IBM InfoSphere Identity Insight

Benutzerhandbuch

Version 9 Release 0

IBM InfoSphere Identity Insight

Benutzerhandbuch

Version 9 Release 0

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 433 gelesen werden.

Impressum

Diese Ausgabe bezieht sich auf Version 9 Release 0 von IBM InfoSphere Identity Insight (Produktnummer 5724-L71) und alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM InfoSphere Identity Insight, User's Guide, Version 9 Release 0,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
TSC Germany
Kst. 2877
Januar 2017

Inhaltsverzeichnis

Vorwort

IBM InfoSphere Identity Insight hilft Unternehmen beim Beheben von geschäftsbezogenen Problemstellungen, die sich auf das Erkennen der wahren Identität einer Person oder eines Gegenstandes ("Wer ist Wer") und das Ermitteln des potenziellen Werts bzw. der Gefahr von Beziehungen ("Wer kennt Wen") unter Kunden, Mitarbeitern, Lieferanten und anderen externen Faktoren beziehen. Diese Analyse erfolgt in Echtzeit und im Kontext vorhandener Geschäftsanwendungen. IBM InfoSphere Identity Insight stellt schnell verlässliche Informationen bereit, mit deren Hilfe in allen Branchen Bedrohungen abgewendet und Betrug, Missbrauch und geheime Absprachen verhindert werden können.

Informationen zu dieser Veröffentlichung

IBM InfoSphere Identity Insight Version 8.1 ist eine skalierbare Entitätsauflösungs- und Analyseplattform zum Schutz vor Sicherheitsrisiken und Betrug. Dieses Handbuch enthält Informationen zu Einsatz und Verwendung der Technologie des Produkts für die Disambiguierung von Identitäten und Beziehungen, mit der Ihr Unternehmen Folgendes ermitteln kann: Wer ist Wer? Wer kennt Wen? Wer macht Was? InfoSphere Identity Insight Version 8.1 sammelt im Laufe der Zeit Identitätskontext und ermittelt anhand verschiedener Informationen aus Unternehmensquellen, ob Personen wirklich das sind, was sie vorgeben. Sie können hoch entwickelte Entitätsalgorithmen zusammen mit einer patentierten, kulturübergreifenden Namensanalyse anwenden, um zu ermitteln, ob eine Person bereits identifiziert wurde, ob sie neu in Ihrem Unternehmen ist oder ob zuvor Verdachtsmomente bestanden, die auf der Basis neuer Fakten korrigiert werden sollten.

Zielgruppe

Dieses Handbuch wurde für Systemadministratoren, Anwendungsentwickler, Datenanalysten und IBM Professional Services-Mitarbeiter konzipiert, um eine erfolgreiche Verwendung des Produkts in der entsprechenden Umgebung zu ermöglichen.

Informationen zu Voraussetzungen und zugehörige Informationen

Dieses Benutzerhandbuch ist eine Untergruppe der in der Onlineversion des Information Centers (http://publib.boulder.ibm.com/infocenter/easii/v8r1m0/index.jsp) enthaltenen Informationen und wird lediglich als Service bereitgestellt. Andere Produktinformationen umfassen Folgendes:

- Releaseinformationen zu IBM InfoSphere Identity Insight Version 8 Release 1
- WebSphere Application Server-Dokumentation
- Dokumentation zu Ihrer Datenbanksoftware
- Dokumentation zur IBM Cognos Business Intelligence-Software
- Dokumentation zur IBM ILOG-Visualisierungssoftware
- Abhängig von der jeweiligen Bereitstellung folgende Informationen:
  - Dokumentation zu Ihrer Software zur Steuerung von Nachrichtenwarteschlangen
  - Dokumentation zu Ihrer Adresskorrektursoftware
  - Dokumentation zu Ihrer ETL-Tool-Software

Senden von Kommentaren

Ihre Rückmeldungen sind wichtig, damit eine bestmögliche Qualität der Informationen geliefert werden kann. Wenn Sie Anmerkungen zu diesem Handbuch oder einer anderen Dokumentation zu IBM InfoSphere Identity Insight haben, verwenden Sie das folgende Formular, um uns Ihre Kommentare zu senden:

http://www.ibm.com/software/data/rcf/

Sie können auch das Information Center aufrufen und die eingebetteten Feedbackformulare und zugehörigen Feedbackoptionen verwenden.

Kontaktieren des IBM Software Support

Vom IBM Software Support erhalten Sie Hilfe bei Produktfehlern.

Vorbereitende Schritte

Bevor Sie sich an den IBM Software Support wenden, muss Ihr Unternehmen einen gültigen IBM Softwarewartungsvertrag abgeschlossen haben und Sie müssen berechtigt sein, Probleme an IBM zu übergeben. Informationen zu den Typen verfügbarer Wartungsverträge finden Sie im Abschnitt „Enhanced Support" des *Software Support Handbook* unter techsupport.services.ibm.com/guides/services.html.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um den IBM Software Support bei einem Problem zu kontaktieren:

Vorgehensweise

1. Definieren Sie das Problem, stellen Sie Hintergrundinformationen zusammen und bestimmen Sie den Schweregrad des Problems. Hilfe hierzu finden Sie im Abschnitt „Contacting IBM" des *Software Support Handbook* unter techsupport.services.ibm.com/guides/beforecontacting.html.
2. Stellen Sie Diagnoseinformationen zusammen.
3. Sie sollten die folgenden Informationen im Fehlerbericht für den IBM Software Support bereitstellen können:
   - Produktname und -version
   - Datenbanktyp und -version
   - Betriebssystemname und -version
4. Übergeben Sie Ihr Problem mit einer der folgenden Methoden an den IBM Software Support:
   - Online: Klicken Sie die Option zum Senden und Nachverfolgen von Problemen auf der Website des IBM Software Support unter http://www.ibm.com/software/support/probsub.html an.
   - Telefonisch: Die Telefonnummer, die Sie für einen Anruf in Ihrem Land benötigen, finden Sie auf der Seite mit den Ansprechpartnern im IBM Software Support Handbook unter techsupport.services.ibm.com/guides/contacts.html.

Nächste Schritte

Wenn das Problem, das Sie übergeben, einen Softwarefehler oder fehlende bzw. fehlerhafte Dokumentation betrifft, erstellt der IBM Software Support einen APAR

(Authorized Program Analysis Report). Der APAR beschreibt das Problem detailliert. Wann immer dies möglich ist, stellt der IBM Software Support eine Ausweichlösung bereit, die Sie implementieren können, bis der APAR behoben und eine entsprechende Programmkorrektur geliefert ist. IBM veröffentlicht behobene APARs täglich auf der Website des IBM Software Support, sodass andere Benutzer, bei denen dasselbe Problem auftritt, von derselben Lösung profitieren können.

Kapitel 1. Übersicht über IBM InfoSphere Identity Insight

IBM® InfoSphere Identity Insight hilft Unternehmen beim Beheben von geschäftsbezogenen Problemstellungen, die sich auf das Erkennen der wahren Identität einer Person oder eines Gegenstandes ('wer ist wer') und das Ermitteln des potenziellen Werts bzw. der Gefahr von Beziehungen ('wer kennt wen') unter Kunden, Mitarbeitern, Lieferanten und anderen externen Faktoren beziehen. IBM InfoSphere Identity Insight stellt schnell verlässliche Informationen bereit, mit deren Hilfe in allen Branchen Bedrohungen abgewendet und Betrug, Missbrauch und geheime Absprachen verhindert werden können.

In vielen Unternehmen sind die Rohdaten bereits vorhanden, die die Identitäten und Beziehungen darstellen. Das Problem der meisten Systeme besteht darin, dass es einfach keine Möglichkeit gibt, die für die optimale Einsichtnahme erforderliche Datenmenge zu verwalten, zu analysieren und aufzulösen.

Mit IBM InfoSphere Identity Insight können Unternehmen Daten in Echtzeit aus jeder beliebigen Quelle wie Kundendatenbanken, Anbieterlisten, Mitarbeiterdatenbanken, Listen für die Einhaltung gesetzlicher Bestimmungen und Datenstromfeeds verwalten, analysieren und integrieren. IBM InfoSphere Identity Insight sendet Echtzeitalerts zur weiteren Untersuchung an Analysten, die Sicherheitsabteilung oder anderes relevantes Personal. IBM InfoSphere Identity Insight kann Ihnen auch helfen, basierend auf einer umfassenden Sicht Ihrer Kunden deren Potenzial für eine Ausdehnung Ihrer Geschäftstätigkeit oder ihre Marktsegmente festzustellen.

Mit IBM InfoSphere Identity Insight können Unternehmen eine zentrale, dynamische Entitätendatenbank erstellen, die als Plattform für alle ihre wissensbasierten Anwendungen verwendet werden kann. Es gibt eine Vielzahl von Protokollen und Technologien, um IBM InfoSphere Identity Insight in andere Unternehmenssysteme zu integrieren.

Erkennen von Identitäten

Mit dem Kernprozess der Entitätsauflösung löst IBM InfoSphere Identity Insight inkonsistente, mehrdeutige Identitätsdatensätze trotz absichtlicher Versuche, die Identität falsch darzustellen, in umfassende und datengruppenübergreifende Entitäten in auf.

Während der Entitätsauflösung führt IBM InfoSphere Identity Insight folgende Schritte aus:

- Es stellt fest, wann mehrere Datensätze, die verschiedene Entitäten zu beschreiben scheinen, tatsächlich eine einzelne Entität sind.
- Es integriert die unterschiedlichen Identitätsdatensätze für jede aufgelöste Entität in eine kombinierte Sicht der Entität, bewahrt jedoch für jeden Datensatz die vollständige Zurückführung (auf die ursprüngliche Datenquelle). Die vollständige Zurückführung (auf die ursprüngliche Datenquelle) stellt sicher, dass die Daten nie verloren gehen und immer zu ihrer ursprünglichen Quelle zurückverfolgt werden können.
- Wenn neue Daten in das System geladen werden, aktualisiert und verwaltet IBM InfoSphere Identity Insight die Informationen im Kontext für die Entitäten in der Entitätendatenbank. Es kann die Bedeutung neuer oder geänderter Daten beim

Laden vollständig erfassen. Dabei nutzt es jede Transaktion optimal und erweitert die umfassende Sicht jeder Entität in der Entitätendatenbank.

Erkennen von Beziehungen

Ausgehend vom Entitätsbeziehungsprozess erkennt IBM InfoSphere Identity Insight beim Laden und Verarbeiten von Datensätzen aus mehreren Datenquellen Beziehungen zwischen Entitäten in der Entitätendatenbank.

Während der Entitätsauflösung führt IBM InfoSphere Identity Insight folgende Schritte aus:

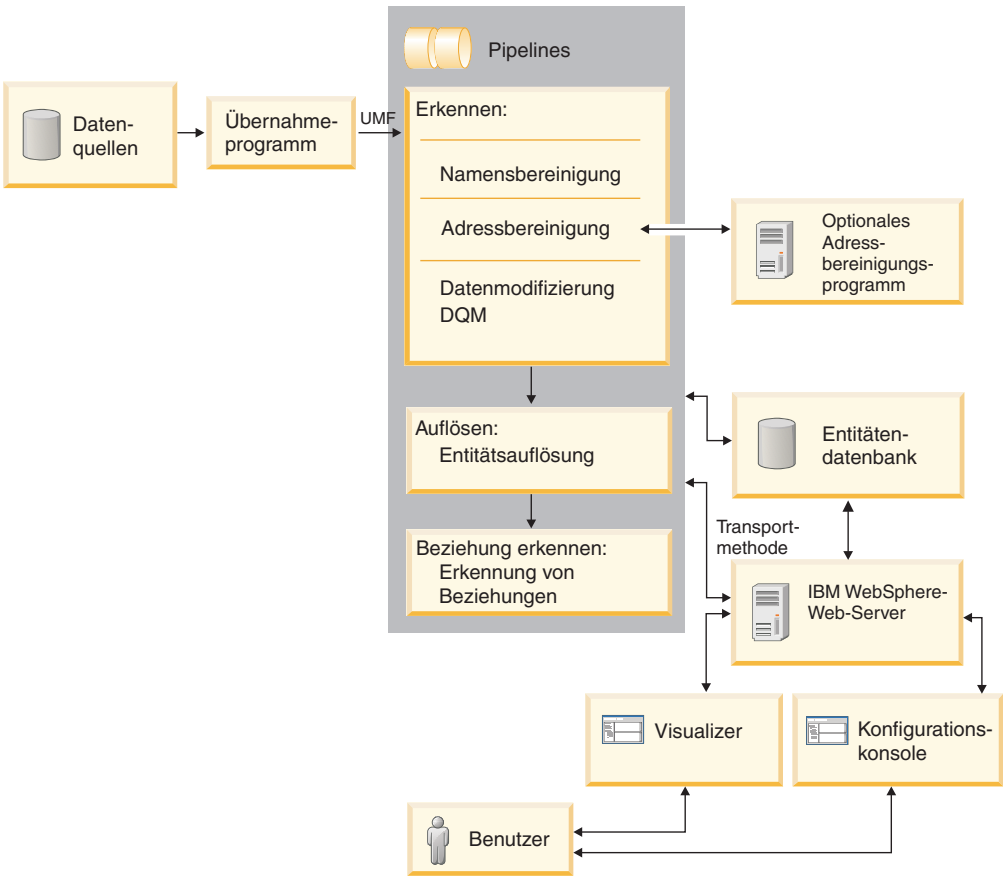
- Es verknüpft Entitäten nach Identitätsattributen wie Telefonnummern und Adressen, um relevante, aber nicht offensichtliche Beziehungen offenzulegen.
- Es stellt Netze von Zuordnungen und Entitäten mithilfe von einzelnen Datenattributen (wie Identifikationsnummern und Namen), Standorten (wie IP-Adressen), Einrichtungen (wie Warenlager, Schulen, Flughäfen oder Hotels), Organisationen (wie Zellen, Clubs oder Verbände), Geld (wie Bargeld oder telegrafische Geldüberweisungen) und Konten (wie Treue-, Bank-, Guthaben-, Kredit- oder Sparkonten) zusammen.
- Es stellt suspekte oder interessante Beziehungen fest (selbst solche, die verdeckt oder verschleiert sind) und versendet Echtzeitalerts basierend auf einer Gruppe benutzerdefinierter Regeln. Mit IBM InfoSphere Identity Insight können Analysten und Prüfer hoch entwickelte Suchen in der Entitätendatenbank ausführen, um jede zusammengehörige Entität und jede Entität oder jedes Attribut, mit der bzw. dem diese Entitäten verknüpft sind, weiter zu erforschen.

IBM InfoSphere Identity Insight unterstützt auch anpassbare regelbasierte Ausnahmeberichterstellung, damit Unternehmen angeben können, welche Entitäten aufgelöst wurden und welche Beziehungen Trigger-Alerts festgestellt haben.

Programmarchitektur

IBM InfoSphere Identity Insight ist ein mehrschichtiges System, in dem Daten durch Übernahmeprogramme aus Datenquellen in das System geladen werden und durch die Pipelines verarbeitet werden, die von Pipelineknoten gehostet werden. Die Verarbeitungsergebnisse werden in die Entitätendatenbank geschrieben und können an andere Systeme oder Datenbanken weitergeleitet werden.

In einer typischen Bereitstellung werden Unternehmensdaten aus mehreren Datenquellen an Übernahmeprogramme gesendet, wo die Daten in UMF (Universal Messaging Format) umgesetzt werden. Jedes Übernahmeprogramm verwendet eine Transportmethode, um die Daten an mindestens eine Pipeline zu senden. Viele dieser Transportmethoden sind bidirektional und das System kann so konfiguriert werden, dass es dem Übernahmeprogramm Antworten bereitstellt.



Mindestens eine Pipeline verarbeitet Ausführungen auf Pipelineknoten. Jede Pipeline verwaltet ihre eigene Verbindung zur Entitätendatenbank. Nach dem Empfang der UMF-Daten von mindestens einem Übernahmeprogramm verarbeitet die Pipeline die Daten datensatzweise durch ihre drei Kernprozesse: 'Erkennen', 'Auflösen' und 'Beziehung erkennen'. Die Pipeline speichert die Ergebnisse der Verarbeitung der einzelnen Datensätze in der Entitätendatenbank.

Benutzer interagieren über die folgenden Schnittstellen mit dem System:

- Die Konfigurationskonsole wird zum Konfigurieren und Überwachen des Systems verwendet.
- Analyst Toolkit-Anwendungen werden zum Analysieren und Disponieren von Alerts, zum Untersuchen von Beziehungen, zum Ausführen von Suchen und zum Generieren von Berichten verwendet.
- Befehlszeilenschnittstellen werden zum Ausführen von Pipelines verwendet.
- Web-Services können zum Ausführen der Pipelines oder zum Integrieren des Produkts in andere Unternehmenssysteme (einschließlich angepasster Benutzerschnittstellen) verwendet werden.

IBM InfoSphere Identity Insight verwendet IBM WebSphere Liberty. Dieser Anwendungsserver hostet die Konfigurationskonsole, Elemente von Analyst Toolkit sowie d ie Web-Services.

Diese leistungsfähige Architektur bietet Skalierbarkeit für jede Art der Bereitstellung. Pipelines können auf einer beliebigen Anzahl kompakter oder umfangreicher Systeme bereitgestellt werden. Mit einer ausreichenden Datenbankkapazität kann die Leistung der Pipelines auf jede gewünschte Stufe skaliert werden.

Übernahmeprogramme

Ein Übernahmeprogramm enthält die Tools und Programme, die Daten übernehmen, sie in UMF (Universal Message Format) umsetzen und die umgesetzten Daten anschließend zur Verarbeitung an die Pipeline übergeben.

Sie können die mit dem Produkt ausgelieferten Übernahmedienstprogramme verwenden, um Daten in UMF umzusetzen, oder Sie können ETL-Tools (ETL - Extrahieren, Transformieren und Laden) wie WebSphere QualityStage als Ihre Übernahmeprogramme verwenden.

Universal Message Format (UMF)

UMF ist eine erweiterbare XML-Version, die für das Strukturieren von Datenquellendateien verwendet wird. UMF enthält Standardtags, die Schlüsselteile von Identitäten, Beziehungen und Aktivitäten darstellen. Daten müssen in UMF konvertiert werden und der UMF-Spezifikation entsprechen, bevor sie von den Pipelines verarbeitet werden können.

UMF besteht aus den folgenden hierarchischen Komponenten:

UMF-Dokumente
: Die Sammlung von UMF-Segmenten, die die Daten strukturiert und den Typ für den Datenquellensatz angibt.

UMF-Segmente
: Die Komponente des UMF-Dokuments, die die Daten für die Datenquelle strukturiert.

UMF-Elemente
: XML-Tags und -Werte, die die Daten in einem UMF-Segment eines UMF-Dokuments definieren.

Die UMF-Spezifikation listet die UMF-Dokumenttypen, die UMF-Segmente in jedem UMF-Dokumenttyp und die gültigen UMF-Elemente in jedem UMF-Segment auf.

Pipelines

Pipelines sind die Komponenten, die Namens- und Adressbereinigungsstandardisierung, Datenqualitätsmanagement und Entitätsauflösung ausführen. Basierend auf der Systemkonfiguration lösen Pipelines auch Beziehungen auf und generieren Alerts.

Pipelines führen drei Kernprozesse aus:

- Erkennen: Hierzu gehört das Optimieren eingehender Daten durch die Ausführung von Datenstandardisierung, -bereinigung, -erweiterung und -qualitätsprüfungen.
- Auflösen: Hierzu gehört das Auflösen von Entitäten.
- Beziehungen erkennen: Hierzu gehört das Erkennen von Beziehungen und Generieren von Alerts.

Pipelines werden von Pipelineknoten gehostet.

Sie können Pipelines für Parallelverarbeitung konfigurieren, damit ein Befehl 'pipeline' mehrere parallele Pipelineverarbeitungsthreads startet, mit deren Hilfe das System mehrere Datenanforderungen gleichzeitig verarbeiten kann. Diese Funktion

kann dazu beitragen, dass die Systemleistung verbessert, die Datenverarbeitungszeit gesenkt und Hardwarespeichereinschränkungen reduziert werden.

Die Pipelineparallelverarbeitung wird an zwei Stellen konfiguriert:

- Die Einstellung für den globalen gemeinsamen Zugriff wird über den Parameter `Gemeinsamer Zugriff für Pipeline (Standard)` auf der Registerkarte **Systemkonfiguration** in der Konfigurationskonsole gesteuert. Der hierfür angegebene Wert bestimmt die Anzahl Parallelverarbeitungsthreads, die von einem Pipelinestartbefehl gestartet werden. Der Standardwert für diesen Parameter ist 1, das heißt, es wird nur ein Pipelineverarbeitungsthread gestartet, sofern dieser Parameter nicht bearbeitet wird.
- Eine Einstellung für lokalen gemeinsamen Zugriff (nach Pipelineknoten) kann in der Pipelinekonfigurationsdatei konfiguriert werden. Wenn Sie einen Parameter für gemeinsamen Zugriff und einen Wert in der Pipelinekonfigurationsdatei nach Pipelineknoten angeben, überschreibt dieser Wert den globalen Systemparameter. Wenn Sie auf diesem Pipelineknoten einen Pipelinestartbefehl absetzen, starten Sie die in der Pipelinekonfigurationsdatei angegebene Anzahl gleichzeitig ablaufender Pipelineverarbeitungsthreads.

Pipelineknoten

Pipelineknoten sind die physischen Maschinen, auf denen mindestens ein Pipelineprozess stattfindet.

Der Pipelineknoten ist die Lokation, an der Sie die ausführbare Pipelinedatei installieren und starten, die die Pipelineprozesse ausführt. Sie konfigurieren und verwalten die Pipelinekonfigurationsdatei für alle Pipelines, die von dieser Maschine gehostet werden. Das System schreibt die Pipelinenachrichten außerdem in die Protokolldateien auf den Pipelineknoten.

