbank wird als "Zieldatenbank" bezeichnet. Ihre On-Premises-Daten können dann sicher von Cognos Analytics on Demand abgerufen und bearbeitet werden.



Anmerkung: IBM Secure Gateway ist nur für die Verwendung mit Cognos Analytics on Demand verfügbar. IBM Secure Gateway wird für Hostbenutzer von Cognos Analytics on Cloud nicht unterstützt. Weitere Informationen finden Sie unter Kapitel 6, „Mieterverwaltung”, auf Seite 115.

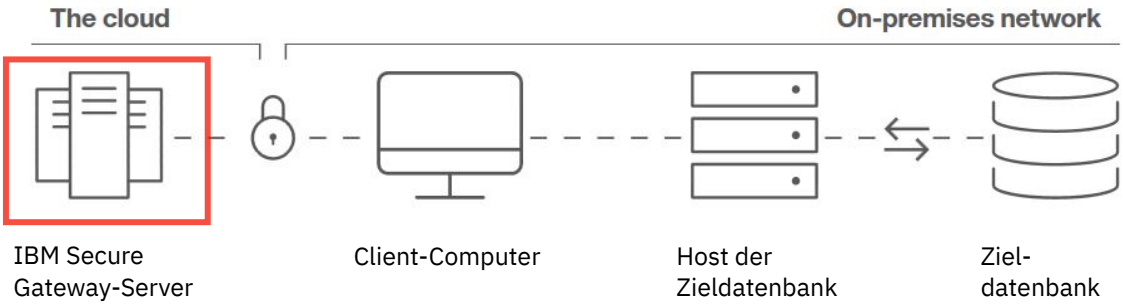
Weitere Informationen

Weitere Informationen zu IBM Secure Gateway finden Sie in den folgenden Ressourcen:

- Informationen zu Secure Gateway (https://cloud.ibm.com/docs/services/SecureGateway?topic=secure-gateway-about-sg
- Häufig gestellte Fragen (https://cloud.ibm.com/docs/services/SecureGateway?topic=securegateway-sg-faq)
- Fehlerbehebung (https://cloud.ibm.com/docs/services/SecureGateway?topic=securegateway-troubles-hooting)

Erstellen einer Secure Gateway-Instanz

Das Erstellen einer Secure Gateway-Instanz ist der **erste** Schritt zum Erstellen einer Verbindung zwischen dem IBM Secure Gateway-Server und Ihren lokalen Daten.



Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Sicheres Gateway**.
   - Wenn noch keine Secure Gateway-Instanzen vorhanden sind, wird die Seite **Sicheres Gateway** angezeigt.
   - Sind andere Gateways vorhanden, wird die **Liste sicherer Gateways** angezeigt.
2. Starten Sie den Assistenten **Verbindung zu einer lokalen Datenbank herstellen**.
   - Wenn Sie sich auf der Seite **Sicheres Gateway** befinden, klicken Sie auf **Erstellen**.
   - Wenn Sie sich auf der Seite **Liste sicherer Gateways** befinden, klicken Sie auf die Schaltfläche 'Gateway hinzufügen' .
3. Geben Sie einen Namen für das Gateway ein.

   Anmerkung: Sie können den Ablaufwert des Tokens an dieser Stelle ignorieren. Er bezieht sich auf das Sicherheitstoken, das für Ihr neues Gateway generiert wird.
4. Klicken Sie auf **Erstellen**.

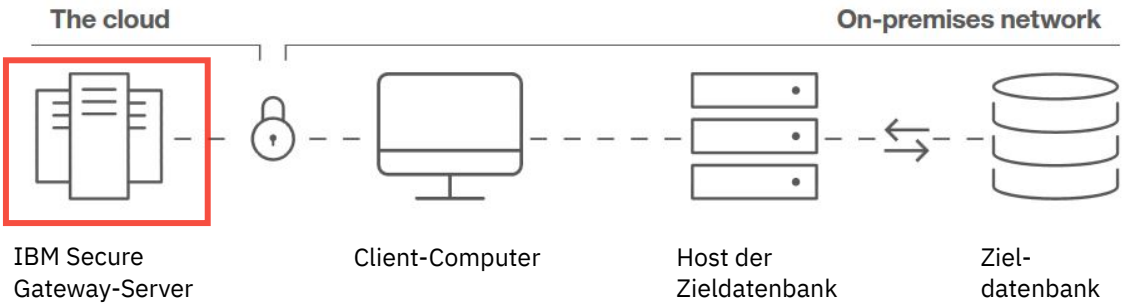
   Die Gateway-Instanz wird erstellt, und der Assistent wechselt auf die nächste Seite.

Nächste Schritte

Im nächsten Schritt müssen Sie den Secure Gateway-Client installieren und konfigurieren.

Anzeigen der Liste der sicheren Gateways

Nachdem Sie einen oder mehrere Gateways erstellt haben, können Sie die Liste der sicheren Gateways anzeigen, um die Eigenschaften und den Status der einzelnen Gateways zu prüfen.



Vorbereitende Schritte

Sie müssen mindestens eine Secure Gateway-Instanz erstellt haben.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Sicheres Gateway**.

   Die **Liste sicherer Gateways** wird angezeigt.

Wichtig: In den folgenden Fällen müssen Sie möglicherweise den Cache Ihres Browsers löschen:

- Wenn die folgende Nachricht angezeigt wird und Sie noch nicht die maximale Anzahl an Gateways gefunden haben, die für Ihren Benutzerlizenztyp zulässig sind:

  ```
  Die maximal zulässige Anzahl der sicheren Gateways wurde überschritten.
  ```

- Wenn der Wert für **Gateway-Verbindung** nicht aktualisiert wurde

Öffnen Sie in Firefox ein privates Fenster. Öffnen Sie in Chrome ein Incognito-Fenster.

2. Prüfen Sie den Wert für **Gateway-Verbindung** Ihres Gateways:

   - Lautet der Wert **Verbunden**, sind Sie bereit, eine Zieldatenbank hinzuzufügen.
   - Lautet der Wert **Nicht verbunden**, müssen Sie wie folgt vorgehen:
     a. Installieren Sie den Secure Gateway-Client.
     b. Konfigurieren Sie den Secure Gateway-Client für die Verbindung mit Ihrem Gateway.
   - Lautet der Wert **Token abgelaufen**, müssen Sie Ihr Token aktualisieren:
     a. Klicken Sie am Ende der Zeile für Ihr Gateway auf die Schaltfläche mit den Auslassungspunkten  .
     b. Klicken Sie auf **Eigenschaften**.
     c. Klicken Sie auf **Sicherheitstoken aktualisieren**.

     Es wird ein neues Sicherheitstoken für Ihr Secure Gateway generiert.
   - Lautet der Wert **Ungültig**, kann das Gateway nicht verwendet werden. Klicken Sie am Ende der Zeile für Ihr Gateway auf die Schaltfläche mit den Auslassungspunkten  , klicken Sie auf **Löschen** und erstellen Sie ein neues Gateway.

3. Prüfen Sie den Wert für **Status** Ihres Gateways:

   - Lautet der Wert **Aktiviert**, ist Ihr Gateway für eine Verbindung zu einer Zieldatenbank verfügbar.
   - Lautet der Wert **Inaktiviert**, ist Ihr Gateway nicht verfügbar.

     Tipp: Sie können das Gateway in Schritt „4" auf Seite 279 aktivieren.

4. Klicken Sie am Ende der Zeile für Ihr Gateway auf die Schaltfläche mit den Auslassungspunkten  und klicken Sie dann auf **Eigenschaften**.

   Die Seite **Eigenschaften für sicheres Gateway** wird angezeigt und enthält u. a. die folgenden Informationen:

   - **Gateway-ID** und **Sicherheitstoken**. Verwenden Sie diese Werte, um Ihren Secure Gateway-Client zu konfigurieren.
   - Ob eine Verbindung zu einem Secure Gateway Client vorhanden ist
   - Gateway-Status

     Tipp: Klicken Sie auf dieses Feld, um zwischen **Aktiviert** und **Inaktiviert** zu wechseln.
   - **Liste sicherer Gateway-Clients**. Klicken Sie zum Erweitern einer Secure Gateway-Clientverbindung auf die Winkelschaltfläche neben dem Namen des Client-Hosts.

Nächste Schritte

Klicken Sie zum Anzeigen der Liste der Ziele auf den Namen des Gateways.