Pipelineknoten verbinden Pipelineprozesse mit den folgenden Komponenten der Produktarchitektur:

Übernahmeprogramme
Im Rahmen des ETL-Prozesses (Extrahieren, Transformieren und Laden) verwenden Übernahmeprogramme Transportmethoden, um UMF-Daten zur Verarbeitung an Pipelines zu senden. Sie verwenden die Transportmethode, die für das Übernahmeprogramm geeignet ist, über das die Verbindung zu den Pipelines hergestellt wird. Wenn Sie z. B. das UMF-Dateidienstprogramm als Übernahmeprogramm einsetzen, verwenden Sie die Dateitransportmethode.

Entitätendatenbank
Die Entitätendatenbank enthält Entitätsinformationen. Pipelines greifen während der Verarbeitung von eingehenden Datensätzen für Entitäts- und Beziehungsauflösung auf Entitätsinformationen zu. Für den Pipelineknoten muss der entsprechende Datenbankclient installiert und konfiguriert sein, damit die Pipelines auf die Entitätendatenbank zugreifen können.

Warteschlangen
Wenn Ihr System Warteschlangen als Transportmethode für das Senden von Daten zur Verarbeitung an die Pipelines verwendet, müssen Sie die entsprechende Software zur Steuerung von Nachrichtenwarteschlangen auf jedem Pipelineknoten installieren und konfigurieren.

Adressbereinigungsserver
Wenn Ihr System zur zusätzlichen Adressbereinigung Adressbereinigungs-

produkte anderer Firmen verwendet, muss jeder Pipelineknoten so konfiguriert werden, dass eine Verbindung zu den Adressbereinigungsservern hergestellt werden kann.

Web-Services
Sie müssen die Transportmethode HTTP verwenden, um die Pipelineprozesse auf dem Pipelineknoten mit den Web-Services zu verbinden.

Anwendungsmonitor

Zur Konfigurationskonsole gehört ein Anwendungsmonitor, mit dem Sie den Status, Statistikdaten und Fehler von Pipelines überwachen und Ergebnisse zwischen Pipelines und anderen Systemen oder Datenbanken weiterleiten können.

Sie müssen die Pipelines, die Sie überwachen oder von denen Sie Ergebnisse weiterleiten wollen, in der Konfigurationskonsole registrieren, um den Anwendungsmonitor nutzen zu können.

Überwachen von Pipelines

Der Anwendungsmonitor arbeitet mit einem SNMP-Agenten zusammen, der auf dem Pipelineknoten ausgeführt wird, der die zu überwachenden Pipelines hostet. Der SNMP-Agent sendet Statistikdaten für alle registrierten Pipelines auf einem Pipelineknoten an den Anwendungsmonitor, der die Daten in der Konfigurationskonsole veröffentlicht. Der Anwendungsmonitor aktualisiert den Status und die Statistikdaten von Pipelines alle 60 Sekunden.

Weiterleiten von Pipelineergebnissen

Über den Anwendungsmonitor können Sie die Ergebnisse der von den Pipelines verarbeiteten Daten an andere Systeme oder Datenbanken weiterleiten. Konfigurieren Sie hierzu in der Konfigurationskonsole Routing-Regeln, die angeben, von welcher Pipeline die Ergebnisse der Pipelineverarbeitung wohin weitergeleitet werden sollen.

Beispielsweise leiten einige Unternehmen eine Untergruppe der Ergebnisse an eine Berichtsdatenbank weiter, anstatt Analysten Berichtsabfragen für die Entitätendatenbank erstellen zu lassen (weil dies eventuell umständlich ist). Die Analysten erstellen und führen ihre Untersuchungsberichtsabfragen für die Berichtsdatenbank aus, die nur die für die Analysten relevanten Entitäts- und Beziehungsinformationen enthält.

Transportmethoden

Transportmethoden versetzen Daten von einem Bereich in einen anderen, und zwar zwischen Übernahmeprogrammen und Pipelines, zwischen Pipelines und der Entitätendatenbank und sogar zwischen Pipelines und externen Systemen.

Sie müssen ein für den verwendeten Transportmodustyp spezifisches Syntaxformat verwenden, das einen URI (Universal Resource Identifier) einschließt, um Daten transportieren zu können.

IBM InfoSphere Identity Insight unterstützt verschiedene Transportmethoden:
- Datenbanken
- Dateien
- HTTP
- Nachrichtenwarteschlangen (IBM WebSphere MQ)

Datenquellen

Datenquellen enthalten die Identitäten, die Sie für Entitätsauflösung verarbeiten und in die Entitätendatenbank laden wollen. Datenquellen enthalten identifizierende Daten (eindeutige persönliche Kennungen für eine Identität) und nicht identifizierende Daten (andere Attribute und Dateneinträge für eine Identität). Die Identitätsdatensätze in der Datenquelle müssen in UMF (Universal Message Format) exportiert werden, bevor sie vom System verarbeitet oder in die Entitätendatenbank geladen werden können. Beispiele für Datenquellen sind Mitarbeiterlisten, Überwachungslisten, Kundenverzeichnisse und Anbieterlisten.

Datenquellen enthalten wichtige Informationen wie Angaben zur ursprünglichen Quelle (weil die ursprünglichen Daten in UMF umgesetzt wurden) oder die externe Referenz für die Datenquelle. Durch diese Details wird jede Datenquelle im System eindeutig.

Wenn während der Entitätsauflösung zwei Entitäten nicht aufgelöst werden, verwendet das System die Informationen zur Datenquelle, um zu ermitteln, welche Informationen zu welcher Entität gehören.

Datenquellenpositionen und Quellensysteme

Sie können eingehende Datenquellen organisieren, indem Sie Datenquellenpositionen sowie Quellensysteme erstellen und diese Ihren Datenquellen zuordnen. Sie können mit Datenquellenpositionen und Quellensystemen zwischen ähnlichen Typen von Datenquellen unterscheiden.

Wenn Sie z. B. Reservierungsdaten und Personalabteilungsdaten von mehreren Standorten verarbeiten, können Sie mit einer Datenquellenposition ermitteln, welcher Standort die Daten beiträgt:

- Eigenschaft X Reservierungsdaten
- Eigenschaft X Personalabteilungsdaten
- Eigenschaft Y Reservierungsdaten
- Eigenschaft Y Personalabteilungsdaten

Konfigurationen nach Datenquelle

Sie können die Ergebnisse der Entitätsauflösung und Beziehungserkennung maximieren, indem Sie jede Datenquelle mithilfe der folgenden Einstellungen konfigurieren:

Rollen
Da Datenquellen Gruppierungen desselben Datentyps sind, können Sie jedem Identitätsdatensatz in derselben eingehenden Datenquelle automatisch dieselbe Rolle zuordnen. Wenn Sie z. B. einer Datenquelle der Personalabteilung die Rolle 'Mitarbeiter' zuordnen, wird allen eingehenden Datensätzen aus der Mitarbeiterliste automatisch die Rolle 'Mitarbeiter' zugeordnet.

Ladeebenen
Sie können festlegen, ob alle Daten in einer eingehenden Datenquelle geladen werden oder nur die Daten, die in mindestens eine Entität aufgelöst werden bzw. mindestens eine Entitätsbeziehung erkennen.

Einstellungen für Beziehungsauflösung
Sie können die Stufe der Beziehungserkennung nach Datenquelle konfigurieren. Sie können z. B. die Beziehungsauflösung für eine Datenquelle in-

aktivieren oder die Anzahl Abgrenzungsgrade für die Erkennung von Beziehungen in dieser bestimmten Datenquelle auswählen.

Entitätendatenbank

Die Entitätendatenbank ist die Datenbank, in der die Identitäten, Entitäten und Daten gespeichert werden, die für Beziehungen, Auflösungen und Alerts verwendet werden.

Die Entitätendatenbank ist der persistente Speicher aller aufgelösten Entitäten und ihrer Beziehungen. Beim Verarbeiten eingehender UMF-Datensätze durch Pipelines werden die neuen Daten ständig mit den Daten verglichen, die sich bereits in der Entitätendatenbank befinden. Daher wird Entitätsauflösung und Beziehungserkennung anhand von zusammengesetzten Entitäten ausgeführt, die alle aufgelaufenen Attribute aller vorherigen Datensätze enthalten.

Benutzerschnittstellen

IBM InfoSphere Identity Insight stellt mehrere Benutzerschnittstellen zum Interagieren mit den Produktmerkmalen bereit.

Konfigurationskonsole

Die Konfigurationskonsole stellt eine taskorientierte Schnittstelle bereit, die Ihnen die Ausführung einiger der wichtigsten Tasks zum Einrichten von Identity Insight für den Betrieb erleichtert.

Die Konfigurationskonsole wird von IBM WebSphere Liberty gehostet.

Verwalten der Systemkonfiguration

Über die Konfigurationskonsole können Sie die meisten Systemparameter und -optionen in einer Gruppe vereinfachter und optimierter Schnittstellen konfigurieren. Die Konsole schreibt die Änderungen dann in die Konfigurationsdatenbank. Direkt an der Konfigurationsdatenbank vorgenommene Änderungen werden nicht unterstützt. Diese Änderungen führen sehr wahrscheinlich zu einem nicht ordnungsgemäß funktionierenden Produkt.

Visualizer

Visualizer ist eine grafische Benutzerschnittstelle, die Analysten und Prüfer zum Analysieren der Ergebnisse von Alerts, Beziehungen und Entitätsauflösungen verwenden.

Visualizer wird von einer integrierten Version von IBM WebSphere Application Server gehostet. Sie konfigurieren Visualizer über die Konfigurationskonsole und die Auswahl **Benutzervorgaben** im Menü **Datei** von Visualizer.

Visualizer-Benutzer können verschiedene Analysetasks ausführen:

Ausführen von Analysen und Dispositionen für Alerts

Von der Entitätsauflösungsverarbeitung generierte Alerts stellen Beziehungs- und Entitätsauflösungen dar, die für ein Unternehmen von Interesse sind. In der Regel überprüfen Analysten Alerts und entscheiden auf Grundlage der Alertinformationen, welche Maßnahme ergriffen werden soll oder dass keine Maßnahme erforderlich ist. Es gibt die folgenden drei Alerttypen: Rollenalerts, Attributalerts und Ereignisalerts.

Visualizer zeigt die Alerts an und stellt Analysten Textsichten und grafisch orientierte Sichten der Alerts und der an den Alerts beteiligten Entitäten

bereit. Analysten können die Details abrufen und anschließend den Dispositionsstatus des Alerts entsprechend festlegen.

Erstellen und Verwalten von Attributalertgeneratoren
Mit Visualizer können Analysten über die Komponente 'Attributalertgenerator' persistente Suchen erstellen und verwalten sowie die Anzeige und den Emfpang von Attributalerts verwalten. Analysten können Attributalertgeneratoren basierend auf Attributdaten erstellen, um Identitäten zu suchen, die basierend auf diesen Attributdaten in Entitäten aufgelöst wurden. Analysten können auch einen Attributalertgenerator erstellen, um eine persistente Suche nach einer bestimmten Entität in der Entitätendatenbank durchzuführen.

Suchen von Entitäten
Visualizer-Benutzer können auch nach verschiedenen Methoden Entitäten für die weitere Analyse suchen:

- Nach Attributen
- Nach Datenquellenbenutzerkonto
- Nach Entitäts-ID
- Nach Auflösung (wie stark das eingegebene Kriterium mit den Identitäten und Entitäten in der Entitätendatenbank basierend auf den Schwellenwerten für die Mindestauflösungsbewertung übereinstimmt)

Hinzufügen von Entitäten und offengelegten Beziehungen
Mit Visualizer können Analysten Datensätze für Entitätsauflösung und Beziehungserkennung hinzufügen. Sie können einen einzelnen Identitätsdatensatz hinzufügen oder eine UMF-Datei laden, die Tausende von Identitätsdatensätzen enthält. Wie beim Hinzufügen von Identitäten durch Übernahmeprogramme werden durch Visualizer hinzugefügte Datensätze von einer Pipeline für Entitätsauflösung und Beziehungserkennung verarbeitet. Die Verarbeitungsergebnisse werden in die Entitätendatenbank geschrieben und Alerts werden in Visualizer veröffentlicht.

Analysten können auch Beziehungen zwischen Entitäten (nach Identität) offenlegen, wenn sie eine Verknüpfung zwischen den Identitäten kennen. Offengelegte Beziehungen sind beispielsweise das Zuordnen von Entitäten zu einander auf der Grundlage von Kontaktdaten für den Notfall oder von in einer Bewerbung aufgelisteten Referenzen. Diese Beziehungen wurden von der Entität in der Anwendung offengelegt.

Generieren und Drucken von Berichten
Visualizer enthält auch mehrere Berichte, die Analysten anzeigen und drucken können, damit sie ihre Arbeit mit Visualizer einfacher verwalten und überwachen können.

Befehlszeilenschnittstellen

Das Produkt verwendet Befehlszeilenschnittstellen, um die Pipelines auszuführen. Sie starten und stoppen Pipelines durch das Absetzen von Befehlen in einer Befehlszeile.

Konfigurationsdienstprogramm

Mit dem Konfigurationsdienstprogramm können Sie Installationseinstellungen nach der Installation anzeigen und modifizieren sowie Programmkorrekturen und Hotfixes installieren.

Sie können Programmkorrekturen und Hotfixes für folgende Anwendungen installieren:

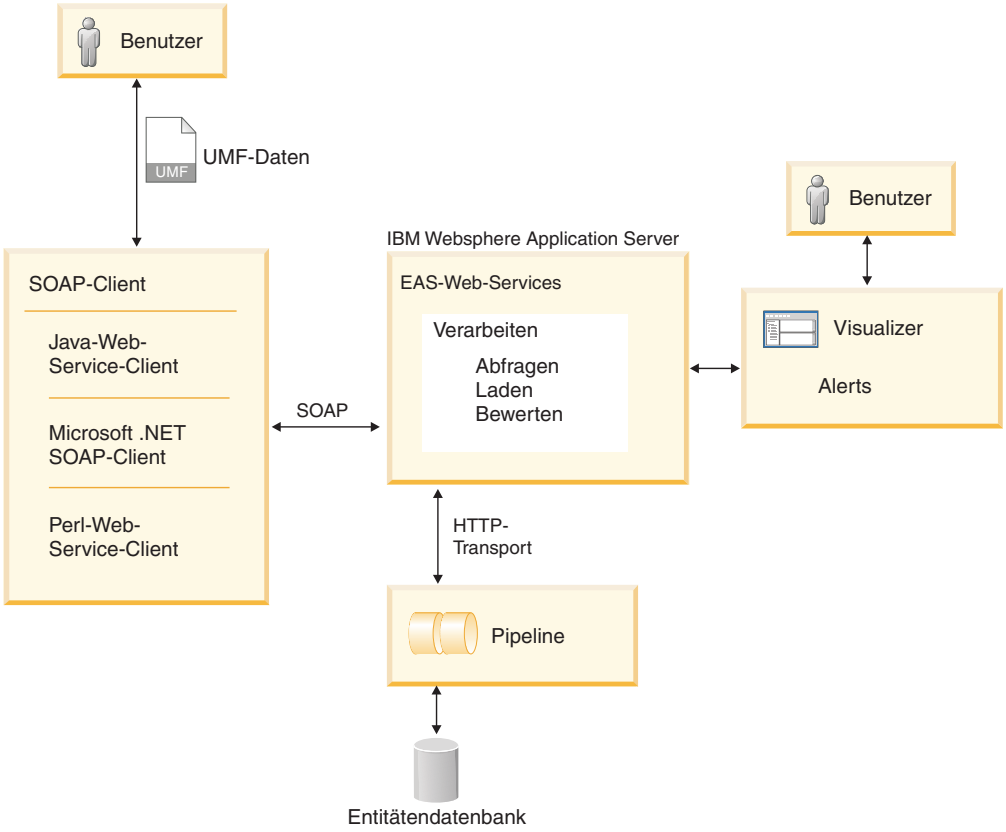
- Konfigurationskonsole
- Visualizer
- Visualizer-Berichte
- Java™ Web Start
- Web-Services
- Grafikanwendung
- Anwendung EntitySearcher
- Produktdokumentation

Sie können auch Einstellungen für Folgendes modifizieren:

- Konfigurationskonsole
- WebSphere-Konfiguration
- Datenbankkonnektivität
  - Konnektivitätseinstellungen für die Entitätendatenbank
  - Konnektivitätseinstellungen für die Anwendungsmonitordatenbank
  - Konnektivitätseinstellungen für die Konfigurationskonsolendatenbank
  - JDBC-Einstellungen

Web-Services

IBM InfoSphere Identity Insight stellt eine Gruppe von Web-Services bereit, mit denen Sie externe Anwendungen erstellen können, die UMF-Daten (Universal Message Format) für Pipelineverarbeitung oder Suchen nach Entitäten in die Entitätendatenbank laden können. Sie können die bidirektionale Transportmethode HTTP (Hypertext Transfer Protocol) verwenden, die eine Standardfunktion in der Pipeline ist.



IBM InfoSphere Identity Insight-Web-Services verwenden vier SOAP-Methoden (Simple Object Access Protocol): Verarbeiten, Suchen, Laden und Bewerten. Das Produkt unterstützt SOAP Version 1.1.

Das Produkt wird mit mehreren Komponenten ausgeliefert, die Sie in die Verwendung von Web-Services einführen.

srd.wsdl
Diese Datei enthält eine Definition der Web-Service-Beschreibungssprache für die Produkt-Web-Services. Sie können diese Datei mit allen SOAP-Toolkits oder -Technologien verwenden, um die Web-Services zu starten. Sie rufen diese Datei auf, indem Sie WebSphere Liberty starten und die Datei http://hostname:port/easws/resources/wsdl/srd.wsdl laden.

wsutil.jar
Diese Datei ist ein Web-Service-Testclient, der für das Testen Ihrer Web-Service-Installation und -Konfiguration bereitgestellt wird. Dieses Dienstprogramm finden Sie im Verzeichnis `ibm-home/easws`.

Kernkonzepte

Für die effektive Verwendung von IBM InfoSphere Identity müssen Sie seine Schlüsselkonzepte wie Entitäten, Identitäten und Attribute verstehen.

Entitäten

Eine Entität ist eine Sammlung von mindestens einer Identität, die für dieselbe Person, dasselbe Unternehmen, denselben Bereich oder dasselbe Element stehen. Entitäten werden in der Entitätendatenbank gespeichert.

Obwohl Entitäten häufig mit Menschen assoziiert werden, können sie ebenso gut Gegenstände wie Unternehmen oder Fahrzeuge sein. Sie können die Daten Ihres Unternehmens sogar mithilfe der erweiterbaren Systemkonfiguration zuordnen und jede beliebige Art von Entität erstellen, die aufgelöst werden oder in Beziehung gesetzt werden soll.

Entitäten setzen sich häufig aus Identitäten zusammen, die aus mehreren verschiedenen Quellensystemen kommen. Die Entitätsauflösung ermittelt, welche Identitäten wirklich dieselbe Entität aufweisen, und erstellt eine zusammengesetzte Entität, die alle Identitäten enthält, die dieser zusammengesetzten Entität zugeordnet sind. Das System wahrt die Möglichkeit zur vollständigen Zurückführung der Datensätze auf die ursprüngliche Datenquelle und gibt die Quelle an, die jeder Identität in der zusammengesetzten Entität zugeordnet ist.

Sie konfigurieren das System derart, dass Entitäten so aufgelöst werden und in Beziehung zueinander gesetzt werden, dass sie die Ziele Ihres Unternehmens erfüllen.

Identitäten

Identitäten sind eine Sammlung von Attributen aus einer Datenquelle, die eine Person, ein Unternehmen, einen Bereich oder ein Element darstellen.

Durch Entitätsauflösung werden Identitäten aufgelöst und aus einzelnen Identitäten werden zusammengesetzte Entitäten erstellt, wenn die Identitäten allgemeine Attribute gemeinsam mit der zusammengesetzten Entität nutzen.

Identitäten wurden zuvor eventuell als Benutzerkonten bezeichnet.

Attribute

Attribute sind Merkmale oder Eigenschaften, die eine Person, ein Unternehmen, einen Bereich oder ein Element beschreiben. Allgemeine Attribute enthalten Informationen wie Namen, Adressen, Telefonnummern, Kreditkartennummern, Steueridentifikationsnummern und Lizenznummern.

Das System unterstützt die folgenden Attributarten:

Namen
: Namensattribute definieren entsprechend dem Entitätsmodell und der eingehenden Identität den Namen der Person, des Unternehmens, des Bereichs oder des Elements. Namensattribute stellen in der Regel Personen und Unternehmen dar, sie können jedoch auf die Namen von Transportmitteln (wie PKWs, LKWs, Schiffe oder Flugzeuge), Gruppen oder jede andere Art von Entität, die Ihr Unternehmen in seinem Entitätsmodell definiert, ausgeweitet werden.

Adressen
: Adressattribute definieren einen Standort der Identität und enthalten in der Regel Standardadressinformationen: Straßenname und Hausnummer, Gebäudenummer, Ort, Bundesland/-staat, Land und Postleitzahl.

Nummern
: Nummernattribute bestehen aus Daten, die in der Regel als eine Nummer beschrieben werden, z. B. Kreditkartennummern, Telefonnummern und Passnummern. Nummern sind nicht ausschließlich auf numerische Zeichen beschränkt, da viele Nummern alphanumerische Zeichen verwenden.

Merkmale

Merkmalattribute definieren weitere Identitätseigenschaften oder -informationen, die durch die anderen Attributarten nicht ausgedrückt werden. Mit Merkmalattributen können Sie das System anpassen, damit Sie Identitätsmerkmale für das Auflösen von Entitäten oder Erkennen von Beziehungen definieren können. Zu gängigen Arten von Merkmalen gehören Geburtsdaten und das Geschlecht.

E-Mails

E-Mail-Attribute definieren Internet-E-Mail-Adressen. E-Mail-Adressen sind in der Regel eindeutig. Einige Studien haben gezeigt, dass Personen, die mehrere Namen verwenden, in der Regel dieselbe oder zwei E-Mail-Adressen verwenden.

In UMF (Universal Message Format) werden die verschiedenen Attributarten in UMF-Segmenten ausgedrückt. Jede Attributart hat ihr eigenes UMF-Segment.

Entitätsauflösung

Entitätsauflösung ist der Prozess, der Entitäten auflöst und Beziehungen erkennt. Die Pipelines führen Entitätsauflösung beim Verarbeiten von eingehenden Identitätsdatensätzen in drei Phasen aus: 'Erkennen', 'Auflösen' und 'Beziehungen erkennen'.

Erkennen

Während der Entitätsauflösung müssen Pipelines die Daten erkennen, indem sie die eingehenden Identitätsdaten prüfen, optimieren und erweitern. Während dieser Erkennungsphase des Pipelineprozesses bereinigen und standardisieren die Pipelines die Datenwerte und prüfen die Datenqualität, um die Integrität der Entitätendatenbank zu schützen.

Datenqualitätsmanagement (DQM)

Datenqualitätsmanagement (DQM) ist der Pipelineprozess, der Daten auf erforderliche Werte, gültige Datentypen und gültige Codes prüft. Sie können DQM auch so konfigurieren, dass die Daten korrigiert werden, indem Standardwerte bereitgestellt, Zahlen und Daten formatiert und neue Codes hinzugefügt werden.

Datenqualitätsmanagement dient so wie Namens- und Adressbereinigung und -standardisierung der Optimierung und Erweiterung der Datenqualität. Diese Datenqualitätsvorbereitung ist ein wesentlicher Schritt in der Entitätsauflösung, weil er die Übereinstimmungwahrscheinlichkeit der sich ergebenden aufgelösten Entitäten und erkannten Beziehungen erhöht.

Sie wenden Datenqualitätsmanagement auf die in das System geladenen Daten an, indem Sie DQM-Regeln konfigurieren. DQM-Regeln können eine Reihe von Reparatur-, Bereinigungs- und Standardisierungsfunktionen für eingehende Identitätsdatenwerte ausführen. Hierzu gehören das ordnungsgemäße Formatieren von Zahlen, Feststellen und Korrigieren von Schreib- oder Transpositionsfehlern sowie das Feststellen und Korrigieren von absichtlichen Ungenauigkeiten, die von Personen eingeführt wurden, die ihre Identitäten verheimlichen wollen.

Für das Produkt wurden mehrere DQM-Regeln nach UMF-Segment vorkonfiguriert, die die gängigsten Datenqualitätsprobleme für das betreffende UMF-Segment verarbeiten. Sie können bei Bedarf zusätzliche DQM-Regeln konfigurieren. Sie müssen sich zuvor jedoch mit der ursprünglichen Qualität der Daten und dem ETL-Prozess (Extrahieren, Transformieren und Laden), mit dem die Identitätsdaten

in UMF umgesetzt wurden, vertraut machen. Wenn Sie wissen, welche weitere Datenmodifizierung erforderlich ist, können Sie die richtigen DQM-Regeln, -Funktionen und -Werte zur Anwendung auf jeden Identitätsdatentyp auswählen, der weitere Datenqualitätsoptimierung benötigt.

Beispiel für die Verwendung einer DQM-Regel

Das Datumsformat für Ihr System ist z. B. TT/MM/JJJJ. In einigen Ihrer Datenquellen sind die Datumswerte jedoch als MM-TT-JJJJ formatiert. Sie können dem UMF-Segment `<NUMBER>` die DQM-Regel 204 hinzufügen, wodurch Sie es so konfigurieren, dass alle als MM-TT-JJJJ formatierten eingehenden Daten in das Datumsformat TT/MM/JJJJ korrigiert werden.

Namensbereinigung und -standardisierung:

Während der Pipelineverarbeitung werden Namen bereinigt und standardisiert, um den Identitätsdatensatz auf optimale Entitätsauflösung vorzubereiten.

Pipelineprozesse stellen die genauesten Namensinformationen zu Entitäten zur aktuellen, zukünftigen und Langzeitverwendung bereit. Wenn neue oder geänderte Identitätsnamensdaten in das System aufgenommen werden, werden sie mit dem Standardisierungsverzeichnis für Produktnamen verglichen, das eine Liste mit Stammnamen und ihren bekannten Derivaten enthält, um den Stammnamen zu ermitteln. Wenn der Stammname angegeben wird, speichert das System diesen Stammnamen und den ursprünglichen Namen für den eingehenden Identitätsdatensatz.

In der folgenden Tabelle werden zwei Beispiele möglicher Derivate desselben Stammnamens einschließlich verschiedener Schreibweisen angezeigt. Die Namen auf der linken Seite sind Derivate des Stammnamens auf der rechten Seite.

Tabelle 1. Beispiele möglicher Derivate für die Stammnamen Richard und Mohammad

Derivate	Stammname
Dick, Dickie, Ricardo Rich, Richie, Rick Rickey, Ricki, Rickie Ricky, Rikki, Ritchie	Richard
Mohamad, Mohammad Mohamed, Mohammed	Mohammad

Der Prozess für Namensbereinigung und -standardisierung korrigiert auch Rechtschreibfehler, falls erforderlich. Das System speichert die ursprüngliche Schreibweise und vorgenommene Korrekturen als Teil des Datensatzes. Bei den meisten anderen Systemen (einschließlich ETL- und Datenbank-Marketing-Tools) ist dies nicht der Fall.

Namensbereinigung und -standardisierung sind ein wichtiger Schritt, um die Übereinstimmungswahrscheinlichkeit der Entitätsauflösung zu steigern. Dieser Prozess ist besonders wichtig, weil die durchschnittliche Person im anglo-amerikanischen Umfeld bis zu fünf verschiedene Versionen ihres Namens für offizielle Zwecke und Verbraucherzwecke verwendet.

Adressbereinigung und -standardisierung:

Adressbereinigung und -standardisierung ist der Pipelineprozess, der Adressinformationen normalisiert und standardisiert, um mögliche Fehler und Verdreher zu beheben und den Identitätsdatensatz auf optimale Entitätsauflösungsverarbeitung vorzubereiten.

Im Rahmen der Adressbereinigung analysieren und standardisieren die Pipelines Adressinformationen. Beispielsweise wird `Street` in `St` oder `123-A Main St` in `123 Main St Apt A` umgesetzt.

Dieser Pipelineprozess prüft auch neue oder geänderte Informationen mithilfe einer globalen Adressdatenbank und Standardisierungssoftware, die von dem Produkt IBM InfoSphere QualityStage oder von einem anderen Adressbereinigungsprodukt wie Group 1 Software CODE-1 bereitgestellt wird. Das ausgewählte Adressbereinigungsprodukt ermittelt, ob die Adressinformationen ordnungsgemäß formatiert sind, korrigiert festgestellte Rechtschreibfehler (wie falsch geschriebene Straßennamen) und korrigiert fehlende oder falsche Informationen (es aktualisiert z. B. den Ortsnamen, damit er mit der Postleitzahl und der Adresse übereinstimmt).

In der folgenden Tabelle werden Beispiele für Adressbereinigung und -standardisierung von der Originaladresse zur korrigierten standardisierten Adresse aufgelistet.

Tabelle 2. Beispiele für den Vergleich von zwei Originaladressen mit der standardisierten Ergebnisadresse

Originaladresse	Standardisierte Adresse

`460 Oak Street`
 	
`Mill Valleu, CA 94914`
	`460 South Oak Street`
	
	`Mill Valley, CA 94914`

`4737 Simeron Drive`
 	
`Easton, MA 02334`
	`4737 Cimmeron Drive`
	
	`Easton, MA 02334`

Der Pipelineprozess zur Adressbereinigung und -standardisierung behält beide Originaladressen sowie die korrigierten und erweiterten Adressen bei, um die Übereinstimmungswahrscheinlichkeit späterer Entitätsauflösung und Beziehungserkennung zu steigern. Durch die Beibehaltung dieser Informationen werden auch bessere Langzeitinformationen bereitgestellt.

Datenqualitätsprüfung:

Wenn Identitätsdaten zur Verarbeitung im System ankommen, prüft die Pipeline die Qualität der Daten, um die Integrität der Entitätendatenbank zu schützen. Jeder eingehende Identitätsdatensatz wird auf korrekte UMF-Konstruktion (Universal Message Format), erforderliche Werte, gültige Datentypen und konfigurierte Datenquellencodes geprüft.

Beim Prüfen der Datenqualität versucht der Prozess, Probleme zu korrigieren, sofern dies möglich und das System entsprechend konfiguriert ist. Wenn das System ermittelt, ob Datenqualitätsprobleme korrigiert werden sollen oder nicht, verwendet es die konfigurierten DQM-Regeln (DQM - Datenqualitätsmanagement). DQM-Regeln definieren, welche Datenqualitätsmängel an eingehenden Identitätsdatensät-

zen korrigiert werden sollen und welche Mängel belassen werden sollen, wobei die Datensätze trotzdem verarbeitet werden können.

Sie können die Datenqualität für eine bestimmte Datenquelle anzeigen, indem Sie den Ladeergebnisbericht anzeigen oder drucken. Im Abschnitt mit der Qualitätszusammenfassung finden Sie hilfreiche Einsichten in die Gesamtdatenqualität für diese Datenquelle oder für eine bestimmte Gruppe von Identitätsdatensätzen, die aus dieser Datenquelle geladen wurden. Mithilfe dieser Informationen können Sie Ihren ETL-Prozess nach Bedarf für eine bestimmte Datenquelle anpassen.

Die Standardprotokollierung und -fehlerbehandlung protokollieren alle Fehler und Korrekturen der Datenqualität sowie Fehler, die das System nicht korrigieren konnte oder nicht korrigiert hat. Prüfen Sie die Systemprotokolle häufig, damit Sie die Datenqualitätsfehler kennen, die von der Pipelineverarbeitung nicht korrigiert wurden. In den meisten Fällen müssen Sie die Datenqualitätsfehler korrigieren und die korrigierten Identitätsdatensätze anschließend für Entitätsauflösungsverarbeitung erneut in eine Pipeline laden.

Beispiele für Datenqualitätsprüfung

Das System kann bei entsprechender Konfiguration automatisch Codes hinzufügen, die nicht als neue Codes erkannt werden. Das Protokoll UMF_EXCEPT zeigt die Ergebnisse neuer Codes an, die vom System hinzugefügt wurden, bzw. Datensätze, die zurückgewiesen und nicht verarbeitet wurden, weil das System einen Code nicht erkannt hat und nicht für das Hinzufügen eines Codes als neuer Code konfiguriert war.

In der folgenden Tabelle werden zwei Beispiele von Codes eingehender Datensätze gezeigt, die noch nicht im System konfiguriert waren.

Tabelle 3. Beispiele von zwei nicht im System konfigurierten Codes und das Ergebnis der Systemverarbeitung

Code	Qualitätsprüfung	Protokoll UMF_EXCEPT
Addr_Type x	neuer Code hinzugefügt	in Protokoll schreiben
Num_Type xxx	neuer Code zurückgewiesen	in Protokoll schreiben

- Im ersten Beispiel ist das System für das automatische Hinzufügen des neuen Codes für den Adresstyp konfiguriert.
- Im zweiten Beispiel ist das System nicht für das automatische Hinzufügen des neuen Codes oder die Entitätsauflösungsverarbeitung des Datensatzes konfiguriert.

In beiden Fällen protokolliert das System die Aktion in der entsprechenden Protokolldatei.

Auflösen

Während der Entitätsauflösung lösen die Pipelines Identitäten in Entitäten auf. Nach der Bereinigung, Standardisierung oder Erweiterung der Datenwerte in den Identitätsdatensätzen verwendet die Pipeline hoch entwickelte Suchalgorithmen, um die Datenwerte im eingehenden Identitätsdatensatz mit vorhandenen Entitäten in der Entitätendatenbank zu vergleichen. Hierdurch wird ermittelt, ob sie dieselbe Entität sind.

Das Auflösen von Entitäten umfasst folgende Phasen:

Generieren von Kandidatenlisten

Das System gleicht die Informationen zum eingehenden Identitätsdatensatz mit bereits in der Entitätendatenbank vorhandene Entitäten ab, um eine Liste mit potenziellen Entitätsauflösungskandidaten zu erstellen. Die Attributwerte jedes Kandidaten reichen für eine Fortsetzung der Entitätsauflösungsauswertung aus. Sie können die Kriterien konfigurieren, mit denen das System die Kandidatenlisten generiert.

Ausführen der Entitätsauflösung

Das System wendet nach der Generierung der Kandidatenlisten die Auflösungsregeln auf jede Entität in der Kandidatenliste an. Es verwendet dabei eine Bewertungsmethode, die eine Auflösungsbewertung berechnet, um zu ermitteln, ob die eingehende Identität und die die vorhandene Entität aufgelöst werden sollen. Sie können Auflösungsregeln konfigurieren und die Schwellenwerte für die Auflösungsbewertungen festlegen, um zu ermitteln, wie ähnlich die Attributwerte sein müssen, damit die eingehende Identität und die Kandidatenentität in eine Entität aufgelöst werden.

Kandidatenlisten

Kandidatenlisten sind die Listen der Entitäten, die potenziell mit dem eingehenden Identitätsdatensatz übereinstimmen können. Die Kandidatenliste wird erstellt, indem die Entitäten abgerufen werden, die basierend auf den in der Konfiguration für Kandidatenerstellungsregeln angegebenen Attributen mit der eingehenden Identität Attribute gemeinsam haben.

Der Entitätsauflösungsprozess verwendet zum Auflösen von Entitäten und Beziehungen nur die in der Kandidatenliste aufgeführten Entitäten.

Da Entitätsauflösung und Beziehungserkennung auf der Grundlage von Attributen ermittelt werden, müssen Sie sorgfältig erwägen, welche Attribute in Ihren Datenquellen die stärksten Kandidaten erstellen.

Nach der Generierung der Kandidatenliste vergleicht der Entitätsauflösungsprozess die eingehende Identität unter Verwendung der konfigurierten Auflösungsregeln mit dem ersten Kandidaten in der Liste. Das System berechnet mit den Auflösungsregeln eine Auflösungsbewertung, die darstellt, wie stark die Attribute der eingehenden Identität mit den Attributen der Kandidatenentität übereinstimmen. Wenn die Attribute der eingehenden Identität die Auflösungsbewertung für diese Regel erfüllen oder übersteigen, wird der eingehende Identitätsdatensatz in die Kandidatenentität aufgelöst.

Wenn die Auflösungsbewertung die für diese Auflösungsregel festgelegte Auflösungsbewertung nicht erfüllt oder nicht übersteigt, springt das System zur nächsten Auflösungsregel, bis der eingehende Identitätsdatensatz in eine Kandidatenentität aufgelöst wurde oder alle Auflösungsregeln ausgeschöpft wurden.

Wenn der eingehende Identitätsdatensatz nicht in eine vorhandene Entität aufgelöst wird, löst das System den Datensatz in eine neue Entität auf und speichert die neue Entität in der Entitätendatenbank.

Auflösungsregeln

Auflösungsregeln sind die Gruppe von Kriterien, mit denen das System definiert, wie verglichene Entitäten aufgelöst werden (wenn sie dieselbe Entität sind oder nicht) und wie sie Beziehungen erkennen (wenn Entitäten nicht in dieselbe Entität aufgelöst werden, wie viele Attribute sie gemeinsam haben).

Beim Definieren von Auflösungsregeln müssen Sie Schwellenwerte angeben, die zur Gesamtauflösungsbewertung beitragen, die bestimmt, ob eine eingehende Identität in eine vorhandene Entität aufgelöst wird:

- Kandidatenschwellenwerte geben an, welche Attributdatenwerte verglichen werden, um zu ermitteln, ob eine Identität und eine Entität in eine zusammengesetzte Entität aufgelöst werden. Der Schwellenwert ist die Mindestbewertung, die ein bestimmter Attributwert bei einem Vergleich der eingehenden Identität mit einer vorhandenen Entität erreichen muss, um die Auflösungsregel zu erfüllen.
- Bestätigungs-/Zurückweisungsschwellenwerte geben an, welche Bewertungsgewichtung (positiv oder negativ) übereinstimmenden oder sich widersprechenden Attributdatenwerten zugewiesen wird, wenn Sie die Verwendung von Zurückweisungen aktivieren.

Sie können auch angeben, wie sich widersprechende Werte für dieselben Attribute sich auf die Auflösungsbewertung auswirken. Diese sich widersprechenden Werte heißen Zurückweisungen. Sie können Auflösungsregeln konfigurieren, die angeben, dass die Regel nicht erfüllt ist, wenn in den Attributwerten Konflikte (Zurückweisungen) vorhanden sind. Sie können auch die Schwellenwerte für eine Auflösungsregel anpassen, um basierend auf den Vergleichsbewertungen, die mindestens eine angegebene Schwellenwertbewertung nicht erfüllen, automatische Zurückweisungen zu erstellen. Je höher eine Schwellenwertbewertung festgelegt wird, desto präziser muss die Übereinstimmung sein, um die Auflösungsregel zu erfüllen.

Erneut auflösen

Es kommt während des Entitätsauflösungsprozesses zu erneuter Auflösung, wenn zwei Entitäten als dieselbe Entität aufgelöst werden und ein zusammengesetzter Entitätsdatensatz erstellt wird. Die Entitätsauflösung startet den Prozess mithilfe des neuen zusammengesetzten Entitätsdatensatzes erneut von Anfang an, um zu prüfen, ob die neue zusammengesetzte Entität in eine der anderen Entitäten in der Entitätendatenbank aufgelöst werden kann.

Wie bei einer neuen eingehenden Entität versucht der Entitätsauflösungsprozess, eine Kandidatenliste mit Entitäten aus der Entitätendatenbank zu generieren. Wenn eine Kandidatenliste generiert werden kann, fängt der Entitätsauflösungsprozess mit der Entitätsauflösung an und vergleicht dabei jeden Kandidaten in der Liste mit der neuen zusammengesetzten Entität. Wenn eine Kandidatenliste nicht generiert werden kann, wird der Entitätsauflösungsprozess vom Beziehungserkennungsprozess abgelöst.

Auflösung aufheben

Das Aufheben der Auflösung ist ein Teil des Entitätsauflösungsprozesses, wenn die Attributwerte in der eingehenden Identität neue Informationen bereitstellen, die angeben, dass eine zusammengesetzte Entität aus zwei Entitäten besteht und dass der zusammengesetzte Entitätsdatensatz in zwei Entitäten aufgeteilt ist. Das System weiß auf Grund der Datenquelle, die jedem Datensatz zugeordnet ist, welche Datensätze zu welcher Entität gehören. Nach dem Aufheben der Auflösung startet das System die erneute Auflösung.

Beispiel für das Aufheben einer Auflösung

Bislang hat das System einen eingehenden Identitätsdatensatz für Will Smith mit der Adresse 1234 Main Street, Anytown, USA, Telefonnummer (201) 555-2244 und E-Mail-Adresse jrsmith@internetprovider.com in William Smith, Sr. mit derselben Adresse und Telefonnummer aufgelöst.

Nun wird ein eingehender Identitätsdatensatz für Will Smith, Jr. mit der E-Mail-Adresse jrsmith@internetprovider.com und der Kreditkartennummer 123-54-9999 verarbeitet.

Basierend auf den neuen Informationen von Will Smith, Jr. und der Kreditkartennummer kann das System ermitteln, dass die Auflösung des zusammengesetzten Entitätsdatensatzes für William Smith, Sr. aufgehoben, d. h. in William Smith, Sr. und William Smith, Jr. aufgeteilt werden muss. Nachdem die eine Entität in zwei Entitäten aufgeteilt wurde, fängt das System mit der erneuten Auflösung an, um zu prüfen, ob andere Entitäten in der Datenbank basierend auf den neuen Informationen in William Smith, Jr. aufgelöst werden.

Beziehung erkennen

Während der Entitätsauflösung führen Pipelines auch den Beziehungserkennungsprozess durch, der Beziehungen zwischen Identitäten und Entitäten erkennt und Alerts für Beziehungen von Interesse generiert.

Das System verwendet Rollen, d. h., Klassifizierungen einer Identität, die den Fokus oder den Zweck der Identität definieren, der darin besteht, Beziehungen zwischen Entitäten zu erkennen und herzustellen. Sie definieren im System Rollen und ordnen diese dann Identitäten nach Datenquelle oder als Teil der Umsetzung der ursprünglichen Datenquellendaten in UMF (Universal Message Format) zu.

Wenn die Pipeline eingehende Identitäten für Entitätsauflösung verarbeitet und die Identität in eine vorhandene Entität auflöst, haben die beiden Datensätze eine nullstufige Beziehung (Abgrenzungsgrad 0), d. h., die eingehende Identität und die Entität sind identisch. Je nach der Systemkonfiguration kann die Entitätsauflösung jedoch über nullstufige Beziehungen hinausgehen.

Nachdem die Pipeline alle Möglichkeiten in der Beziehungserkennungsphase der Entitätsauflösung erschöpft hat, prüft der Beziehungserkennungsprozess die in der Kandidatenliste verbleibenden Entitäten oder jene Entitäten, die nicht in die eingehende Identität aufgelöst wurden, daraufhin, ob zwischen ihnen eine Beziehung besteht. In der Regel werden in der Kandidatenliste befindliche Entitäten mit einer einstufigen Abgrenzung für mindestens ein Attribut mit der eingehenden Identität verknüpft. Dies bedeutet, dass beide Entitäten dieselben Attributdatenwerte für mindestens ein Attribut gemeinsam haben, weshalb sich die Entität in der Kandidatenliste befindet.