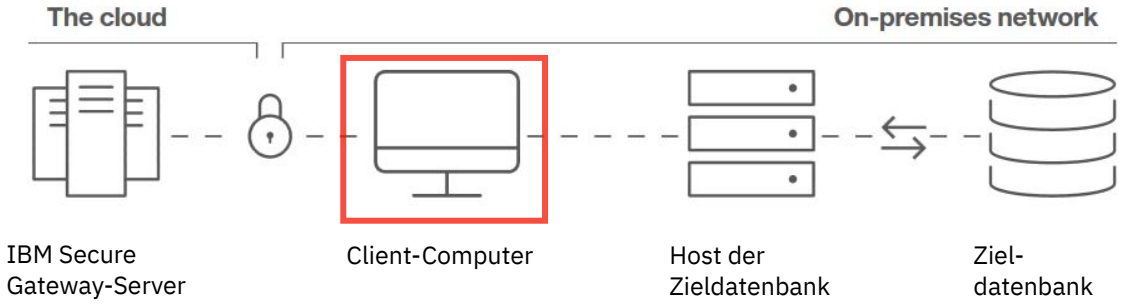
Installation und Konfiguration des Secure Gateway-Clients

Die Installation und Konfiguration des Secure Gateway-Clients ist der zweite Schritt zum Erstellen einer Verbindung zwischen dem IBM Secure Gateway-Server und Ihren lokalen Daten.

Anmerkung: Wenn Ihnen im Assistenten die Seite **Client hinzufügen** angezeigt wird, obwohl Sie den Secure Gateway-Client bereits installiert haben, gehen Sie wie folgt vor:

1. Wählen Sie die Option **Der Client ist bereits installiert** aus und klicken Sie auf **Weiter**.
2. Fahren Sie mit dem Abschnitt „Hinzufügen eines Ziels" auf Seite 289 fort.

Installieren und konfigurieren Sie den Secure Gateway-Client so, dass er sowohl mit dem IBM Secure Gateway on Cloud-Server als auch mit einer lokalen Datenbank, die Secure Gateway verwenden wird, Verbindungen herstellen kann.



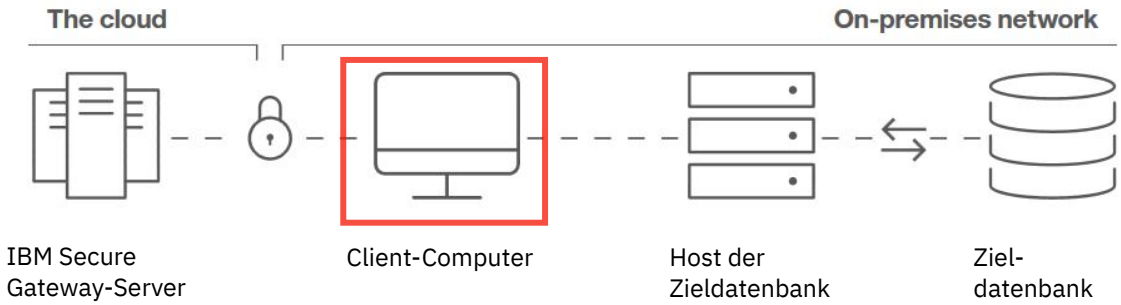
Installationsvoraussetzungen

Informationen zu den System- und Netzanforderungen finden Sie unter Voraussetzungen für die Ausführung des Clients (https: //cloud.ibm.com/docs/services/SecureGateway?topic = secureg_des_client-client-requirements).

Installation des Secure Gateway-Clients mithilfe des IBM Installationsprogramms

Sie können das IBM Installationsprogramm für die Installation des Secure Gateway-Clients auf verschiedenen Plattformen ausführen:

- AIX
- Ubuntu
- Windows
- Red Hat
- Macintosh

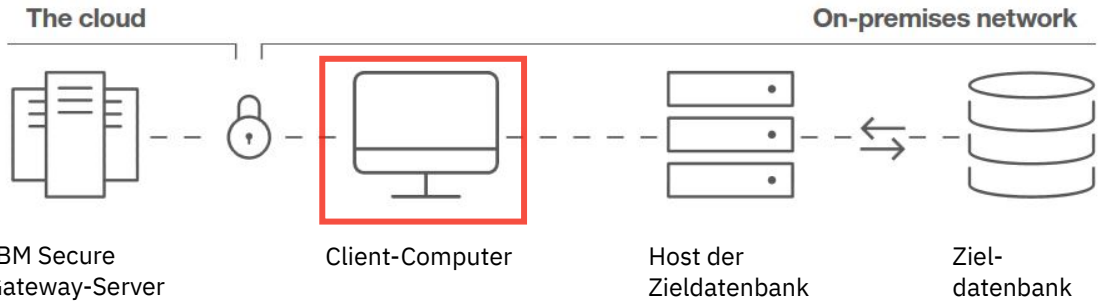


Installation unter Windows mit dem IBM Installationsprogramm

Installieren Sie unter Windows den IBM Secure Gateway-Client mithilfe des IBM Installationsprogramms.

Anmerkung: Wenn Ihnen im Assistenten die Seite **Client hinzufügen** angezeigt wird, obwohl Sie den Secure Gateway-Client bereits installiert haben, gehen Sie wie folgt vor:

1. Wählen Sie die Option **Der Client ist bereits installiert** aus und klicken Sie auf **Weiter**.
2. Fahren Sie mit dem Abschnitt „Hinzufügen eines Ziels" auf Seite 289 fort.



Vorbereitende Schritte

Installieren Sie Secure Gateway in Ihrer IT-Umgebung da, wo es die Sicherheitsrichtlinie Ihres Unternehmens zulässt. Dies ist in der Regel in einer geschützten gelben Zone oder DMZ, in der Ihr Unternehmen die entsprechenden Sicherheitskontrollen zum Schutz lokaler Ressourcen durchführen kann. Befolgen Sie immer die Sicherheitsrichtlinien und -Anweisungen Ihres Unternehmens, wenn Sie den Secure Gateway-Client installieren.

Vorgehensweise

1. Stellen Sie sicher, dass Sie eine Secure Gateway-Instanz erstellt haben.
2. Wählen Sie **IBM Installationsprogramm** und Klicken Sie auf **Weiter**.
3. Wählen Sie im Bereich **Betriebssystem** den Eintrag **Windows** aus.
4. Klicken Sie auf **Download-Client**.
5. Folgen Sie den Eingabeaufforderungen, um den IBM Client zu installieren.
6. Kopieren Sie die Werte für **Gateway-ID** und **Sicherheitstoken** zur späteren Verwendung in eine Textdatei.

   Tipp: Sie benötigen diese Werte, wenn Sie den Client konfigurieren.
7. Klicken Sie auf **Weiter**.

   Der Secure Gateway-Client wird installiert und konfiguriert, und der Assistent wechselt auf die nächste Seite.

Nächste Schritte

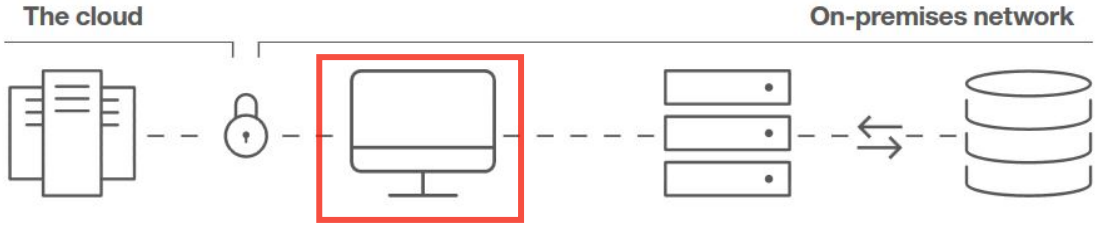
Im nächsten Schritt müssen Sie eine lokale Zieldatenbank hinzufügen.

Installation unter AIX mit dem IBM Installationsprogramm

Installieren Sie unter AIX den IBM Secure Gateway-Client mithilfe des IBM Installationsprogramms.

Anmerkung: Wenn Ihnen im Assistenten die Seite **Client hinzufügen** angezeigt wird, obwohl Sie den Secure Gateway-Client bereits installiert haben, gehen Sie wie folgt vor:

1. Wählen Sie die Option **Der Client ist bereits installiert** aus und klicken Sie auf **Weiter**.
2. Fahren Sie mit dem Abschnitt „Hinzufügen eines Ziels" auf Seite 289 fort.