Nachdem der Prozess eine Beziehung erkannt hat, vergleicht das System die zwischen der Identität und den Entitäten zugeordneten Rollen mit den konfigurierten Rollenalertregeln. Wenn das System feststellt, dass die der Identität zugeordneten Rollen und eine Entität die Kriterien für diese Regel erfüllen, generiert es einen Alert, der angibt, dass eine Beziehung von Interesse erkannt wurde. Je nach der Konfiguration des Systems und der Rollenalertregeln kann es sich um eine ein-, zwei- oder mehrstufige Beziehung handeln.

Beziehungen

Beziehungen sind Verknüpfungen zwischen mindestens zwei Entitäten. Beziehungen werden am Ende des Entitätsauflösungsprozesses erkannt, wenn zwei Entitäten mehrere Datenattributwerte gemeinsam nutzen.

Beziehungen können auf Verknüpfungen basieren, die vom System erkannt und/oder von einem Analysten offengelegt wurden. Nicht jede Beziehung rechtfertigt jedoch die Generierung eines Alerts für weitere Analyse oder Untersuchung. Sie

definieren Beziehungen von Interesse, indem Sie Rollenalertregeln konfigurieren, die angeben, welche Kombination von Rollen, die Entitäten zugeordnet sind, Alerts generieren muss.

Beziehungsbeispiele

Es folgen Beispiele für Beziehungen, die eventuell während der Entitätsauflösung erkannt werden:

- Ein Kunde ist auch ein Lieferant. Auf Grundlage der Geschäftspolitik und der Prozeduren in Ihrem Unternehmen handelt es sich hierbei eventuell um eine Beziehung von Interesse.
- Ein Mitarbeiter kennt einen Kunden. Sofern die Geschäftspolitik und Prozeduren in Ihrem Unternehmen eine derartige Beziehung nicht verbieten, oder abhängig von den Daten, die zwischen dem Mitarbeiter und Kunden ausgetauscht werden, handelt es sich hierbei eventuell nicht um eine Beziehung von Interesse.
- Ein Kunde kennt einen anderen Kunden. Wenn Sie einen sehr guten Kunden haben, ist es nützlich zu wissen, wen dieser Kunde kennt. Sie können dann versuchen, Ihre Geschäftstätigkeit auf den Bekanntenkreis Ihres Kunden auszudehnen.

Degrees of Separation - Übersicht:

Die Komponente Degrees of Separation erweitert das Leistungsspektrum für den Beziehungsabgleich von IBM Relationship Resolution.

Standardmäßig identifiziert IBM InfoSphere Identity Insight potenziell interessante Beziehungen und führt einen Abgleich für Entitäten durch, die einen Abgrenzungsgrad von 1 zu einer eingehenden Identität haben, die in eine Entität aufgelöst wird. Die Aktivierung der Komponente Degrees of Separation erweitert diese Funktionalität auf beinahe uneingeschränkte benutzerdefinierte Angaben für den Abgrenzungsgrad von eingehenden Identitäten, die in Entitäten aufgelöst werden.

Die Komponente Degrees of Separation verwendet Abgrenzungskonfigurationen, Rollen, Rollenalertregeln und Beziehungsbewertungen, um Echtzeit-Link-Analysen für sehr umfangreiche Datenbestände durchzuführen.

Wenn eine eingehende Identität in eine Entität aufgelöst wird, wird ein Entitätsdiagramm erstellt, das die von IBM Relationship Resolution ermittelten einstufigen Beziehungen verwendet. Das Entitätsdiagramm verwendet die einstufigen Beziehungen, um mehrstufige Beziehungsketten zu erzeugen, die von der Entität ausgehen, in die die Identität aufgelöst wurde. Dann kann eine Rollenalertkette durch Verbinden zweier mehrstufiger Beziehungsketten erstellt werden, die jeweils von der Entität ausgehen, in die die eingehende Identität aufgelöst wurde. Die Rollenalertkette kann dann dazu verwendet werden, eine Beziehung zwischen den Entitäten am Ende und innerhalb der mehrstufigen Beziehungskette zu finden.

Degrees of Separation reduziert den Arbeitsaufwand, indem alle Pfade ausgewertet werden, die zwei Entitäten miteinander verbinden, wobei die höchste Pfadrelevanz zur Berichterstellung von Beziehungen verwendet wird. Degrees of Separation kann so konfiguriert werden, dass ein Rollenalert für jede konfigurierte Rollenalertregel pro Entität zurückgemeldet wird, in die die eingehende Identität aufgelöst wurde.

Die Konfiguration von Degrees of Separation kann auf der Registerkarte **Systemkonfiguration** der Konsole über den Wert für Abgrenzungsgrade festgelegt werden.

Impersonal Awareness:

Impersonal Awareness ist eine Produktkomponente, die den traditionellen Beziehungsauflösungsprozess um das Suchen und Analysieren unpersönlicher Beziehungen erweitert. Der Beziehungserkennungsprozess findet Beziehungen zwischen Entitäten auf der Grundlage von Attributwerten, die den Entitäten zugeordnet sind. Manchmal ist es wichtig, Beziehungen zwischen Entitäten zu finden, die auf Aktivitäten oder anderen unpersönlichen Kennungen basieren. Diese auf Aktivitäten oder anderen unpersönlichen Kennungen basierenden Beziehungen zwischen Entitäten werden als *unpersönliche* Beziehungen bezeichnet. Aktivitäten oder unpersönliche Kennungen, die Beziehungen zwischen Personen darstellen, werden *Zuordnungsfakten* genannt.

Unpersönliche Beziehungen sind immer bei mehrstufigen Beziehungen mit mindestens zwei Abgrenzungsgraden vorhanden, weil das Zuordnungsfaktum selbst eine Entität darstellt. Wenn Sie Impersonal Awareness aktivieren und unpersönliche Beziehungen finden wollen, müssen Sie also Ihre Datenquellen für die Verwendung von Degrees of Separation konfigurieren. Diese Komponente erweitert die Entitäts- und Beziehungsauflösung, sodass auch Beziehungen mit mehreren Abgrenzungsgraden gefunden werden.

Beispielsweise enthält eine Telefontransaktion Daten zu Telefonnummern, und zwar die anrufende Nummer sowie die empfangende Nummer. Obwohl eine Person eine andere Person angerufen hat, können diesen Personen allein auf Grundlage der Telefontransaktion keine gemeinsamen Daten zugewiesen werden. Oft ist das Zuordnungsfaktum (der Telefonanruf) schon bekannt, bevor andere Informationen zu den zusammengehörigen Entitäten (die beiden Personen, die das Telefongespräch führten) bekannt sind. Da die Zuordnungsfakten keiner Person zugeordnet werden können, müssen sie als eigenständige Entitäten dargestellt werden, die keine Personen sind, sich aber auf Personen beziehen. Mithilfe von Impersonal Awareness kann jedoch anhand des Telefonanrufs erkannt werden, dass eine Beziehung zwischen zwei Personen vorhanden ist.

UMF beinhaltet eine Funktionalität für Entitätstypen, die es Ihnen ermöglicht, Zuordnungsfakten als Entitätstypen zu definieren. Bei Verwendung dieser Funktionalität werden Zuordnungsfakten in der Entitätendatenbank zu eigenständigen Entitäten. Sie können dann dazu verwendet werden, Beziehungen zwischen Entitäten des Typs 'Person' zu ermitteln. Durch das Konfigurieren neuer Entitätstypen, durch Angeben der entsprechenden Entitätstypen in UMF und durch das Erstellen neuer Auflösungskonfigurationen können diese Zuordnungsfakten dazu verwendet werden, unpersönliche Beziehungen und Konflikte zwischen Entitäten automatisch zu suchen.

Entitäten verschiedener Entitätstypen können nicht typenübergreifend aufgelöst werden, auch wenn die Auflösungsregeln es zulassen und sogar die Daten eine Auflösung unterstützen. Das bedeutet, dass ein Entitätstyp 'Telefonanruf' niemals in einen Entitätstyp 'Person' aufgelöst werden kann.

Analyst Toolkit stellt unpersönliche Beziehungen und zugeordnete Alerts grafisch dar und listet sie auf, wie dies bei persönlichen Beziehungen und zugeordneten Alerts der Fall ist.

Beispiel für Impersonal Awareness

Wenn Sie z. B. unpersönliche Beziehungen unter Verwendung von Telefonanrufen ermitteln wollten, dann würden Sie einen neuen Entitätstyp 'Telefonanruf' erstellen

und Ihren Übernahmeknoten so anpassen, dass jeder Telefonanrufdatensatz mit dem Entitätstypentag *Telefonanruf* gekennzeichnet wird.

Wenn die Datensätze mit den Telefonanrufen in das System aufgenommen wird, findet die Standardauflösung für Entitäten und Beziehungen eine einstufige Beziehung zwischen der Entität mit dem Typ 'Telefonanruf' und der Entität, die den Anruf getätigt hat (Person). Das Programm findet auch eine einstufige Beziehung zwischen der angerufenen Person und der Entität 'Telefonanruf'. Das System findet keine Beziehung zwischen den beiden Personen.

Wenn jedoch Degrees of Separation konfiguriert ist, setzt diese Komponente die Analyse fort und erkennt die zweistufige unpersönliche Beziehung zwischen dem Anrufer und der angerufenen Person. Eine unpersönliche Beziehung ist vorhanden, und zwar auf der Basis der Telefonnummern, die Attribute des Entitätstyps 'Telefonanruf' sind. Degrees of Separation analysiert dann die unpersönliche Beziehung und generiert einen Alert, wenn ein Konflikt gefunden wird.

Rollen

Eine Rolle ist eine Klassifizierung einer Identität, die den Fokus oder den Zweck dieser Identität definiert. Sie können einer Identität mehr als eine Rolle zuordnen. Beim Auflösen von Identitäten in Entitäten übernehmen Entitäten alle zugeordneten Rollen.

Mit Rollen konfigurieren Sie Rollenalertregeln, die Beziehungen von Interesse definieren und Alerts generieren.

Es gibt zwei Methoden, eine Identität einer Rolle zuzuweisen:

Nach eingehender Datenquelle
: Wenn Sie eine neue Datenquelle konfigurieren, ordnen Sie dieser Datenquelle eine Rolle zu. Die Datenquelle weist diese Rolle allen Identitäten zu, die den entsprechenden Code für die Datenquelle enthalten.

Nach UMF
: Wenn Sie die Datenquelle in UMF (Universal Message Format) umsetzen, können Sie Rollen direkt als Teil des UMF-Datensatzes zuordnen. Verwenden Sie hierzu das UMF-Segment `<SEP_ROLES>` mit dem UMF-Tag `<ROLE_CODE>`. Wenn Sie nach UMF konfigurieren, müssen Sie DQM-Regeln und eine Suchtabelle hinzufügen.

Beispiele nützlicher Rollen sind Mitarbeiter, Lieferanten, Kunden oder Überwachungslisten.

Beispiel für das Zuordnen von Rollen mit UMF

Wenn Sie die Rolle 'Mitarbeiter' einem Identitätsdatensatz mithilfe von UMF zuordnen wollen, geben Sie das folgende UMF-Segment `<SEP_ROLES>` und den folgenden UMF-Tag `<ROLE_CODE>` für den Identitätsdatensatz ein:

```
<SEP_ROLES>

    <ROLE_CODE>Mitarbeiter</ROLE_CODE>

</SEP_ROLES>
```

Alerts

Alerts sind Nachrichten oder andere Indikationen, die das Auftreten eines Ereignisses signalisieren.

Es gibt zwei Möglichkeiten, Alerts zu generieren:

- Attributalerts werden generiert, wenn Entitäten mit einer angegebenen Attributsammlung übereinstimmen.
- Rollenalerts werden generiert, wenn Entitäten, die über eine Beziehung mit einer anderen Entität verknüpft sind, gemeinsame Rollen aufweisen, für die der Benutzer angegeben hat, dass sie *von Interesse* sind oder einen *Konflikt* darstellen.

Es ist wichtig zu definieren, welche Alerts die Ziele Ihres Unternehmens erfüllen. Ein guter Ausgangspunkt ist die Frage, welche Beziehungen zwischen Entitäten für Ihr Unternehmen von Interesse sind. Beziehungen basieren auf benutzerkonfigurierten Rollen, die eingehenden Datensätzen durch das Quellensystem zugeordnet werden. Wenn zwei Entitäten genügend Attributdatenwerte gemeinsam haben, ohne dass es zu einer Auflösung kommt, bilden diese Entitäten eine Beziehung. Stellen Sie sicher, dass die für Ihr Unternehmen konfigurierten Rollenalertregeln klar definieren, welche Entitätsrollen eine Beziehung erzeugen, die Ihre Analysten weiter untersuchen wollen.

Alertbeispiele

Es folgen einige Beispiele für Beziehungen von Interesse, für die Ihr Unternehmen die Generierung von Alerts in Betracht ziehen könnte:

- Ein Unternehmensangestellter liefert Ihrem Unternehmen gegen Zahlung auch Waren oder Dienstleistungen.
- Einer Ihrer Kunden hat eine Adresse und einen Namen, die den Angaben einer Person in einer Überwachungsliste der Regierung ähneln.
- Zwei Angestellte, die Arbeitsunfallberichte vorlegen, haben ähnliche Namen und Adressen und dieselbe Telefonnummer.

Attributalerts:

Attributalerts sind Alerts, die von Attributalertgeneratoren erzeugt werden, welche eine permanente Systemabfrage erstellen, von der nach bestimmten Attributen oder Identitäten in der Entitätendatenbank gesucht wird. Sobald Attribute für Entitäten den Kriterien des Attributalertgenerators entsprechen, erzeugt das System einen Attributalert.

Visualizer-Benutzer erstellen ihre eigenen, persönlichen Attributalertgeneratoren. Wenn Sie nach einer bestimmten Identität oder Identitäten oder Entitäten, die einer bestimmten Gruppe von Attributen entsprechen, suchen, können Sie einen eigenen, persönlichen Attributalertgenerator erstellen, der bis zum angegebenen Ablaufdatum nach Übereinstimmungen sucht.

Beispiele für Entitätsattribute, für die Sie eventuell eine Benachrichtigung erhalten wollen:

- Name und eindeutige Nummer (z. B. eine Kreditkartennummer)
- Name und Telefonnummer
- Adresse
- Name und nicht eindeutige Nummer

Attributalertgeneratoren werden in Visualizer konfiguriert und können dort angezeigt werden. Die von Ihnen erstellten Attributalertgeneratoren sind nur für Sie verfügbar.

Beispiel für einen Adressattributalert

Sie überwachen die Adresse 675 Hickory Street Las Vegas, NV. Sie können einen Attributalertgenerator so konfigurieren, dass ein Attributalert erzeugt wird, wenn diese Adresse einem eingehenden Identitätsdatensatz zugeordnet wird, der der Entitätendatenbank hinzugefügt wird.

Rollenalerts:

Ein Rollenalert gibt an, dass eine oder zwei über eine Beziehung verknüpfte Entitäten eine konfigurierte Rollenalertregel erfüllen oder übererfüllen. Rollenalerts basieren auf konfigurierten Rollen und Rollenalertregeln. Sie zeigen eine Warnung oder ein Problem (z. B. dass ein Kunde eine potenziell gefährliche Person kennt) oder einfach interessante Beziehungen (z. B. dass ein Kunde einen Mitarbeiter kennt) an.

Sie geben für Beziehungen an, dass sie *von Interesse* sind oder einen *Konflikt* darstellen, indem Sie Rollenalertregeln konfigurieren, die angeben, welche Rollen nicht in einer einzelnen Entität vorhanden sein sollen oder nicht zwischen einer oder mehreren Entität(en) verknüpft sein können. Sie können mit der Konfigurationskonsole Rollenalertfilter konfigurieren, die festlegen, ob das System neue Alerts generiert, wenn neue Informationen vorliegen (beispielsweise eine neue Identität oder ein neuer Datenquellencode).

Während der Entitätsauflösung wertet die Pipeline Beziehungen zwischen der eingehenden Identität und Entitäten in der Kandidatenliste aus. Nach der Feststellung einer Beziehung zwischen der eingehenden Identität und einer Kandidatenentität wertet das System aus, ob die zugeordneten Rollen einer konfigurierten Rollenalertregel entsprechen. Wenn das der Fall ist, generiert das System einen Rollenalert.

Ein Rollenalert stellt Entitätsdaten zum Zeitpunkt der Rollenalerterstellung fest. In der Anzeige **Rollenalert-Detail** werden die Entitätsdaten so gezeigt, wie sie bei der Erstellung des Rollenalerts existierten. Da sich Entitätsdaten im Laufe der Zeit ändern, enthält die Entitätszusammenfassung die letzten Entitätsdaten. Wenn Sie die aktuellen Daten für eine bestimmte Entität anzeigen wollen, rufen Sie die Entitätszusammenfassung auf.

Sie können in den Komponenten von Analyst's Toolkit (Cognos-Berichte, Identity Insight-Plug-in für i2 und Identity Insight Explorer) Rollenalerts anzeigen und mit ihnen arbeiten.

Rollenalertregeln:

Rollenalerts sind benutzerdefinierte Regeln, die mindestens eine Rolle angeben, die nicht in einer einzelnen Entität vorhanden sein oder nicht zwischen mehreren Entitäten verknüpft werden können. Wenn während der Entitätsauflösung die Kriterien für eine Rollenalertregel erfüllt werden, generiert das System einen Rollenalert.

Obwohl die meisten Rollenalertregeln angeben, wann ein Rollenkonflikt vorliegt, können Sie eine Rollenalertregel definieren, bei der eine Entität, die einer Rolle zugeordnet ist, eine andere Entität kennt, die derselben Rolle zugeordnet ist. Beispielsweise kann es für Sie von Interesse sein, Beziehungen zwischen Ihren Kunden zu kennen und eine Rollenalertregel zu definieren (*Kunde kennt Kunde*), die jedes Mal einen Rollenalert generiert, wenn eine Kundenentität in Beziehung zu einer anderen Kundenentität in der Entitätendatenbank steht.

Da Entitäten aus mehreren Datensätzen bestehen (häufig aus verschiedenen Datenquellen) und da Rollen in der Regel nach Datenquelle zugewiesen werden, kann eine Entität mehreren Rollen zugewiesen werden. Es ist also auch möglich, eine Rollenalertregel zu definieren, die einen Rollenalert generiert, wenn einer Entität basierend auf den eingehenden Daten sowohl die Kundenrolle als auch die Betrügerrolle zugewiesen wird.

Anmerkung: Beachten Sie, dass sich die Anzahl Rollenalertregeln exponentiell erhöhen, wenn das System für die Verwendung einer hohen Anzahl Rollen konfiguriert ist.

Obwohl das System jede Beziehung erkennt, die gegen eine Rollenalertregel verstößt, meldet es standardmäßig nur einen Rollenalert für jede Entität zurück. Wenn das System z. B. erkennt, dass zwischen einer Entität, der die Rolle 'Mitarbeiter' zugeordnet ist, und zwei verschiedenen Lieferantenentitäten eine Beziehung besteht, und wenn eine Rollenalertregel konfiguriert ist, die einen Rollenalert generiert, wenn ein Mitarbeiter einen Lieferanten kennt, werden beide Konflikte erkannt und in die Datenbank geschrieben. Standardmäßig wird jedoch nur ein Rollenalert zurückgemeldet.

Beim Konfigurieren von Rollenalertregeln können Sie auch Alertfilter angeben, die steuern, ob das System einen neuen Alert generiert, wenn vorhandene Entitäten, die an einem zuvor generierten Alert beteiligt waren, um neue Identitäten oder neue Datenquellencodes erweitert werden.

Rollenalertinaktivierung:

Da Daten über die Entitäts- und Beziehungsauflösung verarbeitet werden, verändern sich die Entitäten und Beziehungen zwischen ihnen im Laufe der Zeit. Diese Änderungen, die auf der zeitlich unbegrenzten Analyse neuer und vorhandener Daten basieren, können zur Inaktivierung von Rollenalerts führen. Die Funktion für die Rollenalertinaktivierung von InfoSphere Identity Insight stellt den Analysten den aktuellsten Kontext bereit. Dadurch müssen die Analysten keine Zeit mehr in die Untersuchung nicht mehr aktiver Konflikte investieren.

Die Rollenalertinaktivierung entfernt beziehungsbasierte Rollenalerts, die weiterhin den Status **Anstehend** aufweisen. In der Regel wurden Alerts mit dem Status **Anstehend** noch nicht von einem Analysten geprüft oder verarbeitet. Wenn ein Rollenalert einen anderen Status aufweist, beispielsweise **Abgeschlossen** oder **Zugeordnet**, wird er nicht inaktiviert, auch wenn die Daten die Inaktivierung dieses Rollenalerts unterstützen. Einem Alert kann nur ein Status zugeordnet werden. Wenn der Alert bereits den Status **Zugeordnet** oder **Abgeschlossen** aufweist, wird er daher nicht inaktiviert.

Rollenalerts, die in einer nullstufigen Beziehung auftreten, werden ebenfalls inaktiviert, wenn eine Identität der Entität gelöscht oder ihre Auflösung aufgehoben wird.

Funktionsweise der Rollenalertinaktivierung

Beziehungsbasierte Rollenalerts können aus mehreren Gründen inaktiviert werden:

- Wenn eine Entität ihre Entitäts-ID während der erneuten Auflösung oder der Auflösungsaufhebung im Rahmen der Entitätsauflösung ändert, wird die Beziehung aufgehoben oder an eine neue Entitäts-ID übertragen.
- Wird eine einzelne Entität aufgrund neuer Daten zu zwei separaten Entitäten, wird jeder neuen Entität eine neue Entitäts-ID zugeordnet. Durch die vollständi-

ge Zurückführung werden alle Daten, die zur neuen Entität gehören, aus der alten Entität entfernt und der neuen hinzugefügt, einschließlich der Rollen, die beziehungsbasierte Rollenalerts erstellen.