Vorbereitende Schritte

Installieren Sie Secure Gateway in Ihrer IT-Umgebung da, wo es die Sicherheitsrichtlinie Ihres Unternehmens zulässt. Dies ist in der Regel in einer geschützten gelben Zone oder DMZ, in der Ihr Unternehmen die entsprechenden Sicherheitskontrollen zum Schutz lokaler Ressourcen durchführen kann. Befolgen Sie immer die Sicherheitsrichtlinien und -Anweisungen Ihres Unternehmens, wenn Sie den Secure Gateway-Client installieren.

Vorgehensweise

1. Stellen Sie sicher, dass Sie eine Secure Gateway-Instanz erstellt haben.
2. Wählen Sie **IBM Installationsprogramm** und Klicken Sie auf **Weiter**.
3. Wählen Sie im Bereich **Betriebssystem** den Eintrag **AIX** aus.
4. Klicken Sie auf **Download-Client**.
5. Folgen Sie den Eingabeaufforderungen, um den IBM Client zu installieren.
6. Kopieren Sie die Werte für **Gateway-ID** und **Sicherheitstoken** zur späteren Verwendung in eine Textdatei.

   Tipp: Sie benötigen diese Werte, wenn Sie den Client konfigurieren.
7. Klicken Sie auf **Weiter**.

   Der Secure Gateway-Client wird installiert und konfiguriert, und der Assistent wechselt auf die nächste Seite.

Nächste Schritte

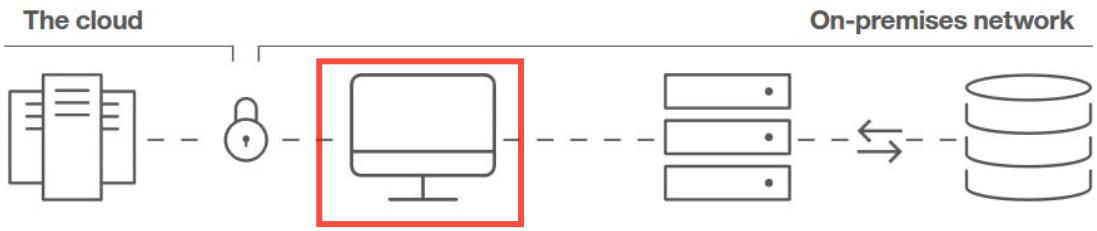
Im nächsten Schritt müssen Sie eine lokale Zieldatenbank hinzufügen.

Installation unter Ubuntu mit dem IBM Installationsprogramm

Installieren Sie unter Ubuntu den IBM Secure Gateway-Client mithilfe des IBM Installationsprogramms.

Anmerkung: Wenn Ihnen im Assistenten die Seite **Client hinzufügen** angezeigt wird, obwohl Sie den Secure Gateway-Client bereits installiert haben, gehen Sie wie folgt vor:

1. Wählen Sie die Option **Der Client ist bereits installiert** aus und klicken Sie auf **Weiter**.
2. Fahren Sie mit dem Abschnitt „Hinzufügen eines Ziels” auf Seite 289 fort.



Vorbereitende Schritte

Installieren Sie Secure Gateway in Ihrer IT-Umgebung da, wo es die Sicherheitsrichtlinie Ihres Unternehmens zulässt. Dies ist in der Regel in einer geschützten gelben Zone oder DMZ, in der Ihr Unternehmen die entsprechenden Sicherheitskontrollen zum Schutz lokaler Ressourcen durchführen kann. Befolgen Sie immer die Sicherheitsrichtlinien und -Anweisungen Ihres Unternehmens, wenn Sie den Secure Gateway-Client installieren.

Vorgehensweise

1. Stellen Sie sicher, dass Sie eine Secure Gateway-Instanz erstellt haben.
2. Wählen Sie **IBM Installationsprogramm** und Klicken Sie auf **Weiter**.
3. Wählen Sie im Bereich **Betriebssystem** den Eintrag **Ubuntu** aus.
4. Klicken Sie auf **Download-Client**.
5. Folgen Sie den Eingabeaufforderungen, um den IBM Client zu installieren.
6. Kopieren Sie die Werte für **Gateway-ID** und **Sicherheitstoken** zur späteren Verwendung in eine Textdatei.

   Tipp: Sie benötigen diese Werte, wenn Sie den Client konfigurieren.
7. Klicken Sie auf **Weiter**.

   Der Secure Gateway-Client wird installiert und konfiguriert, und der Assistent wechselt auf die nächste Seite.

Nächste Schritte

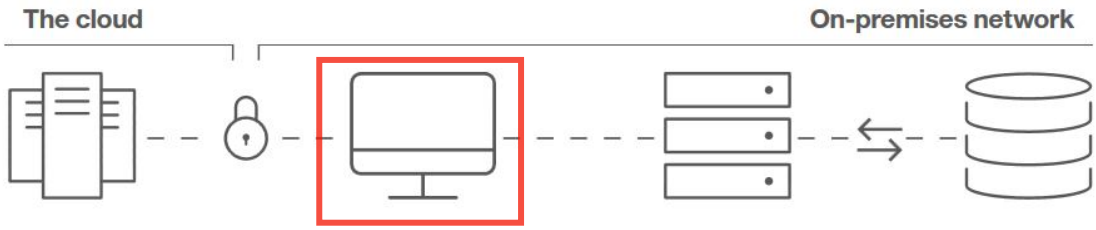
Im nächsten Schritt müssen Sie eine lokale Zieldatenbank hinzufügen.

Installation unter Red Hat mit dem IBM Installationsprogramm

Installieren Sie unter Red Hat den IBM Secure Gateway-Client mithilfe des IBM Installationsprogramms.

Anmerkung: Wenn Ihnen im Assistenten die Seite **Client hinzufügen** angezeigt wird, obwohl Sie den Secure Gateway-Client bereits installiert haben, gehen Sie wie folgt vor:

1. Wählen Sie die Option **Der Client ist bereits installiert** aus und klicken Sie auf **Weiter**.
2. Fahren Sie mit dem Abschnitt „Hinzufügen eines Ziels" auf Seite 289 fort.



Vorbereitende Schritte

Installieren Sie Secure Gateway in Ihrer IT-Umgebung da, wo es die Sicherheitsrichtlinie Ihres Unternehmens zulässt. Dies ist in der Regel in einer geschützten gelben Zone oder DMZ, in der Ihr Unternehmen die entsprechenden Sicherheitskontrollen zum Schutz lokaler Ressourcen durchführen kann. Befolgen Sie immer die Sicherheitsrichtlinien und -Anweisungen Ihres Unternehmens, wenn Sie den Secure Gateway-Client installieren.

Vorgehensweise

1. Stellen Sie sicher, dass Sie eine Secure Gateway-Instanz erstellt haben.
2. Wählen Sie **IBM Installationsprogramm** und Klicken Sie auf **Weiter**.

3. Wählen Sie im Bereich **Betriebssystem** den Eintrag **Red Hat** aus.
4. Klicken Sie auf **Download-Client**.
5. Folgen Sie den Eingabeaufforderungen, um den IBM Client zu installieren.
6. Kopieren Sie die Werte für **Gateway-ID** und **Sicherheitstoken** zur späteren Verwendung in eine Textdatei.

   Tipp: Sie benötigen diese Werte, wenn Sie den Client konfigurieren.
7. Klicken Sie auf **Weiter**.

   Der Secure Gateway-Client wird installiert und konfiguriert, und der Assistent wechselt auf die nächste Seite.

Nächste Schritte

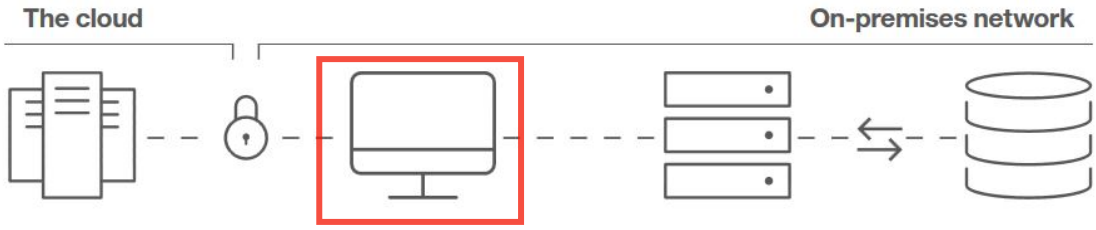
Im nächsten Schritt müssen Sie eine lokale Zieldatenbank hinzufügen.

Installation unter Macintosh mit dem IBM Installationsprogramm

Installieren Sie unter Macintosh den IBM Secure Gateway-Client mithilfe des IBM Installationsprogramms.

Anmerkung: Wenn Ihnen im Assistenten die Seite **Client hinzufügen** angezeigt wird, obwohl Sie den Secure Gateway-Client bereits installiert haben, gehen Sie wie folgt vor:

1. Wählen Sie die Option **Der Client ist bereits installiert** aus und klicken Sie auf **Weiter**.
2. Fahren Sie mit dem Abschnitt „Hinzufügen eines Ziels" auf Seite 289 fort.



Vorbereitende Schritte

Installieren Sie Secure Gateway in Ihrer IT-Umgebung da, wo es die Sicherheitsrichtlinie Ihres Unternehmens zulässt. Dies ist in der Regel in einer geschützten gelben Zone oder DMZ, in der Ihr Unternehmen die entsprechenden Sicherheitskontrollen zum Schutz lokaler Ressourcen durchführen kann. Befolgen Sie immer die Sicherheitsrichtlinien und -Anweisungen Ihres Unternehmens, wenn Sie den Secure Gateway-Client installieren.

Vorgehensweise

1. Stellen Sie sicher, dass Sie eine Secure Gateway-Instanz erstellt haben.
2. Wählen Sie **IBM Installationsprogramm** und Klicken Sie auf **Weiter**.
3. Wählen Sie im Bereich **Betriebssystem** den Eintrag **Macintosh** aus.
4. Klicken Sie auf **Download-Client**.
5. Folgen Sie den Eingabeaufforderungen, um den IBM Client zu installieren.
6. Kopieren Sie die Werte für **Gateway-ID** und **Sicherheitstoken** zur späteren Verwendung in eine Textdatei.

   Tipp: Sie benötigen diese Werte, wenn Sie den Client konfigurieren.
7. Klicken Sie auf **Weiter**.

Der Secure Gateway-Client wird installiert und konfiguriert, und der Assistent wechselt auf die nächste Seite.

Nächste Schritte

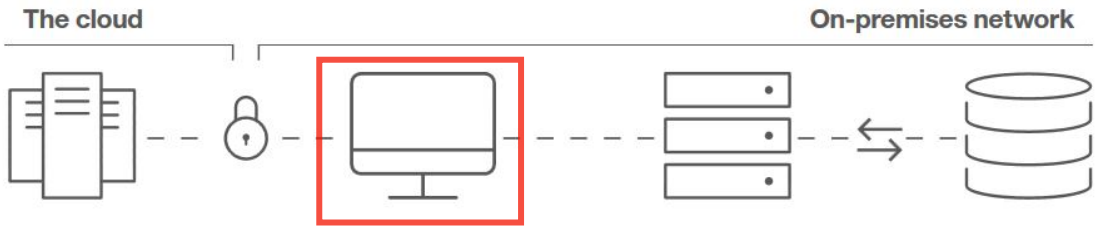
Im nächsten Schritt müssen Sie eine lokale Zieldatenbank hinzufügen.

Installation eines Docker-Images, in dem der Secure Gateway-Client enthalten ist

Anstatt das IBM Installationsprogramm für die Installation des Secure Gateway-Clients zu verwenden, können Sie ein Docker-Image installieren, das den Secure Gateway-Client enthält.

Anmerkung: Wenn Ihnen im Assistenten die Seite **Client hinzufügen** angezeigt wird, obwohl Sie den Secure Gateway-Client bereits installiert haben, gehen Sie wie folgt vor:

1. Wählen Sie die Option **Der Client ist bereits installiert** aus und klicken Sie auf **Weiter**.
2. Fahren Sie mit dem Abschnitt „Hinzufügen eines Ziels" auf Seite 289 fort.



Vorgehensweise

1. Stellen Sie sicher, dass Sie eine Secure Gateway-Instanz erstellt haben.
2. Wählen Sie **Docker installieren** aus und folgen Sie den Eingabeaufforderungen.

   Weitere Informationen finden Sie unter Informationen zu Docker CE (https://docs.docker.com/install/).

   Tipp: Unter Linux können Sie `-h `hostname`` zu Ihrer Docker-Bash-Shell hinzufügen. Dadurch wird anstelle der Docker-ID das System zurückgegeben, auf dem Docker gehostet wird.
3. Öffnen Sie ein Befehlsfenster.
4. Kopieren Sie den Docker-Pull-Befehl und führen Sie ihn aus.
5. Kopieren Sie den Docker-Ausführungsbefehl mit dem Sicherheitstoken und führen Sie ihn aus.
6. Klicken Sie auf **Weiter**.

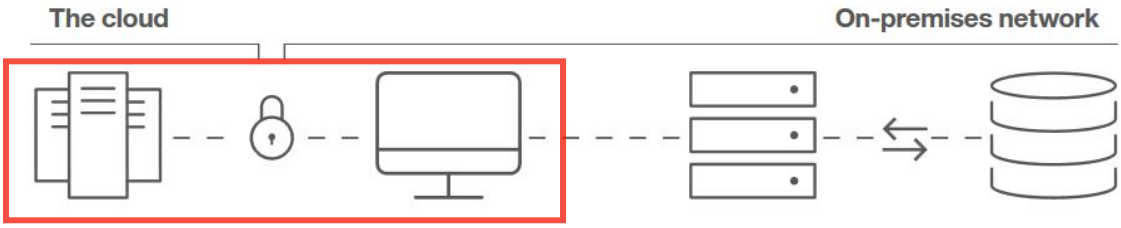
   Der Secure Gateway-Client wird installiert und konfiguriert, und der Assistent wechselt auf die nächste Seite.

Nächste Schritte

Im nächsten Schritt müssen Sie eine lokale Zieldatenbank hinzufügen.

Konfiguration des Secure Gateway-Clients

Konfigurieren Sie Ihren Secure Gateway-Client so, dass eine Verbindung zu Ihrer Secure Gateway-Instanz hergestellt wird.

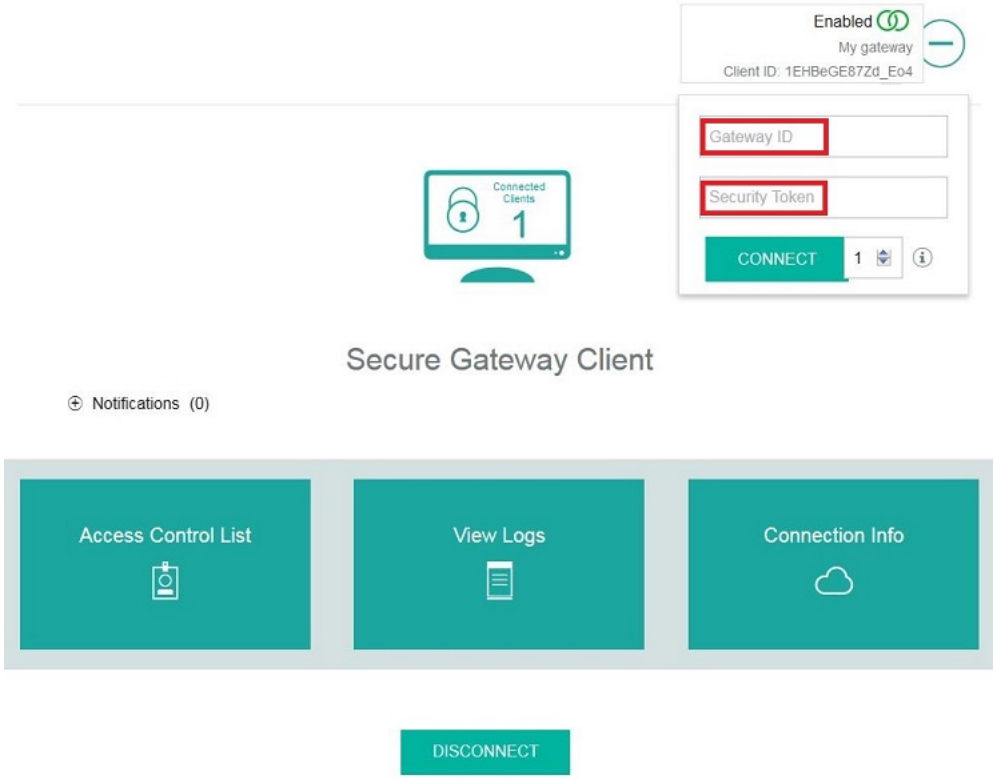


IBM Secure Gateway-Server | Client-Computer | Host der Zieldatenbank | Ziel-datenbank

Vorgehensweise

1. Starten Sie den Secure Gateway-Client, den Sie auf Ihrem lokalen Computer installiert haben.
2. Klicken Sie in der oberen rechten Ecke des Fensters des Secure Gateway-Clients auf das Pluszeichen  .