- Wenn Daten aus der Entitätendatenbank gelöscht werden, kann eine komplette Entität oder eine Schlüsselkomponente einer Beziehung entfernt werden, wodurch ein Rollenalert inaktiviert wird.
- Wenn Daten als generisch markiert sind, können sie nur noch beschränkt oder überhaupt nicht mehr zum Ermitteln von Beziehungen verwendet werden. Wird eine Beziehung entfernt, werden alle Rollenalerts inaktiviert, die von dieser Beziehung abhängig sind.

Austauschrollenalerts

Bei jeder Inaktivierung eines Rollenalerts wertet die Pipeline automatisch alle Konflikte im Beziehungspfad neu aus und sucht nach Daten, die einen alternativen beziehungsbasierten Konflikt unterstützen.

Ein *Beziehungspfad* ist die Kette der Entitäten und Attribute, die eine Entität mit einer anderen verknüpfen. Die Länge des Beziehungspfads wird über die Konfiguration für die Abgrenzungsgrade festgelegt. Die Abgrenzungskonfigurationen werden über die Konfigurationskonsole festgelegt.

Bewertung

Während der Entitätsauflösung berechnet das System, wie stark die Attribute für eine eingehende Identität mit den Attributen einer vorhandenen Entität übereinstimmen. Die Ergebnisse dieser Berechnungsanalyse sind Bewertungen, mit denen das System Identitäten in Entitäten auflöst und Beziehungen zwischen Entitäten erkennt.

Auflösungsbewertungen

Die Auflösungsbewertung ist der Wert, der während der Entitätsauflösung als Ergebnis der Bestätigungs- und Zurückweisungsverarbeitung zugeordnet wird und die Wahrscheinlichkeit definiert, dass die verglichenen Identitäten dieselbe Entität darstellen. Diese benutzerdefinierte Bewertung wird zur Auflösung einer neuen Identität in eine vorhandene Entität verwendet.

Beim Verarbeiten eingehender Identitäten für die Entitätsauflösung vergleicht die Pipeline die gemeinsamen Attributwerte für die Attribute der eingehenden Identität und jeder Entität in der Kandidatenliste. Ein Teil des Vergleichs besteht in der Berechnung von Bewertungen, die darstellen, wie stark die Attributwerte übereinstimmen. Diese Bewertungen werden dann mit den konfigurierten Schwellenwerten und der Auflösungsbewertung für jede Auflösungsregel verglichen. Nachdem der Entitätsauflösungsprozess einen Bestätigungs- und Zurückweisungsprozess zum Verhindern falscher positiver Werte verwendet hat, erstellt das System eine Basisauflösungsbewertung für die eingehende Identität und die Entität in der Kandidatenliste.

Wenn mindestens ein Attribut für weitere Bestätigung oder Zurückweisung konfiguriert ist, wertet der Prozess dieses Attribut bzw. diese Attribute aus. Die Ergebnisse wirken sich auf die Basisauflösungsbewertungen für die eingehende Identität und die Kandidatenentität aus. Wenn die Attributwerte übereinstimmen, kann die Auflösungsbewertung durch das Hinzufügen der konfigurierten Anzahl Punkte positiv beeinflusst werden. Wenn die Attributwerte nicht übereinstimmen, kann die Beziehungsbewertung durch das Subtrahieren der konfigurierten Anzahl Punkte negativ beeinflusst werden. Wenn Sie ein Attribut für Bestätigungen oder Zurück-

weisungen konfigurieren, geben Sie die Anzahl Punkte an, um die die Basisauflösungsbewertung erhöht oder gesenkt werden soll.

Das System vergleicht dann die sich ergebende Auflösungsbewertung der eingehenden Identität und der Kandidatenentität mit jeder Auflösungsregel. Wenn die Auflösungsbewertung die konfigurierte Bewertung der Übereinstimmungswahrscheinlichkeit für die Auflösung für die Auflösungsregel erfüllt oder übersteigt, löst das System die eingehende Identität in die Kandidatenentität auf und erstellt eine zusammengesetzte Entität in der Entitätendatenbank.

Beziehungsbewertungen

Die Beziehungsbewertung ist der Wert, der während der Entitätsauflösung als Ergebnis der Anwendung der Auflösungsregeln zugeordnet wird und der definiert, wie eng die beiden verglichenen Identitäten zusammengehören. Diese Bewertung ist benutzerdefiniert und wird verwendet, um Entitätsbeziehungen zu erkennen.

Während der Entitätsauflösung vergleicht die Pipeline die eingehende Identität (die nicht in eine Entität aufgelöst werden kann) mit den verbleibenden Entitäten in der Kandidatenliste. Obwohl diesen Kandidatenentitäten nicht in die eingehende Identität aufgelöst werden können, werden sie auf Beziehungen ausgewertet.

Während des Beziehungserkennungsprozesses ermitteln die Pipelines Beziehungen, indem sie für jeden Attributdatenwert, den die eingehende Identität und die Entitäten in der Kandidatenliste gemeinsam haben, ab der ersten Entität eine Beziehungsbewertung berechnen:

- Wenn die Beziehungsbewertung die für Beziehungen konfigurierten Kriterien erfüllt (nach Abgrenzungsgraden), ermittelt das System, dass die beiden Entitäten zusammengehören. Die Beziehung wird in beide zusammengesetzte Entitäten geschrieben. Das System prüft dann die konfigurierten Rollenalertregeln, um zu ermitteln, ob die Beziehung von Interesse ist. Wenn das der Fall ist, generiert das System einen Alert. Andernfalls steuert das System die nächste Entität in der Kandidatenliste an.
- Wenn die Beziehungsbewertung die für Beziehungen konfigurierten Kriterien nicht erfüllt, steuert der Prozess die nächste Entität in der Kandidatenliste an, bis alle Entitäten hinsichtlich Beziehungen ausgewertet wurden.

Ereignismanager

Der Ereignismanager erweitert die Funktionalität von IBM InfoSphere Identity Insight durch Kombinieren nahezu in Echtzeit erfolgender Ereignisanalyse und Ereignisüberwachung mit Identitäts- und Beziehungsauflösung. Wenn der Ereignismanager aktiviert ist, ermöglicht er es Ihrem Unternehmen, Geschäftsereignisse zu verfolgen und bei verdächtigen oder interessanten Ereignissen Alerts auszugeben, sodass Sie rechtzeitig geeignete Maßnahmen ergreifen und gegen Bedrohungen und Betrug vorgehen können.

Da die Bedrohungs- und Betrugsszenarios sich ständig ändern, bietet der Ereignismanager Ihnen die Flexibilität, die zu verfolgenden Ereignistypen zu definieren und die Geschäftsregeln für das Verarbeiten von Ereignissen und das Generieren von Ereignisalerts zu konfigurieren. Diese Regeln stellen einen Satz von Kriterien dar, mit dem der Ereignismanager festlegt, wie Ereignisse verarbeitet werden und was einen Ereignisalert auslöst. Sie konfigurieren die Geschäftsregeln auf der Basis Ihrer Geschäftsanforderungen und -szenarios.

Sie legen außerdem fest, was einen Ereignisalert darstellt. Ereignisalerts werden normalerweise nicht von einem einzigen Ereignis ausgelöst, sondern von einer Reihe komplexer Ereignisse, die zu verschiedenen Zeiten in verschiedenen Kontexten auftreten. Sie können z. B. eine Geschäftsregel definieren, die Geldüberweisungen über einen bestimmten Zeitraum hinweg nach Kunde zusammenfasst und einen Alert generiert, wenn die Gesamtsumme den gesetzlich zulässigen Grenzwert überschreitet. Oder Sie können eine Geschäftsregel definieren, die Sie benachrichtigt, wenn zwei Käufe mit derselben Kreditkartennummer innerhalb einer Stunde in mehr als 300 km Abstand voneinander getätigt werden.

Funktionsweise der Ereignisverarbeitung

Der Ereignismanager von IBM InfoSphere Identity Insight arbeitet mit dem komplexen Ereignisprozessor von IBM Active Middleware™ Technology, der sich aus zwei Teilen zusammensetzt - der CEP-Engine und dem Eclipse™-basierten Tool **Rule Author**. Sie konfigurieren die Geschäftsregeln für Ereignisse und Ereignisalerts im Tool **Rule Author** und exportieren diese Konfiguration anschließend als Datei `CEP.XML`. Wenn die Pipeline nach der Aktivierung des Ereignismanagers formatierte eingehende UMF-Daten im Datensegment EVENT entdeckt, verarbeitet sie die Daten für die Identitätsauflösung und leitet die verarbeiteten Daten an die CEP-Engine weiter. Die CEP-Engine verarbeitet die Ereignisdaten für die in der Datei `CEP.XML` konfigurierten Ereignisgeschäftsregeln und gibt die Entscheidungsinformationen an die IBM InfoSphere Identity Insight-Pipeline zurück, wo die Ereignisinformationen in der Entitätendatenbank gespeichert werden. Wenn Ereignisalerts mit einem Ereignis oder einer Kombination von Ereignissen verknüpft sind, können Sie den Ereignismanager so konfigurieren, dass diese Ereignisalerts in Visualizer oder einer anderen Visualisierungskomponente für die weitere Analyse und Disposition angezeigt werden.

Sie können Ihre Clientanwendung auch so konfigurieren, dass die CEP-Engine sofortige Entscheidungen an sie zurückgeben kann, sodass für die Vertreter Ihres Unternehmens Informationen direkt vor Ort bereitgestellt werden. Die CEP-Engine könnte z. B. Ihre Kundendienstmitarbeiter unverzüglich veranlassen, eine Überweisung zu stoppen, die den gesetzlich zulässigen Höchstbetrag für Überweisungen innerhalb eines Zeitraums von 24 Stunden überschreitet.

Ereignisse

Ereignisse stellen Informationen über etwas dar, das sich in einem Geschäftsbereich zugetragen hat, z. B. eine Konteneröffnung oder eine Überweisung durch einen Kunden. Im Ereignismanager enthalten Ereignisse Attribute, die auf den entsprechenden Ereignistypen basieren.

Ereignisalerts

Ein Ereignisalert tritt auf, wenn mindestens ein Ereignis festgelegte Kriterien über einen angegebenen Zeitraum erfüllt. Ereignisalerts basieren auf komplexen Ereignisgeschäftsregeln und weiteren, in einer Ereignisregeldatei (`cep.xml`) enthaltenen Konfigurationen. Diese Alerts können interessante Situationen aufzeigen, z. B. dass in der letzten Stunde zwei oder mehr Kauftransaktionen über mehr als 10.000 Euro an Orten, die 200 Kilometer voneinander entfernt sind, aufgetreten sind.

Ereignistypen

Ereignistypen kategorisieren Ereignisse und definieren die Maßeinheit für den Wert, der Ereignissen im Ereignismanager zugeordnet ist. Beispiele von Ereignistypen sind Geldüberweisungen, Kontoeröffnungen oder Kreditkartentransaktionen.

Ereignistypen sind für die Ereignisverarbeitung erforderlich, da die benutzerdefinierten Geschäftsregeln, die der Ereignisprozessor verwendet, einen bestimmten Ereignistyp aufrufen. Wenn der Ereignistyp nicht vorhanden ist, kann der Ereignisprozessor das Ereignis nicht verarbeiten.

Ereignisregeln

Die Ereignisgeschäftsregeln sind eine Gruppe von Geschäftsregeln, die festlegen, wie eingehende Ereignisdatensätze von der CEP-Engine (Complex Event Processing) verarbeitet werden und welcher Typ von Ereignisantwort (z. B. ein Ereignisalert) an die Pipeline und die Clientanwendung zurückgegeben wird. Wollen Sie konfigurieren Ereignisregeln im Eclipse-basierten™ Tool **CEP Rule Author**. Ereignisregeln sind unter einem CEP-Projekt gruppiert und werden in eine Ereignisregeldatei `cep.xml` exportiert.

Sie konfigurieren Ereignisregeln, um auf der Basis der für Ihr Unternehmen oder Ihre Analysten interessanten Elemente Informationen und Alerts zurückzugeben. Ereignisregeln können so konfiguriert werden, dass sie Alerts zu Daten eines einzelnen eingehenden Ereignisdatensatzes generieren. Die Mehrzahl der Ereignisregeln gruppieren jedoch eine Sammlung komplexer Ereignisdaten und lösen einen Alert aus, wenn ein bestimmter Schwellenwert erreicht oder eine bestimmte Bedingung erfüllt ist.

Im Tool **Rule Author** werden die Ereignisgeschäftsregeln *Situationen* genannt. Weitere Informationen finden Sie in „CEP-Terminologie" auf Seite 33.

Allgemeine Ereignisregeln enthalten Summier- oder Zählfunktionen. Sie können beispielsweise eine Ereignisregel so konfigurieren, dass sie einen Ereignisalert generiert, wenn eine Entität innerhalb von 24 Stunden mehr als 15.000 Euro überweist.

Erste Schritte mit dem Ereignismanager

Die folgenden Schritte können als Prüfliste für das Konfigurieren und Verwenden des Ereignismanagers dienen.

Vorgehensweise

1. Erforderlich: Installieren Sie das Eclipse-basierte CEP-Tool 'Rule Author'. Das Eclipse™-basierte Tool **Rule Author** wird nicht automatisch mit dem Produkt installiert. (Die Funktionalität des Ereignismanagers und die CEP-Engine werden automatisch installiert.) Das Tool **Rule Author** ist in einer ZIP-Datei im Produktdownload enthalten.
2. Erforderlich: Verwenden Sie das Tool **Rule Author**, um ein CEP-Projekt zu erstellen, in dem alle Ereignisregeln und Konfigurationen für den Ereignismanager gruppiert werden.
3. Erforderlich: Importieren Sie im Tool **Rule Author** die Ereignisregeldatei `cep.xml` in das CEP-Projekt und passen Sie die Datei an, indem Sie die Ereignisregeln erstellen, die den Anforderungen Ihrer Szenarien für die Geschäftsereignisverarbeitung und die Alertverwendung entsprechen. Bevor Sie eine Originaldatei ändern, sollten Sie sie vorsichtshalber sichern oder in ein anderes Verzeichnis kopieren.

   Wichtig: Die für die Benennung der Ereignisregeldatei verwendete Groß-/Kleinschreibung muss inbesondere in der UNIX-Umgebung beachtet werden. Der Dateiname darf nur Kleinbuchstaben enthalten.

4. Erforderlich: Exportieren Sie die Ereignisregeldatei `cep.xml`. Die CEP-Engine und der Ereignismanager verwenden diese XML-Ereignisregeldatei zur Verarbeitung von Ereignissen und zum Ermitteln, wann Alerts generiert werden sollen. Die exportierte XML-Datei muss den Namen `cep.xml` haben und sich im Verzeichnis *ausgangsverzeichnis_für_produktinstallation*`/ibm-home/gem/` befinden.
5. Erforderlich: Konfigurieren Sie Systemparameter für den Ereignismanager in der Konfigurationskonsole.

   Hinweis: Damit diese Änderungen der Systemkonfiguration in Kraft treten, müssen Sie alle aktiven Pipelines stoppen und erneut starten. Sie können entweder alle aktiven Pipelines vor dem Konfigurieren von Systemparametern und Ereignistypen für den Ereignismanager stoppen oder Sie stoppen alle aktiven Pipelines nach dem Konfigurieren der Systemparameter und Ereignistypen für den Ereignismanager und starten die Pipelines dann erneut.
6. Erforderlich: Konfigurieren Sie Ereignistypen in der Konfigurationskonsole.

   Hinweis: Damit diese Änderungen der Systemkonfiguration in Kraft treten, müssen Sie alle aktiven Pipelines stoppen und erneut starten. Sie können entweder alle aktiven Pipelines vor dem Konfigurieren von Systemparametern und Ereignistypen für den Ereignismanager stoppen oder Sie stoppen alle aktiven Pipelines nach dem Konfigurieren der Systemparameter und Ereignistypen für den Ereignismanager und starten die Pipelines dann erneut.
7. Gehen Sie wie folgt vor, um Ereignisalerts in den Analyst Toolkit-Anwendungen anzuzeigen:
   a. Optional: Identity Insight enthält bereits Standardaktivitätscodes zur Verarbeitung von Ereignisalerts (**Anstehend**, **Zugeordnet** und **Geschlossen**). Aber Sie können, falls gewünscht, in der Konfigurationskonsole zusätzliche Aktivitätscodes für Ereignisalerts erstellen. Stoppen Sie alle aktiven Pipelines, bevor Sie die Aktivitätscodes erstellen, und starten Sie dann die Pipelines wieder, nachdem die Aktivitätscodes erstellt wurden.
   b. Optional: Sie können Ereignisalerts prüfen, den Status von Ereignisalerts ändern, sich selbst Ereignisalerts zuordnen oder Ereignisalerts anderen Alertgruppen für andere Analysten zuordnen.
   c. Optional: Wenn Sie die kompletten Details zu einem bestimmten Ereignisalert anzeigen lassen wollen, können Sie den Detailsbericht für Ereignisalerts generieren.
   d. Optional: Sie können das Ereignisalertprotokoll für eine Entität in der Entitätszusammenfassung anzeigen.
   e. Optional: Von der Entitätszusammenfassung aus können Sie **Ereignisse anzeigen** anklicken, um alle Ereignisse, die mit der Entität verknüpft sind, anzuzeigen, auch solche, die keinen Ereignisalert generiert haben. Oder Sie können **Bericht** anklicken, um einen Bericht zu allen Ereignissen zu drucken, der auch alle Ereignisse beinhaltet, die mit der Entität verknüpft sind.
8. Erforderlich: Verwenden Sie die Definitionen von EVENT-Datensegmenten, um Ereignisverarbeitungsinformationen in die von Ihnen konvertierten UMF-Daten aufzunehmen, damit diese an die Pipelines gesendet werden.
9. Optional: Wenn Sie Systemnachrichten (einschließlich Ereignismanagernachrichten) an Ihre Clientanwendung senden wollen, müssen Sie eine HTTP-Pipeline verwenden. Außerdem muss garantiert sein, dass Ihre Clientanwendung Nachrichten vom Standarddokument für die SYSTEM_MESSAGE-Rückgabe empfangen kann.

10. Optional: Nachdem der Ereignismanager Ereignisse verarbeitet hat, können Sie die Ereignismanagerprotokolldateien und die zugehörigen Konfigurationskonsolenprotokolldateien überprüfen.

Aktivieren des Ereignismanagers in der Konfigurationskonsole

Bevor Sie Ereignisse mithilfe des Ereignismanagers verarbeiten können, müssen Sie den Ereignismanager in der Konfigurationskonsole aktivieren und konfigurieren.

Informationen zu diesem Vorgang

Vorgehensweise

1. Klicken Sie in der Konfigurationskonsole die Registerkarte **Systemkonfiguration** an.
2. Modifizieren Sie den Wert von **Ereignisverarbeitung aktivieren**, um die Ereignisverarbeitung zu aktivieren.
3. Modifizieren Sie den Wert von **Ereignisprozessor-URI**, um den Universal Resource Identifier (URI) als CEP zu konfigurieren. Der Standardwert sollte http://localhost:13510/gem lauten.
4. Modifizieren Sie den Wert für **Zeitlimit für Ereignisprozessor**, um die Einstellung für die gesamte Ereignisverarbeitungsdauer zu erhöhen. Diese Einstellung gibt die Zeit an (in Sekunden), die die Pipeline auf eine Antwort vom externen Ereignisprozessor (CEP) wartet, bevor ein Zeitlimit überschritten und ein Fehler ausgegeben wird.
5. Modifizieren Sie den Wert für **Ereignisprotokollfenster**, um die Anzahl der Tage im Ereignisverlauf zu modifizieren, die zur Verwendung bei der Auswertung eines neuen eingehenden Ereignisses an die Pipeline gesendet werden.
6. Klicken Sie **Speichern** an.

Konfigurieren des CEP-Moduls des Ereignismanagers

In IBM InfoSphere Identity Insight bezieht sich *CEP* (Complex Event Processing) auf die mit dem Produkt bereitgestellten CEP-Tools. Diese Tools stellen die Komponenten im Ereignismanager dar, mit denen die Identitäts- und Beziehungsauflösung erweitert wird, um Ereignistransaktionen verarbeiten und Ereignisalerts generieren zu können. Dieser Abschnitt enthält Informationen zum Konfigurieren der CEP-Tools für ihre ordnungsgemäße Funktionsweise im Ereignismanager.

Architektur

Die CEP-Komponente des Ereignismanagers besteht aus zwei Tools:

Eclipse™-basiertes Tool Rule Author
: Das Eclipse-basierte Tool **CEP Rule Author** ist die Komponente, die Sie zum Konfigurieren von Ereignisregeln und zu deren Export in die Datei `cep.xml` verwenden. Diese Ereignisregeldatei legt fest, wie Ereignisse verarbeitet werden und was einen Ereignisalert auslöst.

  Beim Installieren von IBM InfoSphere Identity Insight installieren Sie auch eine komprimierte Datei, die das Tool **Rule Author** und sein Benutzerhandbuch enthält. Sie müssen die Tooldateien jedoch zunächst dekomprimieren, bevor Sie mit der Konfiguration der Ereignisregeln beginnen können.

CEP-Engine (Complex Event Processing)
: Die CEP-Engine ist die Komponente, die eingehende Ereignisdaten gemäß der in der Datei `cep.xml` konfigurierten Ereignisregeln verarbeitet.

Wenn die Pipeline Daten empfängt, die mit dem Datensegment EVENT eines eingehenden UMF-Dokuments formatiert wurden, sendet sie diese Daten zur Ereignisverarbeitung an die CEP-Engine. Wenn die CEP-Engine die Ereignisdaten anhand der konfigurierten Datei `cep.xml` ausgewertet hat, sendet sie die Ergebnisse an die Pipeline zurück. Wenn die Ereignisdaten eine konfigurierte Ereignisregel erfüllen oder übererfüllen, sendet die CEP-Engine auch ein Signal zum Generieren eines Ereignisalerts an die Pipeline zurück. Ungeachtet dessen, ob ein Ereignisalert generiert wird, werden die endgültigen Ereignisdaten, die die Pipeline empfängt, in die Entitätendatenbank geschrieben.