   Sie werden aufgefordert, die **Gateway-ID** und das **Sicherheitstoken** einzugeben.



3. Geben Sie die Werte für **Gateway-ID** und **Sicherheitstoken** aus der Eigenschaftenseite ein, wenn Sie die **Liste sicherer Gateways** anzeigen.
4. Klicken Sie auf **VERBINDEN**.
5. Wechseln Sie auf die Seite **Liste sicherer Gateways**.

   Es wird der Status **Nicht verbunden** angezeigt.
6. Klicken Sie auf **Aktualisieren**.

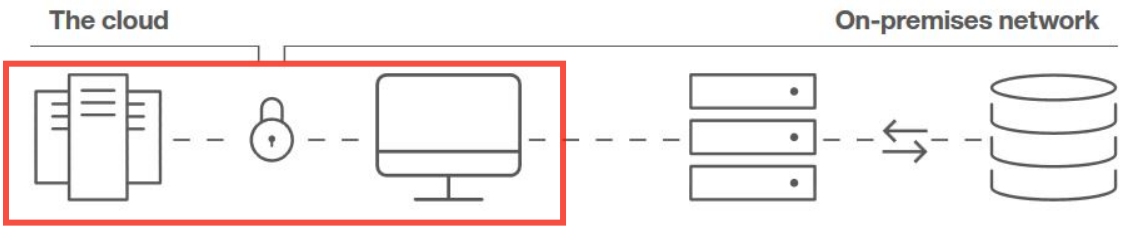
   Der Status ändert sich in **Verbunden**. Dies bestätigt, dass Ihr Secure Gateway-Client mit Ihrer Secure Gateway-Instanz in der Cloud verbunden ist.

Nächste Schritte

Sie können jetzt eine Verbindung zu einem Ziel herstellen oder die Eigenschaften Ihres Secure Gateway-Clients anzeigen.

Anzeigen der Eigenschaften des Secure Gateway-Clients

Nachdem Sie eine Secure Gateway-Instanz erstellt und eine oder mehrere Instanzen des Secure Gateway-Clients mit dieser Instanz verbunden haben, können Sie die Eigenschaften des Secure Gateway-Clients anzeigen. Auf diese Weise können Sie die Gateway-Client-Verbindung überprüfen oder Probleme beheben.



Vorbereitende Schritte

Sie müssen mindestens eine Secure Gateway-Instanz erstellt und mindestens eine Secure Gateway-Client-Verbindung konfiguriert haben.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Sicheres Gateway**.

   Die **Liste sicherer Gateways** wird angezeigt.
2. Klicken Sie am Ende der Zeile für Ihr Gateway auf die Schaltfläche mit den Auslassungspunkten  und klicken Sie dann auf **Eigenschaften**.

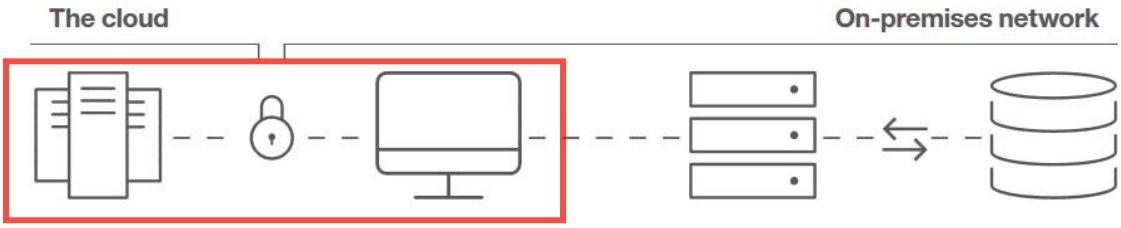
   Die Seite **Eigenschaften für sicheres Gateway** wird angezeigt. Unten befindet sich eine Liste aller **Secure Gateway-Client**-Verbindungen zum aktuellen Gateway.
3. Klicken Sie zum Erweitern einer Secure Gateway-Clientverbindung auf die Winkelschaltfläche neben dem Namen des Client-Hosts.

   Clienteigenschaften wie dessen Verbindungsstatus und die Client-ID werden angezeigt.
4. Klicken Sie zum Überprüfen der Leistung Ihrer Secure Gateway-Client-Server-Verbindung auf **Latenztest**.
5. Klicken Sie zum Beheben von Problemen der Client-Server-Verbindung auf **Clientprotokolle anzeigen**.

Latenztest

Sie können einen Latenztest für Ihre Secure Gateway-Client-Server-Verbindung ausführen. Dieser Test misst, wie lange Daten brauchen, um zwischen Ihrem lokalen Secure Gateway-Client und dem cloudbasierten Secure Gateway-Server hin- und herzugelangen.

Weitere Informationen finden Sie unter Informationen zur Latenz (https://cloud.ibm.com/docs/infrastructure/direct-link?topic=direct-link-understanding-latency).



Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Sicheres Gateway**.

   Die **Liste sicherer Gateways** wird angezeigt.

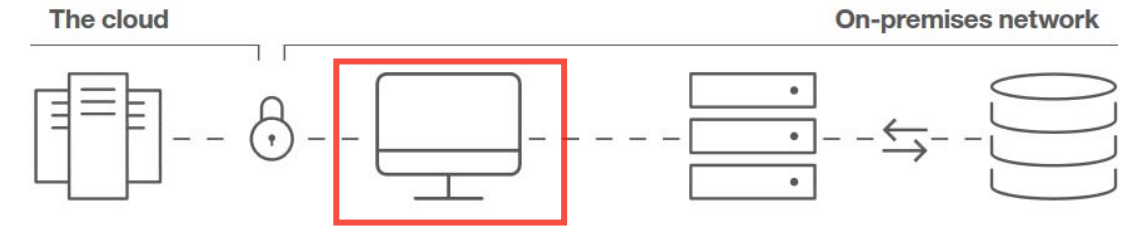
   Tipp: Wenn Sie gerade Ihre Verbindung abgeschlossen haben, aber der Wert für **Gateway-Verbindung** für Ihr Gateway **Nicht verbunden** lautet, klicken Sie auf **Aktualisieren**, um den Wert auf **Verbunden** zu aktualisieren.
2. Klicken Sie am Ende der Zeile für Ihr Gateway auf die Schaltfläche mit den Auslassungspunkten und klicken Sie dann auf **Eigenschaften**.
3. Erweitern Sie unten auf der Seite **Eigenschaften für sicheres Gateway** im Bereich **Secure Gateway-Client** den Namen des Computers, auf dem Sie den Secure Gateway-Client installiert haben.
4. Klicken Sie auf **Latenztest**.

Ergebnisse

Die Zeit für die Server-Client-Latenz und für die Client-Server-Latenz wird angezeigt (jeweils in Millisekunden).

Clientprotokolle

In Clientprotokollen werden Ereignisse aufgezeichnet, die sich auf die Verbindung zwischen dem IBM Secure Gateway-Client und dem IBM Secure Gateway-Server beziehen.



Anzeigen von Protokollnachrichten

Führen Sie die folgenden Schritte aus, um die Protokollnachrichten anzuzeigen:

1. Klicken Sie auf **Verwalten** > **Sicheres Gateway**.

   Die **Liste sicherer Gateways** wird angezeigt.

   Tipp: Wenn Sie gerade Ihre Verbindung abgeschlossen haben, aber der Wert für **Gateway-Verbindung** für Ihr Gateway **Nicht verbunden** lautet, klicken Sie auf **Aktualisieren**, um den Wert auf **Verbunden** zu aktualisieren.