Die CEP-Engine wird standardmäßig mit IBM InfoSphere Identity Insight installiert.

Diese CEP-Komponenten sind Teil einer bestimmten Version von IBM Active Middleware™ Technology, die im Ereignismanager enthalten ist. Diese CEP-Komponenten sind in dem von Ihnen erworbenen Produkt enthalten.

Datei cep.xml

Die Datei `cep.xml` enthält die Ereignisregeln und weitere Einstellungen, die für die Verarbeitung von Ereignisdaten und die Generierung von Ereignisalerts erforderlich sind. Die Ereignismanagerfunktion in der Pipeline und die CEP-Engine können nur Ereignisse mit der Ereignisregeldatei `cep.xml` verarbeiten. Diese Datei weist das XML-Format (E**x**tensible **M**arkup **L**anguage) auf, da Daten, die in die Pipeline gehen, das UMF-Format (**U**niversal **M**essaging **F**ormat) aufweisen, ein auf XML basierendes Format.

Ein Beispiel der Datei `cep.xml` ist in Ihrer Produktinstallation enthalten. Diese enthält viele der erforderlichen Konfigurationseinstellungen, die der Ereignismanager für die Arbeit mit der CEP-Engine benötigt. Sie können die Beispieldatei `cep.xml` in ein CEP-Projekt importieren und anschließend die Ereignisgeschäftsregeln konfigurieren.

Anmerkung: Erstellen Sie eine Sicherungskopie der Originaldatei und speichern Sie diese in einem anderen Verzeichnis, bevor Sie die Ereignisregeldatei `cep.xml` importieren und Änderungen an dieser Datei vornehmen oder diese exportieren. Erwägen Sie bei jeder Änderung der Ereignisregeldatei die Verwendung eines Versionssteuerungssystems oder eines Systems zur Quellcodeverwaltung.

Zusätzliche Ressourcen für CEP

Weitere detaillierte Informationen zur Verwendung des Eclipse-basierten Tools **Rule Author** enthält das Benutzerhandbuch zum Tool. Das Handbuch mit dem Namen `AMT3.0.UserGuide.PDF` befindet sich im Verzeichnis *`installationspfad`*`/cep/`.

Installieren des Eclipse-basierten CEP-Tools 'Rule Author'

Führen Sie folgende Schritte aus, um das Eclipse™-basierte Tool **Rule Author** auf einer Workstation zu installieren. Der Ereignismanager und die CEP-Engine werden mit dem Produktinstallationsprogramm installiert. Das Tool **Rule Author** müssen Sie jedoch über eine in der Installation enthaltene ZIP-Datei installieren.

Vorbereitende Schritte

Das Tool **Rule Author** funktioniert nur auf einem Microsoft Windows-Betriebssystem und erfordert Java Version 1.5 oder höher.

Informationen zu diesem Vorgang

Sie verwenden das Tool **Rule Author**, um die Regeln und Schwellenwerte zu konfigurieren, die zur Überwachung Ihres Unternehmens verwendet werden, und Sie exportieren diese Informationen anschließend in die Ereignisregeldatei (`cep.xml`). Der Ereignismanager und die CEP-Engine (Complex Event Processor) verwenden die Ereignisregeldatei zum Verarbeiten von Ereignissen sowie zum Ermitteln von Ereignisalerts. Ereignisalerts können mit einem Einzelereignis oder einer Kombination von Ereignissen verknüpft sein. Sie können den Ereignismanager so konfigurieren, dass diese Ereignisalerts zur weiteren Analyse in Analyst Toolkit oder einem anderen Visualisierungstool angezeigt werden.

Gehen Sie wie folgt vor, um das Eclipse-basierte Tool **Rule Author** aus der ZIP-Datei zu installieren:

Vorgehensweise

1. Navigieren Sie zum Produktinstallationsverzeichnis.
2. Navigieren Sie zum Unterverzeichnis `/cep`.
3. Kopieren Sie die Datei `CEP_3.0.1.1.03.zip` auf ein Microsoft Windows-Clientsystem.
4. Dekomprimieren Sie die Datei `CEP_3.0.1.1.03 file` in *`laufwerkbuchstabe`*`:/CEP/`.

Nächste Schritte

Detaillierte Informationen zur Verwendung des Tools **Rule Author** finden Sie im Benutzerhandbuch, das sich in der Datei `cep/AMT3.0_UserGuide.PDF` befindet.

Starten des Tools 'Rule Author':

Sie müssen zuerst das Tool starten, bevor Sie das Eclipse-basierte™-Tool **Rule Author** verwenden können. Das Tool **Rule Author** wird von den IBM InfoSphere Identity Insight-Komponenten getrennt installiert und gestartet.

Informationen zu diesem Vorgang

Das Tool **Rule Author** funktioniert nur auf einem Client mit einem Microsoft Windows-Betriebssystem und erfordert Java Version 1.5 oder höher.

Vorgehensweise

1. Öffnen Sie Microsoft Windows Explorer und navigieren Sie in das Verzeichnis, in dem das Eclipse-basierte Tool **Rule Author** installiert ist.
2. Klicken Sie das Stapelscript `AmitIDE.cmd` doppelt an. Das Stapelscript öffnet die ausführbare Datei des Authoring-Tools für Regeln.

CEP-Terminologie

Einige der im Eclipse-basierten™ Tool **Rule Author** verwendeten Begriffe weichen möglicherweise von den in IBM InfoSphere Identity Insight und seinen Komponenten verwendeten Begriffen geringfügig ab. Dieses Glossar erleichtert Ihnen das Verständnis der CEP-Begriffe (Complex Event Processing) und ihrer Beziehung zum Ereignismanager und anderen Komponenten wie Visualizer.

Datei cep.xml
: Die Datei `cep.xml` enthält alle Ereignisgeschäftsregeln und alle für den Ereignismanager und die CEP-Engine erforderlichen CEP-Konfigurationsein-

stellungen zum Verarbeiten eingehender Ereignisdatensätze. Eine Ereignisregeldatei mit diesem Namen muss in das Verzeichnis *produktinstallationsverzeichnis*\ibm-home\gem\ exportiert werden.

Wichtig: Der Dateiname darf nur Kleinbuchstaben enthalten, insbesondere in UNIX-Umgebungen.

Sie verwalten mithilfe des Tools **Rule Author** die Ereignisregeldatei und exportieren sie.

Eine Beispielereignisregeldatei `cep.xml` ist in der IBM InfoSphere Identity Insight-Produktinstallation enthalten. Diese Beispieldatei enthält bereits viele der erforderlichen Einstellungen und Konfigurationen, die für die Arbeit mit dem Ereignismanager erforderlich sind. Sie können die Beispielereignisregeldatei `cep.xml` in das Tool **Rule Author** importieren und zunächst eine Sicherungskopie der Originaldatei erstellen, um anschließend Ereignisgeschäftsregeln hinzuzufügen und die Datei an die erforderliche Position zu exportieren. Erwägen Sie die Verwendung eines Versionssteuerungssystems oder eines Systems zur Quellcodeverwaltung, um die Datei vor und nach ihrer Änderung zu speichern.

CEP-Engine
Die CEP-Engine (Complex Event Processing) ist der Mechanismus, bei dem eingehende Ereignisdaten von der Pipeline verarbeitet und gemäß der in einem CEP-Projekt definierten Regeln ausgewertet werden. Das CEP-Projekt ist in der Datei `cep.xml` definiert, die über das Tool **Rule Author** konfiguriert und exportiert wird.

Die vom Ereignismanager zurzeit verwendete CEP-Engine ist Teil des Produkts IBM Active Middleware™ Technology. Die Version der CEP-Engine, die für den Ereignismanager erforderlich ist, stellt Teil von IBM InfoSphere Identity Insight dar und wird zusammen mit diesem Programm installiert. Sie müssen jedoch den Ereignismanager in der Konfigurationskonsole und die Ereignisregeln im Tool **Rule Author** konfigurieren, bevor Sie Ereignisse mit der CEP-Engine erfolgreich verarbeiten können.

CEP-Projekte
Projekte stellen eine übergeordnete Gruppe dar, die der CEP zur Aufnahme einer Gruppierung von Ereignissen, Lebensdauerangaben und Regeln verwendet. Wenn Sie den Ereignismanager verwenden wollen, müssen Sie **ein** CEP-Projekt erstellen, das alle Ereignisinformationen einschließlich der Geschäftsereignisregeln für die Ereignisse enthält, die Sie überwachen wollen. Der Ereignismanager verwendet jeweils nur ein CEP-Projekt, doch ein einzelnes Projekt kann mehrere Ereignistypen und mehrere Regeln pro Ereignistyp testen.

Sie erstellen und verwalten das CEP-Projekt im Tool **Rule Author**.

Tool 'Rule Author' (Eclipse-basiertes Tool 'Rule Author')
Mit diesem Tool können Sie CEP-Projekte, Ereignisse und andere Konfigurationen definieren, die Teil der von der CEP-Engine für die Verarbeitung von Ereignissen und die Generierung von Ereignisalerts verwendeten Ereignisregeldatei `cep.xml` sind.

Ereignisklassen
Wenn Sie den Ereignismanager verwenden wollen, muss Ihr CEP-Projekt die folgenden Ereignisklassen enthalten, die in der Beispieldatei `cep.xml` vorkonfiguriert sind:

- `EAS_START.event`: Gibt den Lebensdauerinitiator des Ereignismanagers an.

- EAS_STOP.event: Gibt das Lebensdauerabschlusssignal des Ereignismanagers an.
- EVENT.event: Definiert die Geschäftsregeln (oder Situationen) für den Ereignismanager, die zum Verarbeiten eingehender Ereignisdaten und zum Generieren von Ereignisalerts verwendet werden.

EVENT.event

Diese CEP-Ereignisklasse ordnet die Eingabedaten zu, die von der Pipeline zur Verarbeitung an die CEP-Engine weitergegeben werden. Die Zuordnung entspricht direkt der Tabelle GEM_EVENT in der Entitätendatenbank. Mithilfe des Tools **Rule Author** können Sie sicherstellen, dass die EAS_EVENT zugeordneten Attribute mit den Datenzuordnungen in der Tabelle GEM_EVENT übereinstimmen.

Lebensdauerangaben

In CEP gibt die Lebensdauer das Zeitintervall an, während dessen Situationen (Ereignisregeln) relevant sind. Eine Lebensdauer wird immer durch einen Initiator gestartet und durch ein abschlusssignal beendet. Die Lebensdauerangaben werden einer Ereignisklasse zugeordnet.

Im Ereignismanager muss die Ereignisklasse EVENT den Lebensdauerinitiator EAS_START und das Lebensdauerabschlusssignal EAS_STOP enthalten.

Situationen

Situationen in **Rule Author** sind äquivalent zu den *Ereignisregeln*. Sie können mit dem Tool **Rule Author** Situationen konfigurieren, mit denen die Geschäftsregeln definiert werden, die festlegen, welche Ereignisse oder Ereigniskombination für Ihr Unternehmen aussagekräftig sind/ist und welche einen Ereignisalert auslösen/auslöst.

Situationen werden einem CEP-Projekt und einer Ereignisklasse zugeordnet und sind in der Ereignisregeldatei cep.xml enthalten.

Wenn UMF-Daten in der Pipeline ankommmen, werden Datensätze (oder UMF_ENTITY-Eingabedokumente), die eine Definition des Datensegments EVENT enthalten, an die CEP-Engine gesendet. Die CEP-Engine wertet diese eingehenden Ereignisdaten für die in der Ereignisregeldatei cep.xml konfigurierten Situationen aus. Wenn ein Ereignis eine definierte Situation erfüllt oder übererfüllt, sendet die CEP-Steuerkomponente einen Ereignisalert an die Pipeline zurück, der in den Analyst Toolkit-Anwendungen oder in einem anderen Visualisierungstool Ihrer Wahl angezeigt werden kann.

Schwellenwertbedingung

Sie definieren Schwellenwertbedingungen als Teil einer Ereignisregel (Situation). Betrachten Sie Schwellenwertbedingungen als Datenfilter oder Datenschnellprüfungen. Bei der Verarbeitung prüft die CEP-Engine die eingehenden Ereignisdaten, um zu ermitteln, ob sie die angegebene Schwellenwertbedingung erfüllen, bevor die Daten gemäß der Regel verarbeitet werden. Wenn die Daten die Schwellenwertbedingung erfüllen, verarbeitet die CEP-Engine die Ereignisdaten gemäß der Regel. Wenn die Daten die Schwellenwertbedingung nicht erfüllen, geht die CEP-Engine zur nächsten Ereignisregel über.

Wenn Sie beispielsweise nur Ereignisse verarbeiten wollen, die in der Filiale 102 aufgetreten sind, erstellen Sie eine Schwellenwertbedingung mit der Angabe EVENT_LOC='102'.

Schlüssel UMF_LOG_ID

UMF_LOG_ID ist eine eindeutige fortlaufende Zahl, die jedem Datensatz bei seiner Verarbeitung zugewiesen wird. In einem CEP-Projekt stellt

UMF_LOG_ID einen Gruppierungsschlüssel dar, der allen erforderlichen Ereignisklassen und Lebensdauerindikatoren des Ereignismanagers zugeordnet ist. Dieser Gruppierungsschlüssel stellt sicher, dass alle eingehenden Datensätze mit demselben Schlüssel UMF_LOG_ID zusammen verarbeitet werden.

Wenn Sie die in Ihrem Produkt enthaltene Beispieldatei cep.xml in ein CEP-Projekt importieren, ist der Schlüssel UMF_LOG_ID bereits konfiguriert und den Ereignisklassen und Lebensdauerindikatoren des Ereignismanagers zugeordnet.

Konfigurieren der Ereignisregeldatei cep.xml

Die in der Ereignisregeldatei cep.xml konfigurierten Informationen legen fest, wie der Ereignismanager und der CEP-Engineprozess eingehende Ereignisdaten verarbeiten und welche Antworten an Ihre Clientanwendung, die Pipeline, die Entitätendatenbank und die Anwendungen zurückgegeben werden. Ereignisregeln stellen einen Großteil der in der Datei cep.xml enthaltenen Informationen dar, die Regeln sind jedoch nicht die einzigen erforderlichen Informationen. Für die ordnungsgemäße Verarbeitung von Ereignissen durch den Ereignismanager müssen verschiedene weitere Elemente und Einstellungen ebenfalls einbezogen werden.

Ihr Produkt enthält eine Beispieldatei cep.xml, in der alle erforderlichen Elemente und Einstellungen bereits konfiguriert vorliegen. Wenn Sie die Beispieldatei cep.xml importieren, müssen Sie diese Elemente oder Einstellungen nicht konfigurieren oder ändern, sondern können sich auf die Konfiguration der Ereignisgeschäftsregeln und deren Hinzufügung zur Datei cep.xml konzentrieren. Da Ereignisregeln in jedem Unternehmen eindeutig sind, enthält die Beispieldatei cep.xml keine vorkonfigurierten Ereignisregeln (oder Situationstypen).

Erforderliche Elemente und Einstellungen für die Datei cep.xml

Diese Informationen dienen Ihnen als Referenz. Wenn Sie die bereitgestellte Beispieldatei cep.xml nicht importieren wollen, sondern eine völlig neue Datei erstellen wollen, können Sie anhand dieser Informationen sicherstellen, dass die Datei alle erforderlichen Elemente und Einstellungen aufweist. Wenn die Ereignisregeldatei cep.xml, die Sie zur Verwendung mit dem Ereignismanager exportieren, nicht vollständig ist (d. h. diese Informationen nicht enthält), kann der Ereignismanager die eingehenden Ereignisdaten nicht verarbeiten.

Ereignisklassen

Ereignisklassen beschreiben die verschiedenen Ereignisstrukturen, die von der CEP-Engine erkannt werden müssen. Die folgenden Ereignisklassen müssen Bestandteil der Ereignisregeldatei cep.xml sein, damit sie Ereignisse verarbeiten können:

EAS_START.event

Diese Ereignisklasse wird der Lebensdauerinitiator für den Ereignismanager oder das Signal für die CEP-Engine zum Starten der Ereignisverarbeitung.

EAS_STOP.event

Diese Ereignisklasse wird das Lebensdauerabschlusssignal für den Ereignismanager oder das Signal für die CEP-Engine zum Stoppen der Ereignisverarbeitung.

EVENT.event

Diese Ereignisklasse stellt die Basis für jede von Ihnen erstellte Ereignisgeschäftsregel dar. Sie enthält die Informationen, die die ein-

gehenden Ereignisdatensatzdaten der Ereignismanagertabelle (GEM_EVENT) und dem Datensegment EVENT zuordnen.

Lebensdauer

In CEP ist die Lebensdauer ein Zeitintervall, während dessen bestimmte Ereignisregeln relevant sind. Da die Pipeline Daten echtzeitnah verarbeitet, dient die Lebensdauer ausschließlich dazu, den Anfang und das Ende eines Ereignisdatensatzes zu melden.

Die für die Ereignismanagerverarbeitung erforderlichen Informationen zur Lebensdauer umfassen die folgenden Elemente:

EAS_START

Dieses Element ist der erforderliche Lebensdauerinitiator und gibt den Anfang eines Ereignisses an. Sie legen dieses Lebensdauerelement in der Tabelle **Event Initiators** auf der Registerkarte **Lifespan: Initiators** fest.

EAS_STOP

Dieses Element ist das erforderliche Lebensdauerabschlusssignal und gibt das Ende eines Ereignisses an. Sie wählen das abschlusssignal für **Terminate By Event** auf der Registerkarte **Lifespan: Terminators & Keys** aus.

UMF_LOG_ID-Gruppierungsschlüssel

UMF_LOG_ID ist eine eindeutige fortlaufende Zahl, die jedem Datensatz bei seiner Verarbeitung zugewiesen wird. In einem CEP-Projekt stellt der UMF_LOG_ID-Gruppierungsschlüssel sicher, dass alle eingehenden Datensätze mit demselben UMF_LOG_ID-Gruppierungsschlüssel zusammen verarbeitet werden. Dieser Gruppierungsschlüssel ist allen Ereignisklassen und Lebensdauerindikatoren zugeordnet.

EVENT.event-Attribute

Die für diese Ereignisklasse erforderlichen Attribute werden direkt dem Datensegment EVENT zugeordnet. Dies sind die Felder in der Tabelle GEM_EVENT der Entitätendatenbank. Falls erforderliche Attribute von EVENT.event fehlen, schlägt die Ereignisverarbeitung fehl. Möglicherweise werden Fehlernachrichten angezeigt, die beispielsweise über ungültigen oder fehlerhaften XML-Code oder über fehlende Informationen in der XML-Datei der CEP-Konfiguration informieren.

Geben Sie diese Attribute auf der Registerkarte **Situation**: **General & Event** jeder Ereignisregel an.

Erstellen eines CEP-Projekts:

CEP-Projekte stellen eine Gruppierung von Ereignisregeln, Lebensdauerangaben und weiteren Ereignisinformationen dar, die vom Ereignismanager und von der CEP-Engine verwendet werden. CEP-Projekte sind Bestandteil der Ereignisregeldatei cep.xml und werden im Eclipse-basierten™ CEP-Tool **Rule Author** erstellt und verwaltet. Sie müssen zunächst ein CEP-Projekt definieren, bevor Sie Ereignisgeschäftsregeln für den Ereignismanager konfigurieren können.

Vorbereitende Schritte

- Das CEP-Tool **Rule Author** muss bereits installiert sein und die zugehörigen Dateien müssen dekomprimiert sein.
- Das CEP-Tool **Rule Author** funktioniert nur unter einem Microsoft Windows-Betriebssystem und erfordert Java Version 1.5 oder höher.

Vorgehensweise

1. Wählen Sie im CEP-Tool **Rule Author File** > **New** > **Project** aus.
2. Wählen Sie **Event Processing Project** aus und klicken Sie **Next** an.
3. Klicken Sie **Finish** an. Das CEP-Projekt wird im linken Navigationsteilfenster angezeigt.

Nächste Schritte

Importieren Sie die in der Produktinstallation enthaltene Beispielereignisregeldatei `ibm-home\gem\cep.xml`. Diese Datei enthält bereits die für die Arbeit mit dem Ereignismanager erforderlichen Elemente und Einstellungen. Nachdem Sie diese erforderlichen Objekte in das CEP-Projekt importiert haben, können Sie die Ereignisgeschäftsregeln konfigurieren und anschließend die endgültige Ereignisregeldatei `cep.xml` exportieren, um die Verarbeitung von Ereignissen über den Ereignismanager zu starten.

Importieren der Ereignisregeldatei cep.xml:

Die Ereignisregeldatei `cep.xml` enthält die Informationen, die von der CEP-Engine und vom Ereignismanager zum Verarbeiten von Ereignissen und zum Generieren von Ereignisalerts verwendet werden. Eine Beispieldatei `cep.xml` ist in Ihrer Produktinstallation enthalten, die die für das Arbeiten mit dem Ereignismanager erforderlichen Elemente und Einstellungen bereits enthält. Sie brauchen also keine völlig neue Datei zu erstellen, sondern können die vorhandene Datei `cep.xml` in ein CEP-Projekt importieren.

Vorbereitende Schritte

- Erstellen Sie eine Backup-Kopie der ursprünglichen Ereignisregeldatei `cep.xml`, damit Sie, falls erforderlich, zur Originaldatei zurückkehren können. Erwägen Sie die Verwaltung der Datei in einem Versionssteuerungssystem oder in einem System zur Quellcodeverwaltung.
- Das Eclipse-basierte™ Tool **Rule Author** muss installiert sein und die zugehörigen Dateien müssen dekomprimiert sein.
- Beachten Sie, dass das Tool **Rule Author** nur auf einem Client mit einem Microsoft Windows-Betriebssystem funktioniert und Java Version 1.5 oder höher erfordert.
- Sie müssen bereits ein CEP-Projekt im Tool **Rule Author** erstellt haben.