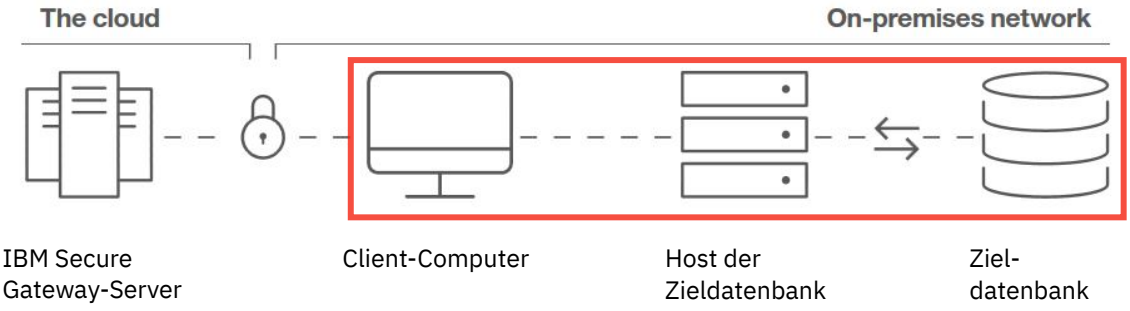
2. Klicken Sie am Ende der Zeile für Ihr Gateway auf die Schaltfläche mit den Auslassungspunkten  und klicken Sie dann auf **Eigenschaften**.
3. Erweitern Sie unten auf der Seite **Eigenschaften für sicheres Gateway** im Bereich **Secure Gateway-Client** den Namen des Computers, auf dem Sie den Secure Gateway-Client installiert haben.
4. Klicken Sie auf **Clientprotokolle anzeigen**.

Wenn eine Protokollnachricht unklar ist, fragen Sie Ihren Administrator, welche Aktionen Sie möglicherweise ausführen sollten.

Hinzufügen eines Ziels

Das Hinzufügen eines Ziels ist der **dritte** Schritt zum Erstellen einer Verbindung zwischen dem IBM Secure Gateway-Server und Ihren lokalen Daten.

Fügen Sie ein Ziel hinzu, um die lokale Datenbank zu definieren, die Sie Ihrem Gateway zuordnen.



Vorgehensweise

1. Stellen Sie sicher, dass Sie Ihren IBM Secure Gateway-Client installiert und konfiguriert haben.

   Wenn Sie nach der Installation und Konfiguration des Secure Gateway-Clients auf **Weiter** geklickt haben, wird die Seite **Ziel hinzufügen** angezeigt.
2. Wenn Sie den Secure Gateway-Client zuvor installiert und konfiguriert und anschließend den Assistenten beendet haben, führen Sie die folgenden Schritte aus:
   a) Klicken Sie auf **Verwalten** > **Sicheres Gateway**.
   b) Klicken Sie auf der Seite **Liste sicherer Gateways** auf Ihr Gateway.
   c) Klicken Sie auf der Seite **Zielliste** auf die Schaltfläche 'Ziel hinzufügen' ⊕.

   Die Seite **Ziel hinzufügen** wird angezeigt.
3. Geben Sie einen Namen für Ihr Ziel ein.

   Tipp: Binden Sie den Datenbanktyp in den Namen ein.
4. Geben Sie den Namen des Computers und die Portnummer für Ihre Datenbank ein.
5. Klicken Sie auf **Weiter**.

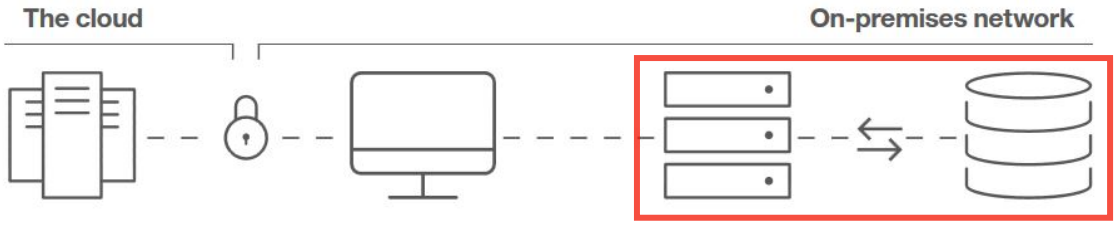
   Das Ziel wird hinzugefügt und wird auf der Zielliste angezeigt, wenn Sie sie das nächste Mal anzeigen.

Nächste Schritte

Im nächsten Schritt müssen Sie gültige Zieldatenbanken angeben, auf die über das sichere Gateway zugegriffen werden kann.

Anzeigen der Zielliste

Nachdem Sie ein oder mehrere Ziele erstellt haben, können Sie die Liste der Ziele anzeigen, um die Eigenschaften und den Status der einzelnen Ziele zu prüfen.



Vorbereitende Schritte

Sie müssen mindestens ein Ziel hinzugefügt haben.

Vorgehensweise

1. Führen Sie die Schritte zum Anzeigen der Liste sicherer Gateways aus.
2. Klicken Sie in der Liste der sicheren Gateways auf den Namen des Gateways.

   Die **Liste der Ziele** wird angezeigt.
3. Prüfen Sie den Wert für **Zielverbindung** Ihres Ziels:

   Wichtig: Möglicherweise müssen Sie den Cache Ihres Browsers löschen, bevor der Wert für **Zielverbindung** aktualisiert wird. Öffnen Sie in Firefox ein privates Fenster. Öffnen Sie in Chrome ein Incognito-Fenster.

   - Lautet der Wert **Verbunden**, besteht eine Verbindung zum Zielhost.
   - Lautet der Wert **Blockiert durch ACL**, klicken Sie auf den Link **Blockiert durch ACL**, um die Zugriffssteuerungsliste für Ihr Ziel zu konfigurieren.
   - Lautet der Wert **Ungültig**, gibt es zwei Möglichkeiten:
     a. Der Secure Gateway-Service ist möglicherweise vorübergehend nicht verfügbar. In diesem Fall ist die Zielverbindung noch immer gültig und sie wird als **Verbunden** angezeigt, wenn der Service wieder verfügbar ist. Wenn Ihre Zielverbindung ursprünglich gültig war, prüfen Sie die Liste der Ziele später. Anschließend können Sie prüfen, ob der Zielverbindungswert nicht mehr ungültig ist und ob der Secure Gateway-Service daher wieder aktiv ist.
     b. Das Ziel kann nicht verwendet werden. Klicken Sie am Ende der Zeile für Ihr Ziel auf die Schaltfläche mit den Auslassungspunkten, klicken Sie auf **Löschen** und fügen Sie ein neues Ziel hinzu.
4. Prüfen Sie den Wert für **Status** Ihres Ziels:

   - Lautet der Wert **Aktiviert**, ist Ihr Ziel für eine Verbindung zu einem sicheren Gateway verfügbar.
   - Lautet er **Inaktiviert**, ist Ihr Ziel nicht verfügbar.

     Tipp: Sie können das Ziel in Schritt „5" auf Seite 290 aktivieren.
5. Klicken Sie am Ende der Zeile für Ihr Ziel auf die Schaltfläche mit den Auslassungspunkten und klicken Sie dann auf **Eigenschaften**.

   Die Seite **Zieleigenschaften** wird angezeigt und enthält u. a. die folgenden Informationen:

   - Hostname und Portnummer des Ziels. Verwenden Sie diesen Wert, wenn Sie eine Datenserververbindung auf dem Zielcomputer erstellen.
   - Status des Ziels

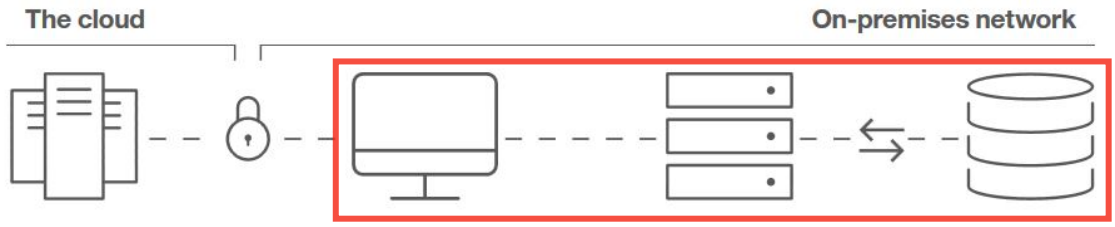
Tipp: Klicken Sie auf dieses Feld, um zwischen **Aktiviert** und **Inaktiviert** zu wechseln.

- **Liste mit Datenserververbindungen**. Klicken Sie auf die Winkelschaltfläche >, um alle Datenserververbindungen aufzulisten, die Sie bereits erstellt haben.

Herstellen einer Verbindung zu einer lokalen Zieldatenbank

Das Herstellen einer Verbindung zu einer lokalen Zieldatenbank ist der **vierte** Schritt zum Erstellen einer Verbindung zwischen dem IBM Secure Gateway-Server und Ihren lokalen Daten.

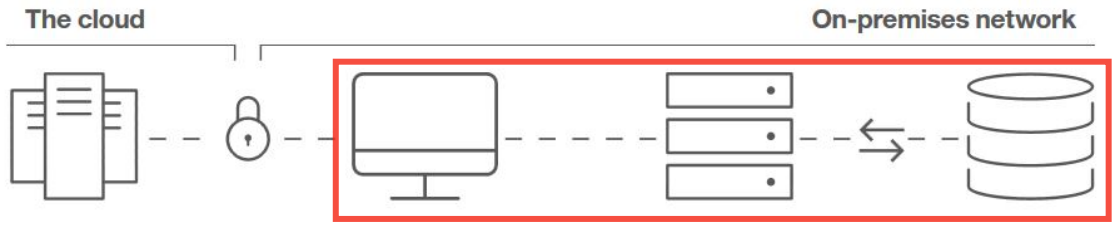
Verbinden Sie den Secure Gateway Client mit einer Zieldatenbank, um die sichere gemeinsame Nutzung von On-Premises-Daten mit Cognos Analytics on Cloud on Demand zu ermöglichen.



IBM Secure Gateway-Server | Client-Computer | Host der Zieldatenbank | Ziel-datenbank

Angeben der Datenbanken im Zugriff

Bearbeiten Sie die IBM Secure Gateway-Zugriffssteuerungsliste (ACL) so, dass Ihre lokale Datenbank als gültige Zieldatenbank für Ihre Secure Gateway-Instanz angegeben wird. Auf diese Weise können Sie sicher auf Ihre On-Premises-Daten in IBM Cognos Analytics on Demand zugreifen.



IBM Secure Gateway-Server | Client-Computer | Host der Zieldatenbank | Ziel-datenbank

Bei der ACL handelt es sich um eine Datei, in der Sie die Namen und Portnummern der Computer auflisten, die berechtigt sind, Ihre lokalen Daten über das sichere Gateway zu hosten.

Ausführlichere Informationen finden Sie im Abschnitt Zugriffssteuerungsliste (https://cloud.ibm.com/docs/services/SecureGateway?topic=securegateway-acl).

Bearbeitung der Zugriffssteuerungsliste

Führen Sie die folgenden Schritte aus, wenn Sie die Befehlszeilenschnittstelle (**Option 1**) verwenden möchten:

1. Öffnen Sie ein Befehlsfenster.
2. Führen Sie den folgenden Befehl aus:

   `acl allow` *`Datenbankhostname:Portnummer`*

   Dabei ist *Datenbankhostname* der Name des Computers, auf dem sich die Datenbank befindet, und *Portnummer* ist die Portnummer der Datenbank.
3. Klicken Sie im Assistenten **Verbindung zu einer lokalen Datenbank herstellen** auf **OK**.

Führen Sie die folgenden Schritte aus, wenn Sie die Schnittstelle des Secure Gateway-Clients (**Option 2**) verwenden möchten:

1. Starten Sie den Secure Gateway-Client auf Ihrem lokalen Computer.
2. Klicken Sie auf **Zugriffssteuerungsliste**.
3. Geben Sie unter **Zugriff zulassen** den Hostnamen und den Port des Zielcomputers ein.
4. Klicken Sie im Assistenten **Verbindung zu einer lokalen Datenbank herstellen** auf **OK**.

Nächste Schritte

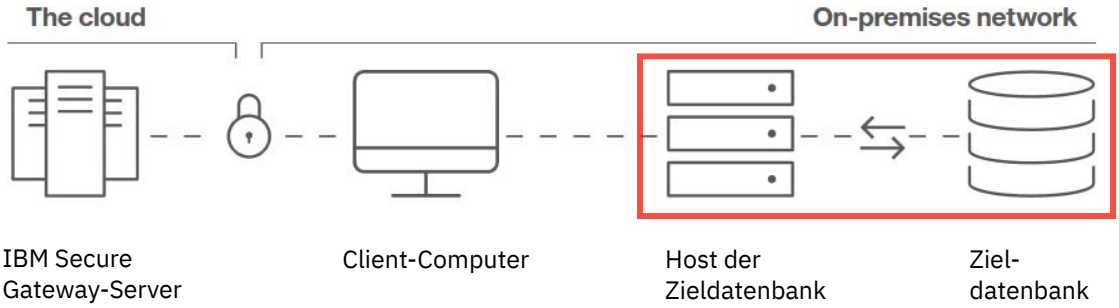
Im nächsten Schritt müssen Sie eine Datenserververbindung auf dem Zielcomputer erstellen.

Tipp: Möglicherweise haben Sie bereits eine Datenserververbindung eingerichtet, die Sie für Ihre Zieldatenbank verwenden können.

Herstellen einer Datenserververbindung auf dem Zielcomputer

Eine Datenserververbindung gibt die Parameter an, die zum Herstellen einer Verbindung mit der Zieldatenbank Ihrer Secure Gateway-Instanz erforderlich sind.

Anmerkung: Für Verbindungen mit Secure Gateway-Datenservern können nur relationale Datenbanken verwendet werden.



Jeder Datenserver kann über eine oder mehrere Verbindungen verfügen. Die Verbindungsnamen müssen eindeutig sein.

Informationen zu Datenserververbindungen, die nicht als Secure Gateway-Ziele verwendet werden, finden Sie unter „Datenserver” auf Seite 25.

Vorgehensweise

1. Klicken Sie auf **Verwalten** > **Datenserververbindungen**.
2. Klicken Sie im Fensterbereich **Datenserververbindungen** auf das Symbol **Datenserver hinzufügen** .
3. Wählen Sie den Datenservertyp in der Liste der unterstützten Typen aus.

   Tipp: Sie müssen einen relationalen Datenservertyp auswählen.
4. Geben Sie im Feld **Neue Datenserververbindung** einen eindeutigen Namen für die Verbindung ein.
5. Klicken Sie neben **Verbindungsdetails** auf **Bearbeiten** und geben Sie die Verbindungsdetails für den Typ der Verbindung ein, die Sie erstellen.

   Geben Sie die JDBC-URL an. Unter den Verbindungsdetails können Sie die Syntax und eine Beispiel-URL anzeigen. Möglicherweise müssen Sie sich an den Datenbankadministrator wenden, um weitere Details zu erhalten, oder die Informationen in der Dokumentation des Datenbankanbieter lesen.

   Wichtig: Die JDBC-URL darf nur einen einzigen Hostnamen und nur eine einzige statische Portnummer enthalten.

6. Wählen Sie im Fenster ***Datenservertyp*-Verbindung bearbeiten** im Bereich **Ziel für sicheres Gateway** die von Ihnen erstellten Gateway- und Zielnamen aus.
7. Geben Sie unter **Authentifizierungsmethode** an, wie auf den Datenserver zugegriffen werden soll.

   Sie können eine der nachfolgend aufgeführten Optionen auswählen.

   'Anonyme Verbindung herstellen' oder 'Integrierte Sicherheit'

   Wählen Sie die Option **Anonyme Verbindung herstellen**, wenn der anonyme Zugriff auf den Datenserver zulässig ist.

   Zur Eingabe der Benutzer-ID und des Kennworts auffordern

   Wählen Sie diese Option aus, wenn der Benutzer bei jeder Anmeldung zur Eingabe der Datenbank-Berechtigungsnachweise aufgefordert werden soll.

   Externen Namespace verwenden

   Wählen Sie diese Option aus, um die Verbindung gegen einen Namespace zu schützen, der für Cognos Analytics konfiguriert ist. Wählen Sie einen der verfügbaren Namespaces über das Dropdown-Menü aus.

   Die folgende Anmeldung verwenden

   Wählen Sie diese Option, um eine Anmeldung für die Verbindung zuzuweisen.

   Wählen Sie die Anmeldung in der Dropdown-Liste aus oder erstellen Sie eine neue Anmeldung, indem Sie auf das Symbol 'Hinzufügen' klicken. Geben Sie im Fenster **Neue Datenserververbindung** auf der Registerkarte **Berechtigungsnachweise** eine Benutzer-ID und ein Kennwort ein.