Vorgehensweise

1. Wählen Sie im Tool **Rule Author File** > **Import** aus.
2. Wählen Sie **Event Processing Definition** aus und klicken Sie **Next** an.
3. Navigieren Sie zur Datei `cep.xml` und wählen Sie sie aus. Denken Sie daran, den Standarddateityp von `DEF` in `XML` zu ändern. Diese Datei befindet sich in der Regel im Verzeichnis *`produktinstallationsverzeichnis`*`\ibm-home\gem`.
4. Überprüfen Sie die folgenden Elemente:
   - Stellen Sie sicher, dass alle Dateiinhalte ausgewählt sind. (Blenden Sie gegebenenfalls den obersten Ordner ein, um die Dateiinhalte zu prüfen.)
   - Stellen Sie sicher, dass der korrekte CEP-Projektname angezeigt wird. (Navigieren Sie, falls erforderlich, zum Projekt und wählen Sie es aus.)
5. Klicken Sie **Finish** an. Klicken Sie **OK** an, um die vorhandene Datei zu überschreiben, wenn Sie diese Nachricht empfangen. Wenn die Datei erfolgreich importiert wurde, werden im Tool **Rule Author** mehrere Pluszeichen im linken Navigationsteilfenster angezeigt.

Nächste Schritte

Fügen Sie Geschäftsereignisregeln hinzu und exportieren Sie anschließend die Ereignisregeldatei `cep.xml` in das Verzeichnis *produktinstallationsverzeichnis*`\ibm-home\gem\`.

Exportieren der Ereignisregeldatei cep.xml:

Damit der Ereignismanager die CEP-Regeln (Complex Event Processing) ausführen kann, müssen Sie die Ereignisregeldatei `cep.xml` exportieren, die Sie im Eclipse-basierten™ Tool **Rule Author** konfiguriert haben.

Vorbereitende Schritte

Das Tool **Rule Author** funktioniert nur auf einem Client mit einem Microsoft Windows-Betriebssystem und erfordert Java Version 1.5 oder höher.

Informationen zu diesem Vorgang

- Wenn die CEP-Engine beim Exportieren der Ereignisregeldatei bereits betriebsbereit ist, müssen Sie die Datei auf dem IBM WebSphere-Server erneut laden, damit die Änderungen, die an der neuen exportierten Ereignisregeldatei `cep.xml` vorgenommen wurden, berücksichtigt werden.

Vorgehensweise

1. Wählen Sie im Tool **Rule Author File** > **Export** aus.
2. Wählen Sie **Event Processing Definition** aus und klicken Sie **Next** an.
3. Wählen Sie das CEP-Projekt aus.
4. Setzen Sie die Definitionsdatei für die Ereignisverarbeitung auf die neue Ereignisregeldatei `cep.xml`. Die Datei befindet sich in der Regel im Verzeichnis *produktinstallationsverzeichnis*`\ibm-home\gem\cep.xml`.
5. Klicken Sie **Finish** an. Wenn Sie das System vor dem Überschreiben einer vorhandenen Datei `cep.xml` warnt, klicken Sie **OK** an.
6. Optional: Wenn der IBM WebSphere-Server zurzeit aktiv ist, laden Sie die CEP-Regeln erneut. Wenn die CEP-Engine auf dem Produktanwendungsserver startet, lädt CEP die aktuelle Ereignisregeldatei `cep.xml`. Wenn während des Exports der Datei der WebSphere-Server aktiv ist, werden die Änderungen erst nach dem erneuten Laden der neuen Datei `cep.xml` berücksichtigt.
   a. Öffnen Sie ein Web-Browserfenster und navigieren Sie zum WebSphere-Server. Beispiel: `http://localhost:13510/gem`.
   b. Klicken Sie **Reload Rules** an.

      Anmerkung: Der WebSphere-Server bestätigt nicht explizit, dass die Regeln erneut geladen wurden.

Richtlinien für die Konfiguration von Ereignisregelergebnissen

Ereignisregeln definieren, wie Ereignisse verarbeitet werden und welche Situationen Ereignisalerts generieren. Ereignisregeln (im Eclipse™-basierten Tool **CEP Rule Author** *Situationstypen* genannt) sind in der Ereignisregeldatei `cep.xml` enthalten, die vom Ereignismanager und der CEP-Engine zum Verarbeiten eingehender Ereignisdaten verwendet wird. Die von Ihnen definierten komplexen Ereignisregeln sind in Ihrem Unternehmen eindeutig.

Berücksichtigen Sie die folgenden Aspekte, bevor Sie mit der Definition von Ereignisregeln beginnen, damit die Regeln im Ereignismanager funktionieren:

- Beachten Sie, dass sich die Ereignisregeln auf eine Entität und die Transaktionen beziehen müssen, die eine Entität ausführen kann. Entitäten sind in der Regel Personen, können jedoch auch Orte oder Dinge darstellen. Ein Schiff kann beispielsweise auch eine Entität sein.
- Ereignisregeln müssen als Prozedurdeklarationsanweisung (wie 'Ort=Texas') oder als mathematischer Ausdruck (Summe, Anzahl, Mittelwert) mit Zeitangabe angegeben werden.

Für einzelne Ereignisgeschäftsregeln erforderliche Situationsattribute

Wenn Ereignisdaten vom komplexen Ereignisprozessor an die Entitätendatenbank zurückgegeben werden sollen, müssen Sie die erforderlichen Situationsattribute für jede von Ihnen erstelle Ereignisgeschäftsregel manuell hinzufügen. Diese Attribute sind nicht Teil der Beispielereignisregeldatei `cep.xml`. Beim Importieren dieser Originaldatei Ereignisgeschäftsregeln (Situationen) daher nicht automatisch erstellt oder diese Attribute werden nicht automatisch neuen oder vorhandenen Regeln hinzugefügt.

Diese Situationsattribute ordnen Ereignisdaten direkt der Ereignismanagertabelle `GEM_EVENT` zu (und gleichen den UMF-Code von jedem eingehenden Ereignisdatensatz ab). Ohne diese erforderlichen Attribute werden keine von der CEP-Engine verarbeiteten Daten über die Pipeline an den Ereignismanager zurückgegeben.

Tabelle 4. Erforderliche Situationsattribute für komplexe Ereignisgeschäftsregeln

Attributname	Attributtyp	Attributausdruck	Attributbeschreibung
EVENT_SIT_STATUS	Zeichenfolge	"PENDING"	Gibt den Ereignisalertstatus für den Ereignisalert an. Im Bericht des i2-Plug-ins und des Explorers sowie in der Cognos-Alertzusammenfassung wird der Ereignisalertstatus als Teil der Alertzusammenfassung angezeigt. Alle neu generierten Alerts erhalten in der Regel den Status **Anstehend**, der angibt, dass ein Analyst diesen Alert analysieren und beheben muss. Beachten Sie, dass ein Ereignisalertstatus eine beliebige, für Ihr Unternehmen hilfreiche Angabe sein kann und als Ereignisstatus in der Konfigurationskonsole konfiguriert ist. Wenn das Ereignis nicht in den Benutzerschnittstellen der Komponente 'Analyst Toolkit' angezeigt werden soll, verwenden Sie den Ereignisalertstatus CLOSED.
REASON_DESC	Zeichenfolge	"*<Beschreibung der Ereignisregel oder des Alerts>*"	Beschreibt die Ereignisregel, die den Ereignisalert ausgelöst hat. Wählen Sie dafür eine für Ihre Analysten aussagekräftige Beschreibung. Wenn die Ereignisregel beispielsweise einen Alert generiert, sobald eine Entität innerhalb von 24 Stunden Transaktionen von über 1.500 Euro tätigt, können Sie als Ursachenbeschreibung (REASON_DESC) den Text "Summeüber1500" eingeben.

Tabelle 4. Erforderliche Situationsattribute für komplexe Ereignisgeschäftsregeln (Forts.)

Attributname	Attributtyp	Attributausdruck	Attributbeschreibung
ALERT_GROUP	Zeichenfolge	"<*Alertgruppe*>"	Gibt an, welcher Alertgruppe zugeordnet werden sollen, die von dieser Ereignisregel generiert wurden. Dieser Wert lautet in der Regel DEFAULT. Sie können jedoch eine beliebige andere, in der Konfigurationskonsole konfigurierte Alertgruppe eingeben.

Aufrufen der Details zu Ereignisalerts

Ereignisalerts werden in der Regel von mehreren komplexen Ereignissen ausgelöst. Sie können Ereignisalerts in den Analyst Toolkit-Anwendungen oder in einer Clientanwendung anzeigen. Die Details zu den Ereignissen, die zu diesem Alert geführt haben, sind standardmäßig jedoch nicht enthalten.

Wenn Sie die Details zu den Ereignissen, die zum Ereignisalert geführt haben, ebenfalls anzeigen wollen, müssen Sie das folgende Situationsattribut aufnehmen:

Tabelle 5. Einstellungen, die zum Erstellen des Situationsattributs EVENTS in einer Ereignisregel erforderlich sind

Name	Typ	Ausdruck	Dimension (Schaltfläche 'Show Advanced')
EVENTS	Ganze Zahl	Ereignis.EreignisID	[] (zur Angabe, dass die Ereignis-ID ein Bereich ist] Sie müssen das Situationsattribut bearbeiten und die Schaltfläche Show Advanced anklicken, um die Einstellung für diese Spalte anzuzeigen und zu definieren.

Bewährte Verfahren

Wenn Sie Ihre Ereignisalerts in den Analyst Toolkit-Anwendungen anzeigen, wählen Sie für das Situationsattribut REASON_DESC eine einfache Textzeichenfolge, anstatt der Nachricht Werte aus dem Ereignis hinzuzufügen. Die Analyst Toolkit-Gruppen gruppieren die allgemeinen Alerts in einer Alertzusammenfassung, die auch die Anzahl der in der Zusammenfassung enthaltenen Alerts angibt. Analysten klicken eine Alertzusammenfassung an, um alle in dieser Zusammenfassung enthaltenen Alerts zu beheben.

Wenn Sie in REASON_DESC Werte aus dem Ereignis definieren, wird jeder Ereignisalert als separate Alertzusammenfassung mit der Anzahl 1 angezeigt. Das heißt, dass Ihren Analysten jeder Ereignisalert sowohl in der Alertzusammenfassung als auch in den Alertdetailbereichen des Fensters **Alertzusammenfassung** angezeigt wird.

Erstellen einer Ereignisregel zum Summieren komplexer Ereignisse

Erstellen Sie eine grundlegende Ereignisregel SUM, um die Gesamtzahl der Ereignisse zu summieren und einen Ereignisalert zu erstellen, wenn die Summe dieser Ereignisse einen festgelegten Schwellenwert überschreitet. Sie können beispielsweise eine Ereignisregel erstellen, die alle Geldüberweisungen summiert, die von einer bestimmten Person innerhalb von 24 Stunden getätigt wurden und einen Ereignisalert senden, wenn die Summe dieser Geldüberweisungen (Ereignisse) über 15.000 Euro beträgt.

Vorbereitende Schritte

Sie müssen ein vorhandenes CEP-Projekt haben, das Ereignisregeln und alle Regelkonfigurationen gruppiert.

Informationen zu diesem Vorgang

Diese Schritte enthalten die grundlegenden Anweisungen zum Erstellen einer einfachen Geschäftsregel, die den Wert Ihrer Auswahl summiert. Bei einigen Schritten gibt es mehrere Wege, die zum selben Endergebnis führen. Weitere Informationen finden Sie im Abschnitt zu Situationen im Benutzerhandbuch zu IBM Advanced Middleware™ Technology (Handbuch zum Eclipse-basierten™ Tool 'CEP Rule Author'), das zum Lieferumfang des Produkts gehört.

Vorgehensweise

1. Klicken Sie im linken Navigationsteilfenster mit der rechten Maustaste **Situation** an und wählen Sie **New** > **Situation** aus. Stellen Sie sicher, dass der korrekte Projektname in **Event Processing Project** angezeigt wird.
2. Geben Sie einen eindeutigen Regelnamen in **Situation name** ein. Der Situationsname ist der Ereignisregelname, der in der Entitätendatenbank und in Visualizer angezeigt wird, wenn Sie dort Ereignisalerts anzeigen. Wählen Sie einen Namen aus, der für die Benutzer, die die Ereignisalerts analysieren, aussagekräftig ist. Wenn Sie beispielsweise eine Regel erstellen, um den Wert aller Ereignisse zu summieren und anschließend einen Alert zu senden, wenn die Summe der Ereignisse die Grenze von 15.000 Euro überschreitet, geben Sie dieser Regel möglicherweise den Namen Summeüber15T.
3. Wählen Sie in **Select source** den Eintrag **Empty of Type** und anschließend **atleast** in der Dropdown-Liste aus. Die Situation **atleast** kann sowohl Ereigniswerte summieren als auch die Informationen zu jedem Ereignis speichern, das die Ereignisregel erfüllt hat. Weitere Informationen zu Situationstypen finden Sie im Benutzerhandbuch im Abschnitt zu den Situationseigenschaften.
4. Klicken Sie **Finish** an. Wenn die Hauptsituationsanzeige geöffnet wird, sehen Sie im Problemabschnitt möglicherweise mehrere Fehler. Diese Fehler weisen auf fehlende Werte hin, können im Moment aber ignoriert werden. Diese Fehler sind nicht mehr vorhanden, wenn Sie diese Schritte durchgeführt haben.
5. Wählen Sie im Bereich **Events** den Eintrag EVENT als Basisereignis für diese Regel aus. EVENT ist stets das Basisereignis für jede Ereignisgeschäftsregel. Es enthält die erforderliche Zuordnung zur Entitätendatenbank GEM_TABLE und zum Datensegment EVENT.

6. Optional: Sie können eine *Schwellenwertbedingung* erstellen, um Ereignisse zu filtern, bevor sie gemäß dieser Regel ausgewertet werden, wodurch nur Ereignisse berücksichtigt werden, die die angegebene Schwellenwertbedingung erfüllen.
7. Klicken Sie zum Erstellen des Summierungsausdrucks **Show Advanced** und anschließend **Edit** an.
8. Wählen Sie in **Quantifier** den Eintrag `each` aus. Diese Auswahl stellt sicher, dass jeder eingehende Ereignisdatensatz in die Gesamtsumme eingeht, der die Bedingungen dieser Ereignisregel erfüllt.
9. Klicken Sie **...** in **Weight** an, um das Feld zu bearbeiten. Verwenden Sie das Ausdruckserstellungsprogramm, um das Ereignisfeld für die Summierung auszuwählen. Stellen Sie sicher, dass der Ausdruck im Bereich **Expression Builder Text** angezeigt wird und klicken Sie anschließend **OK** an. Die Gewichtung jedes Ereignisses entspricht standardmäßig dem Wert 1. Bei der Auswertung der Ereignisregel wird die Summe aller Gewichtungen mit dem Attribut **Quantity** auf der Registerkarte **Condition & Results** verglichen. Wenn die Gesamtsumme mindestens der angegebenen Menge entspricht, wird ein Ereignisalert generiert. Wenn Sie beispielsweise die Werte jedes Ereignisses summieren wollen, das die Ereignisregel erfüllt, wählen Sie `EVENT.EVENT_VALUE` aus.
10. Optional: Wenn das für die Gewichtung ausgewählte Feld Dezimalziffern enthält (vom Typ 'double'), verwenden Sie das Ausdruckserstellungsprogramm, um einen Ausdruck zu erstellen, der Folgendes ausführen soll:
    a. Multiplizieren der Berechnungsergebnisse mit 100, damit bei der Konvertierung der Eurobeträge in Centbeträge die Dezimalziffern beibehalten werden.
    b. Konvertieren des Datentyps 'double' in eine ganze Zahl. Dazu stehen Konvertierungsfunktionen bereit.

    Wenn Sie beispielsweise die Werte von Ereignissen summieren (`EVENT.EVENT_VALUE`), können Sie `EVENT.EVENT_VALUE*100` in den Bereich **Expression Builder Text** eingeben. Anschließend können Sie beispielsweise **Functions** > **Math** > **Round** auswählen, um das Ergebnis auf den nächsten ganzzahligen Wert zu runden. Der endgültige Ausdruck wird in folgender Form angezeigt: `Round(EVENT.EVENT_VALUE*100)`.
11. Klicken Sie in **Sum Expression** das Feld **...** an, um das Feld zu bearbeiten und das zu summierende Ereignisfeld auszuwählen. Wenn Sie beispielsweise den Wert jedes Ereignisses summieren wollen, das die Ereignisregel erfüllt oder übererfüllt, wählen Sie `EVENT_VALUE` aus.
12. Optional: Wenn Sie nur Ereignisse summieren wollen, die eine bestimmte Bedingung erfüllen, geben Sie die Bedingung in das Feld **Threshold Condition** ein oder verwenden Sie zur Unterstützung das Ausdruckserstellungsprogramm. Wenn Sie beispielsweise nur die Werte der Ereignisse summieren wollen, die in der Filiale 102 aufgetreten sind, geben Sie EVENT.EVENT_LOC="102" ein. Die Funktionsweise dieses Felds ähnelt einem Filter, wobei Ereignisse automatisch übersprungen werden, die die Bedingung nicht erfüllen oder übererfüllen.

    Tipp: Klicken Sie zum Vereinfachen Ihrer Anzeige und zum einfacheren Erkennen von **Threshold Condition** die Schaltfläche **Hide Advanced** an.
13. Wählen Sie auf der Registerkarte **Condition & Results** in **Lifespan** den Eintrag `EASLifeSpan` aus. Dieses Feld wird rot angezeigt, bis Sie eine Auswahl treffen. Die rote Farbe gibt an, dass es sich um ein erforderliches Feld handelt und dass einer der Fehler im Problemabschnitt sich auf dieses Feld bezieht.

Wenn Sie die Auswahl für die Lebensdauer getroffen haben, wird der Fehler im Bereich **Problems** von der Anzeige entfernt.

14. Geben Sie in **Quantity** die Menge "atleast" ein, bis zu der die Ereignisregel die Summierung vornimmt, bevor sie den Ereignisalert generiert. Denken Sie daran, Eurobeträge mit 100 zu multiplizieren. Geben Sie beispielsweise `1500000` ein, um einen Ereignisalert zu generieren, wenn mindestens die Summe 15.000 Euro erreicht ist.
15. Beachten Sie, dass in **Detection Mode** der Eintrag `immediate` ausgewählt ist. Behalten Sie diese Auswahl bei. Der Erkennungsmodus legt fest, wann Ergebnisse der Ereignisse berechnet und zurückgemeldet werden sollen. Die Auswahl `immediate` generiert einen Alert, sobald die Summe die Menge erreicht hat.
16. Geben Sie in `Situation Attributes` die erforderlichen Situationswerte für die folgenden Situationsattribute ein:
    - `EVENT_SIT_STATUS`
    - `REASON_DESC`
    - `ALERT_GROUP`
17. Optional: Wenn Sie die Details aller Ereignisse beibehalten wollen, die Teil der Summe darstellen, fügen Sie mithilfe der folgenden Informationen das Situationsattribut `EVENTS` hinzu:
    a. Geben Sie in **Name** die Zeichenfolge `EVENTS` ein.
    b. Geben Sie in **Type** die Zeichenfolge `ganze Zahl` ein.
    c. Geben Sie in **Expression** die Zeichenfolge `EVENT_ID` ein (oder wählen Sie diese im Ausdruckserstellungsprogramm aus).
    d. Klicken Sie **Show Advanced** an, um die Spalte **Dimensions** anzuzeigen, und geben Sie `[]` in die Spalte ein, um anzugeben, dass der Typ ein Ereignisarray ist.

    Diese Werte weisen CEP an, die interne Ereignis-ID (`EVENT_ID`) jedes Ereignisses, das in die Gesamtsumme eingeht, zusammen mit dem Ereignisalert zurück an die Pipeline zu senden. Die Pipeline schreibt jede Ereignis-ID (`EVENT_ID`) in die Entitätendatenbank und sendet die Informationen an Visualizer oder an die Clientanwendung, die zur Anzeige der Ereignisalerts verwendet wird. Die Ereignis-ID (`EVENT_ID`) ist eine interne fortlaufende Zahl (ID), die von der Pipeline erstellt wird, wenn sie Ereignisdaten an die CEP-Engine sendet.
18. Speichern Sie die Ereignisregel.

Erstellen einer Ereignisregel zum Zählen komplexer Ereignisse

Erstellen Sie eine grundlegende Ereignisregel COUNT, um Ereignisse zu zählen und einen Ereignisalert zu generieren, wenn die Gesamtanzahl einen festgelegten Schwellenwert überschreitet. Sie könnten beispielsweise eine Ereignisregel erstellen, die alle Geldüberweisungen in einem Zeitraum von 24 Stunden zählt und einen Ereignisalert sendet, wenn mehr als 500 Transaktionen 500 getätigt werden.

Vorbereitende Schritte

Sie müssen ein vorhandenes CEP-Projekt haben, das Ereignisregeln und alle Regelkonfigurationen gruppiert.

Informationen zu diesem Vorgang

Diese Schritte enthalten die grundlegenden Anweisungen zum Erstellen einer einfachen Geschäftsregel, die den Wert Ihrer Auswahl zählt. Bei einigen Schritten gibt

es mehrere Wege, die zum selben Endergebnis führen. Weitere Informationen finden Sie im Abschnitt zu Situationen im Benutzerhandbuch zu IBM Advanced Middleware™ Technology (Handbuch zum Eclipse-basierten™ Tool 'CEP Rule Author'), das zum Lieferumfang des Produkts gehört.