   Um die Anmeldung auf bestimmte Benutzer, Rollen oder Gruppen zu beschränken, klicken Sie auf der Registerkarte **Berechtigungen** auf das Symbol 'Hinzufügen' und geben die Zugriffsberechtigungen für die Anmeldung an.
8. Klicken Sie auf **Testen**, um die Datenserververbindung zu überprüfen, und anschließend auf **Speichern**, um die neue Datenserververbindung zu speichern.

Ergebnisse

Der neue Verbindungsname wird im Fenster **Datenserververbindungen** angezeigt. Sie können die Datenserververbindung bearbeiten, beispielsweise durch Hinzufügen oder Ändern der entsprechenden Anmeldung, indem Sie auf ihren Namen klicken.

Nächste Schritte

Sie sind nun bereit, Cognos Analytics on Demand mit Ihren On-Premises-Daten zu verwenden.

Weitere Informationen finden Sie in der Veröffentlichung *Cognos Analytics - Datenmodellierung*.

Framework Manager for Cognos Analytics on Demand installieren und konfigurieren

Framework Manager kann nur dann zusammen mit dem IBM Cognos Analytics on Demand-Angebot verwendet werden, wenn der Kunde über S&S (Support & Subscription, Support und Abonnement) für das On-Premises-Angebot verfügt. Andernfalls ist Framework Manager nicht mit dem on Demand-Angebot verfügbar.

Für Framework Manager müssen die folgenden Bedingungen erfüllt sein, um eine Verbindung zum Cognos Analytics on Demand-Angebot herzustellen:

- Sie benötigen eine Berechtigung für die On-Premises-Framework Manager-Software.

  Weitere Informationen finden Sie unter "Cognos Analytics-Angebote" im Handbuch *IBM Cognos Analytics - Erste Schritte*.

- Der dynamische Abfragemodus (DQM) muss in Framework Manager aktiviert sein.

  Der kompatible Abfragemodus (CQM) wird in der Cloud nicht unterstützt.
- Datenquellenverbindungen müssen über die Verwaltungsschnittstelle **Verwalten** von Cognos Analytics erstellt werden.

  Datenquellenverbindungen, die in Framework Manager erstellt werden, sind in der Benutzerschnittstelle **Verwalten** nicht sichtbar. Weitere Informationen finden Sie unter "Datenserververbindung erstellen" im Handbuch *IBM Cognos Analytics - Verwaltung*.

Vorbereitende Schritte

Cognos Analytics on Demand weist immer das neueste Release auf. Überprüfen Sie als bewährtes Verfahren IBM Fix Central (www.ibm.com/support/fixcentral) zuerst, um festzustellen, ob es eine Version von Framework Manager für die aktuelle Version von Cognos Analytics on Demand gibt. Wenn nicht, laden Sie die allgemeine Release-Version von Framework Manager von Passport Advantage (www.ibm.com/software/passportadvantage/index.html) herunter.

Vorgehensweise

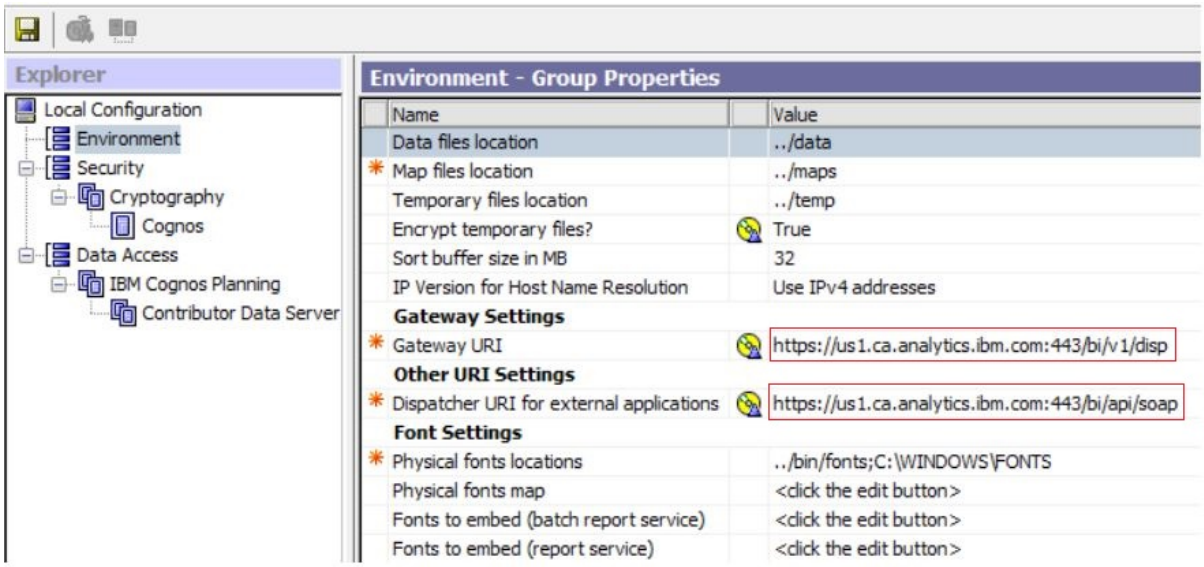
1. Laden Sie die neueste Version der Framework Manager-Installationsdateien von Passport Advantage für allgemeine Releases oder von Fix Central für einen vorläufigen Fix herunter.

   Die Namen der Dateien, die Sie herunterladen müssen, verwenden das Format `analytics-installer-x.x.xxxxxxxx-win.exe` und `caclient-xx.x.x-xxxxxxxxxx.zip`. Ein Beispiel für Dateinamen für die Version 11.1.7 von Cognos Analytics on Demand ist `analytics-installer-2.0.20100517-win.exe` und `caclient-11.1.7-2101190846.zip`.
2. Führen Sie die Installationsdatei `analytics-installer-x.x.xxxxxxxx-win.exe` aus.
3. Wählen Sie im Installationsassistenten eine Sprache aus und klicken Sie auf **Weiter**.
4. Navigieren Sie zu den heruntergeladenen Clientinstallationsmedien und klicken Sie auf **Weiter**.
5. Wählen Sie **Cognos Analytics-Tools** aus und klicken Sie auf **Weiter**.
6. Wählen Sie **IBM Cognos Framework Manager** aus, klicken Sie auf **Weiter**, akzeptieren Sie die Lizenzvereinbarung und klicken Sie erneut auf **Weiter** .
7. Legen Sie die Installationsposition und den Verknüpfungsordner fest und klicken Sie auf **Weiter**. Befolgen Sie die restlichen Anweisungen im Assistenten, um Framework Manager zu installieren.
8. Starten Sie IBM Cognos Configuration for Framework Manager.
9. Klicken Sie im Fenster **Explorer** auf **Umgebung**.
10. Legen Sie im Teilfenster **Eigenschaften** die Option **Temporäre Dateien verschlüsseln** auf 'True' (als bewährtes Verfahren) fest.
11. Legen Sie die Eigenschaften wie folgt fest:

    Gateway-URI
    Setzen Sie diese Eigenschaft auf `https://`*`CA_Cloud_Name`*`.ca.analytics.ibm.com:443/bi/v1/disp`, wobei *CA_Cloud_Name* durch den Namen Ihres Rechenzentrums ersetzt werden sollte.

    Dispatcher-URI für externe Anwendungen
    Setzen Sie diese Eigenschaft auf `https://`*`CA_Cloud_Name`*`.ca.analytics.ibm.com:443/bi/api/soap`, wobei *CA_Cloud_Name* durch den Namen Ihres Rechenzentrums ersetzt werden sollte.

    Im folgenden Beispiel ist der Wert für *CA_Cloud_Name* als `us1` angegeben.



12. Klicken Sie im Menü **Datei** auf **Speichern**.

    Die Framework Manager-Konfiguration sollte ohne Fehler gespeichert werden. Wenn Sie jedoch die folgende Warnung erhalten: "Die kryptografischen Informationen können nicht verschlüsselt werden. Möchten Sie die Konfiguration als unverschlüsselten Text speichern?"oder allgemeine Konnektivitäts-probleme mit Framework Manager auftreten, stellen Sie sicher, dass Folgendes zutrifft:

    - Die Eigenschaften **Gateway-URI** und **Dispatcher-URI für externe Anwendungen** in Cognos Configuration for Framework Manager.

      Stellen Sie sicher, dass der Rechenzentrumteil der URIs und die Portnummer korrekt sind.
    - Die Framework Manager-Version.

      Die Framework Manager-Version muss mit der Cognos Analytics on Demand-Version kompatibel sein.

Index

E

F

G

H

I

J

L

M