Vorgehensweise

1. Klicken Sie im linken Navigationsteilfenster mit der rechten Maustaste **Situation** an und wählen Sie **New** > **Situation** aus. Stellen Sie sicher, dass der korrekte Projektname in **Event Processing Project** angezeigt wird.
2. Geben Sie einen eindeutigen Regelnamen in **Situation name** ein. Der Situationsname ist der Ereignisregelname, der in der Entitätendatenbank und in Visualizer angezeigt wird, wenn Sie dort Ereignisalerts anzeigen. Wählen Sie einen Namen aus, der für die Benutzer, die die Ereignisalerts analysieren, aussagekräftig ist. Wenn Sie beispielsweise eine Regel erstellen, die alle Ereignisse zählt, die in einer bestimmten Filiale auftreten, könnten Sie diese Regel `AnzahlTransaktionenFiliale102` nennen.
3. Wählen Sie in **Select source** den Eintrag **Empty of Type** und anschließend einen der folgenden Werte in der Dropdown-Liste aus:
   - **atleast**: Während der Lebensdauer sind mindestens *n* Ereignisse eingetroffen.
   - **atmost**: Am Ende der Lebensdauer sind maximal *n* Ereignisse eingetroffen.

   Beide Situationstypen können sowohl Ereigniswerte zählen als auch die Informationen zu jedem Ereignis speichern, das die Ereignisregel erfüllt hat. Weitere Informationen zu Situationstypen finden Sie im Benutzerhandbuch im Abschnitt zu den Situationseigenschaften.
4. Klicken Sie **Finish** an. Wenn die Hauptsituationsanzeige geöffnet wird, sehen Sie im Problemabschnitt möglicherweise mehrere Fehler. Diese Fehler weisen auf fehlende Werte hin, können im Moment aber ignoriert werden. Diese Fehler sind nicht mehr vorhanden, wenn Sie diese Schritte durchgeführt haben.
5. Wählen Sie im Bereich **Events** den Eintrag `EVENT` als Basisereignis für diese Regel aus. `EVENT` ist stets das Basisereignis für jede Ereignisgeschäftsregel. Es enthält die erforderliche Zuordnung zur Entitätendatenbank `GEM_TABLE` und zum Datensegment `EVENT`.
6. Optional: Sie können eine *Schwellenwertbedingung* erstellen, um Ereignisse zu filtern, bevor sie gemäß dieser Regel ausgewertet werden, wodurch nur Ereignisse berücksichtigt werden, die die angegebene Schwellenwertbedingung erfüllen.
7. Wählen Sie auf der Registerkarte **Condition & Results** in **Lifespan** den Eintrag `EASLifeSpan` aus. Dieses Feld wird rot angezeigt, bis Sie eine Auswahl treffen. Die rote Farbe gibt an, dass es sich um ein erforderliches Feld handelt und dass einer der Fehler im Problemabschnitt sich auf dieses Feld bezieht. Wenn Sie die Auswahl für die Lebensdauer getroffen haben, wird der Fehler im Bereich **Problems** von der Anzeige entfernt.
8. Geben Sie in **Quantity** die Menge "atleast" oder "atmost" ein, bis zu der die Ereignisregel zählt, bevor sie den Ereignisalert generiert.
9. Beachten Sie, dass in **Detection Mode** der Eintrag `immediate` ausgewählt ist. Behalten Sie diese Auswahl bei. Der Erkennungsmodus legt fest, wann Ergebnisse der Ereignisse berechnet und zurückgemeldet werden sollen. Die Auswahl `immediate` generiert einen Alert, sobald die Anzahl die Menge erreicht hat.
10. Geben Sie in `Situation Attributes` die erforderlichen Attributnamen, Typen und Ausdrücke für die Situation ein:

- EVENT_SIT_STATUS
- REASON_DESC
- ALERT_GROUP

11. Wenn Sie die Details aller Ereignisse beibehalten wollen, die bei der Anzahl berücksichtigt werden, fügen Sie mithilfe der folgenden Informationen das Situationsattribut EVENTS hinzu:
    a. Geben Sie in **Name** die Zeichenfolge EVENTS ein.
    b. Geben Sie in **Type** die Zeichenfolge ganze Zahl ein.
    c. Geben Sie in **Expression** die Zeichenfolge EVENT_ID ein (oder wählen Sie diese im Ausdruckserstellungsprogramm aus).
    d. Klicken Sie **Show Advanced** an, um die Spalte **Dimensions** anzuzeigen, und geben Sie [] in die Spalte ein, um anzugeben, dass der Typ ein Ereignisarray ist.

    Diese Werte weisen CEP an, die interne Ereignis-ID (EVENT_ID) jedes Ereignisses, das in die Gesamtsumme eingeht, zusammen mit dem Ereignisalert zurück an die Pipeline zu senden. Die Pipeline schreibt jede Ereignis-ID (EVENT_ID) in die Entitätendatenbank und sendet die Informationen an Visualizer oder an die Clientanwendung, die zur Anzeige der Ereignisalerts verwendet wird. Die Ereignis-ID (EVENT_ID) ist eine interne fortlaufende Zahl (ID), die von der Pipeline erstellt wird, wenn sie Ereignisdaten an die CEP-Engine sendet.
12. Speichern Sie die Ereignisregel.

Behindertengerechte Bedienung

Funktionen zur behindertengerechten Bedienung helfen Menschen mit körperlichen Behinderungen wie eingeschränktem Bewegungs- oder Sehvermögen, erfolgreich mit Softwareprodukten zu arbeiten.

In der folgenden Liste sind die wichtigsten Eingabehilfen angegeben:

- Wenn Sie den empfohlenen Browser Internet Explorer verwenden, steht Ihnen die gesamte Funktionalität der Benutzerschnittstelle auch zur Verfügung, wenn Sie an Stelle der Maus die Tastatur zur Navigation verwenden.
- Das Produkt ist mit Hilfstechnologien kompatibel.
- Sie können in einem behindertengerechten Format auf die IBM InfoSphere Identity Insight-Dokumentation zugreifen.

Tastaturzugriff

Die IBM InfoSphere Identity Insight-Konfigurationskonsole und Visualizer sind vollständig für die behindertengerechte Bedienung geeignet, wenn sie mit dem Browser Internet Explorer angezeigt werden.

Sie können die Konfigurationskonsole und Visualizer auch ausschließlich über die Tastatur bedienen. Sie können Tasten oder Tastenkombinationen zur Ausführung von Operationen verwenden, die sich auch mithilfe einer Maus ausführen lassen. Standardtastatureingaben des Betriebssystems werden für Standardoperationen des Betriebssystems verwendet.

In allen unterstützten Betriebssystemen und unterstützten Browsern ist der Bereich des aktiven Fensters hervorgehoben, auf den Ihre Tastatureingaben angewendet

werden. In Textfeldern und Textbereichen wird ein blinkender Cursor in Form einer Einfügemarke angezeigt. Andere Felder werden durch eine gestrichelte Umrandung hervorgehoben.

Anmerkung: In der Konfigurationskonsole kann im Browser Mozilla Firefox mithilfe der Tastatur navigiert werden. Es gibt jedoch ein bekanntes Problem, das darin besteht, dass Tastaturdirektaufrufe, die die Tasten **Alt** und eine numerische Taste verwenden, in diesem Browser nicht unterstützt werden.

Behindertengerechte Anzeige

Die Konfigurationskonsole und Visualizer verfügen über Funktionen, die die behindertengerechte Bedienung für Benutzer mit eingeschränktem Sehvermögen oder anderen Sehbehinderungen verbessern. Zu diesen Erweiterungen behindertengerechter Bedienung gehört auch die Unterstützung anpassbare Schrifteigenschaften.

Sie können die Farbe, Größe und Schriftart für den Text in Menüs und Dialogfeldern nach Benutzerschnittstelle auswählen:

- Konfigurationskonsole: über Ihre Browsereinstellungen
- Visualizer: über die Einstellungen in **Benutzervorgaben für die Anzeige konfigurieren**

Sie brauchen nicht in der Lage zu sein, zwischen Farben zu unterscheiden, um alle Funktionen in diesem Produkt verwenden zu können.

Kompatibilität mit Hilfstechnologien

Die Visualizer-Benutzerschnittstelle unterstützt Java Accessibility API. Hiermit können Sie Sprachausgabeprogramme und andere Hilfstechnologien verwenden. In der Konfigurationskonsole können Sie Sprachausgabeprogramme in den unterstützten Browsern aktivieren.

Dokumentation in behindertengerechtem Format

Die Dokumentation für IBM InfoSphere Identity Insight wird in XHTML 1.0 bereitstellt. Dieses Format kann in den meisten Web-Browsern angezeigt werden. Mit XHTML können Sie Dokumentation entsprechend den Anzeigevorgaben anzeigen, die in Ihrem Browser festgelegt sind. XHTML ermöglicht Ihnen außerdem, Sprachausgabeprogramme und andere Hilfstechnologien zu verwenden.

Tastaturkurzbefehle und Direktaufrufe der Konfigurationskonsole

Die Konfigurationskonsole ist uneingeschränkt für behindertengerechte Bedienung geeignet, wenn unterstützte Browser verwendet werden. Das heißt, Sie können Tasten oder Tastenkombinationen verwenden, um Operationen auszuführen, die sich auch mithilfe einer Maus ausführen lassen.

Anmerkung: In der Konfigurationskonsole kann im Browser Mozilla Firefox mithilfe der Tastatur navigiert werden, die aufgeführten Tastenkombinationen **Alt** + ***Ziffer*** funktionieren in diesem Browser jedoch nicht einwandfrei.

Tabelle 6. Allgemeine Tastaturkurzbefehle und Direktaufrufe

Aktion	**Direktaufruf**
Zum nächsten aktivierten Anzeigenelement (Eingabefeld, Schaltfläche, Link) wechseln (Anzeigefelder werden übersprungen)	**Tabulatortaste**
Zum vorherigen aktivierten Anzeigenelement (Eingabefeld, Schaltfläche, Link) wechseln (Anzeigefelder werden übersprungen)	**Umschalttaste** + **Tabulator**
Aktion ausführen (Link oder Schaltfläche)	**Eingabetaste**

Tabelle 7. Feldnavigation

Aktion	**Taste oder Direktaufruf**
In einer Dropdown-Liste nach oben oder nach unten bewegen In mehreren Zeilen eines Textbereichsfelds nach oben oder nach unten bewegen	Aufwärtspfeil oder Abwärtspfeil
In einem Texteingabefeld nach links oder rechts bewegen	Linkspfeil oder Rechtspfeil
An den Anfang eines Texteingabefelds gehen An den Anfang der aktuellen Zeile in einem großen Textbereichsfeld gehen	**Taste für erste Eingabeposition**
An das Ende eines Eingabefelds gehen An das Ende der aktuellen Zeile in einem großen Textbereichsfeld gehen	**Endetaste**
An das Ende eines Texteingabefelds gehen Zur nächsten Seite in einem Textbereichsfeld gehen	**Vorblättertaste**
An den Anfang eines Texteingabefelds gehen Zur vorherigen Seite in einem Textbereichsfeld gehen	**Zurückblättertaste**
Dropdown-Liste einblenden oder ausblenden	**Alt** + Aufwärts- oder Abwärtspfeil
An den Anfang eines Textbereichs gehen	**Strg** + **Zurückblättertaste**
An das Ende eines Textbereichs gehen	**Strg** + **Vorblättertaste**

Tabelle 8. Navigation in der Anzeige

Aktion	**Direktaufruf**
(Zur Verwendung in Sprachausgabeprogrammen) Alle Navigations- und Aktionslinks im Seitenkopf überspringen	**Alt** + **0**
Den Bereich für 'Position:' und die Aktionen in der rechten oberen Ecke aktivieren	**Alt** + **1**
Menüs oder Untermenüs aktivieren	**Alt** + **2**
Übergeordnete Registerkarten aktivieren	**Alt** + **3**
Übergeordnete Links aktivieren	**Alt** + **4**
(Nur Detailanzeigen) Die Einträge im linken Navigationsteilfenster aktivieren	**Alt** + **5**

Tabelle 8. Navigation in der Anzeige (Forts.)

Aktion	Direktaufruf
(Nur Detailanzeigen) Untergeordnete Registerkarten und Detailaktionsschaltflächen aktiveren	**Alt** + **6**
Beliebiges Formularfeld im Hauptinhaltsbereich aktivieren	**Alt** + **7**
(Zur Verwendung in Sprachausgabeprogrammen) Überspringt das Verzeichnis zu den Feldern von Detailanzeigen	**Alt** + **8**
(Zur Verwendung in Sprachausgabeprogrammen) Springt zur Hilfefußzeile am unteren Rand der Anzeige	**Alt** + **9**

Tabelle 9. Bearbeitungsaktionen (innerhalb von Eingabefeldern)

Aktion	Direktaufruf
Kopieren	**Strg** + **C**
Ausschneiden	**Strg** + **X**
Einfügen	**Strg** + **V**
Alles auswählen	**Strg** + **A**
Rückgängig machen	**Strg** + **Z**
Zeichen links vom Cursor löschen	**Rücktaste**
Zeichen rechts vom Cursor löschen	**Löschtaste**

Tastaturkurzbefehle und Direktaufrufe von Visualizer

Visualizer ist uneingeschränkt für behindertengerechte Bedienung geeignet. Das heißt, Sie können Tasten oder Tastenkombinationen verwenden, um Operationen auszuführen, die sich auch mithilfe einer Maus ausführen lassen.

Tabelle 10. Allgemeine Tastaturkurzbefehle und Direktaufrufe

Aktion	Direktaufruf
Zum nächsten aktivierten Anzeigenelement (Eingabefeld, Schaltfläche, Link) wechseln	**Tabulatortaste**
Zum vorherigen aktivierten Anzeigenelement (Eingabefeld, Schaltfläche, Link) wechseln	**Umschalttaste** + **Tabulator**
Aktion ausführen (Link oder Schaltfläche)	**Eingabetaste** oder Leertaste
Zeigt das Fenster für die Berichtskriterien an (Standardwert: Bericht zu den Attributalertgeneratoren)	**Strg** + **A**
Zeigt das Fenster zum Laden der UMF-Datei an	**Strg** + **B**
Zeigt den Dialog 'Kennwort ändern' an	**Strg** + **H**
Sperrt die Anwendung. Der aktuelle Benutzer befindet sich weiterhin in einer Visualizer-Sitzung, die Anzeige ist jedoch gesperrt.	**Strg** + **L**

Tabelle 10. Allgemeine Tastaturkurzbefehle und Direktaufrufe (Forts.)

Aktion	**Direktaufruf**
Zeigt den Dialog 'Drucken' in Fenstern oder auf Registerkarten an, mit dem Sie Informationen oder Berichte (z. B. die Entitätszusammenfassung) drucken können	**Strg** + **P**
Meldet den aktuellen Benutzer von der Visualizer-Sitzung ab und beendet die Anwendung	**Strg** + **Q**
Zeigt den Dialog 'Benutzervorgaben für die Anzeige konfigurieren' an	**Strg** + **R**
Zeigt das Information Center des Produkts an	**F1**
Zeigt das Fenster 'Produktinfo' an, das die Produktversionsnummer enthält	**Umschalttaste** + **F1**

Tabelle 11. Feldnavigation

Aktion	**Taste oder Direktaufruf**
In das darüber oder darunter liegende Feld bewegen In einer Dropdown-Liste nach oben oder nach unten bewegen In mehreren Textzeilen in einem Eingabefeld nach oben oder nach unten bewegen	Aufwärtspfeil oder Abwärtspfeil
In einem Eingabefeld nach links oder rechts bewegen	Linkspfeil oder Rechtspfeil
An den Anfang eines Eingabefelds gehen An den Anfang der aktuellen Zeile in einem großen Textfeld gehen	**Taste für erste Eingabeposition**
An das Ende eines Eingabefelds gehen An das Ende der aktuellen Zeile in einem großen Textfeld gehen	**Endetaste**
An das Ende eines Eingabefelds gehen	**Vorblättertaste**
An den Anfang eines Eingabefelds gehen	**Zurückblättertaste**
Dropdown-Liste einblenden oder ausblenden	**Alt** + Aufwärts- oder Abwärtspfeil
Blendet ein Twistie ein oder aus (wenn ein Twistie ausgewählt ist)	Leertaste
Aus einer Tabelle heraus zum nächsten Steuerelement bewegen	**Strg** + **Tabulator**

Tabelle 12. Bearbeitungsaktionen

Aktion	**Direktaufruf**
Kopieren	**Strg** + **C**
Ausschneiden	**Strg** + **X**
Einfügen	**Strg** + **V**

Tabelle 12. Bearbeitungsaktionen (Forts.)

Aktion	**Direktaufruf**
Wählt den gesamten Text in Textfeldern aus	**Strg** + **A**
Rückgängig machen	**Strg** + **Z**
Zeichen links vom Cursor löschen	**Rücktaste**
Zeichen rechts vom Cursor löschen	**Löschtaste**

Kapitel 2. Systemvoraussetzungen und Planung

Dieser Referenzabschnitt enthält Informationen zu unterstützten Plattformen, zu Systemvoraussetzungen und zur Systemarchitektur.

Detaillierte Systemvoraussetzungen

Diese Voraussetzungen geben die Hardware- und Softwareprodukte an, die Sie vor dem Öffnen eines Problemberichts beim IBM Support Team installieren und verwenden müssen.

Systemvoraussetzungen bei Ausführung unter IBM AIX

In der folgenden Liste sind die Produkte aufgeführt, die unterstützt werden, wenn IBM InfoSphere Identity Insight unter dem Betriebssystem AIX ausgeführt wird.

Tabelle 13. Systemvoraussetzungen bei Ausführung unter IBM AIX

Betriebssysteme	• IBM AIX 7.1L
Hardwarevoraussetzungen	• POWER7 (64 Bit) • POWER6 • POWER5
Java	Folgendes wird mit dem Produkt installiert: • IBM Java Runtime Environment (64 Bit) Version 8
Datenbanken	• IBM DB2 Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 oder höher)
Datenbankclients	• DB2-Client Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • DB2-Client Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Client mit Oracle 12c beim Herstellen einer Verbindung zu Oracle 12c. • Client mit Oracle 11g Release 2 beim Herstellen einer Verbindung zu Oracle 11g Release 2.

Tabelle 13. Systemvoraussetzungen bei Ausführung unter IBM AIX (Forts.)

JDBC-Clients (Java Database Connectivity)	• JDBC-Treiber des DB2-Clients Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • JDBC-Treiber des DB2-Clients Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • JDBC-Treiber für Oracle 12c beim Herstellen einer Verbindung zu Oracle 12c. • JDBC-Treiber für Oracle 11g beim Herstellen einer Verbindung zu Oracle 11g.
Web-Browser	• Mozilla Firefox
Software zur Steuerung von Nachrichtenwarteschlangen	• IBM WebSphere MQ
Sonstiges	• IBM C++ Runtime Environment Components for AIX. Weitere Informationen zu dieser Voraussetzung finden Sie in den folgenden Unterstützungsinformationen: http://www-01.ibm.com/support/docview.wss?uid=swg24025181.

Systemvoraussetzungen bei Ausführung unter HP-UX

In der folgenden Liste sind die Produkte aufgeführt, die unterstützt werden, wenn IBM InfoSphere Identity Insight unter dem Betriebssystem HP-UX ausgeführt wird.

Tabelle 14. Systemvoraussetzungen bei Ausführung unter HP-UX

Betriebssysteme	• HPUX 11i v3
Hardwarevoraussetzungen	• Intel Itanium 2 (IA64)
Java	Folgendes wird mit dem Produkt installiert: • IBM Java Runtime Environment (64 Bit) for HPUX, Java Technology Edition, Version 6
Java-Voraussetzungen für Client	HP-UX wird als Clientplattform nicht unterstützt. Auf Maschinen mit unterstützten Clientplattformen, die eine Verbindung zur Konfigurationskonsole oder zu Visualizer herstellen, muss SUN Java SE Runtime Environment (JRE) Version 6 installiert sein.
Datenbanken	• IBM DB2 Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 oder höher)

Tabelle 14. Systemvoraussetzungen bei Ausführung unter HP-UX (Forts.)

Datenbankclients	• DB2-Client Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • DB2-Client Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Client mit Oracle 12c beim Herstellen einer Verbindung zu Oracle 12c. • Client mit Oracle 11g Release 2 beim Herstellen einer Verbindung zu Oracle 11g Release 2.
JDBC-Clients (Java Database Connectivity) für die Konfigurationskonsole und Visualizer	• JDBC-Treiber des DB2-Clients Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • JDBC-Treiber des DB2-Clients Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • JDBC-Treiber für Oracle 12c beim Herstellen einer Verbindung zu Oracle 12c. • JDBC-Treiber für Oracle 11g beim Herstellen einer Verbindung zu Oracle 11g.
Web-Browser	• Mozilla Firefox
Unterstützte Software zur Steuerung von Nachrichtenwarteschlangen	• IBM WebSphere MQ

Systemvoraussetzungen bei Ausführung unter Linux x86

In der folgenden Liste sind die Produkte aufgeführt, die unterstützt werden, wenn IBM InfoSphere Identity Insight unter dem Betriebssystem Linux x86 ausgeführt wird.

Tabelle 15. Systemvoraussetzungen bei Ausführung unter Linux x86

Betriebssysteme	• Red Hat Enterprise Linux AS, Version 6.0 • Red Hat Enterprise Linux AS, Version 5.0 • Novell SUSE Linux Enterprise Server, Version 10
Hardwarevoraussetzungen	• Intel x86 (IA32)
Java	Folgendes wird mit dem Produkt installiert: • IBM Runtime Environment (32 Bit) for Linux auf Intel-Architektur, Java Technology Edition, Version 6
Java-Voraussetzungen für Client	Auf Maschinen mit unterstützten Clientplattformen, die eine Verbindung zur Konfigurationskonsole oder zu Visualizer herstellen, muss SUN Java SE Runtime Environment (JRE) Version 6 installiert sein.

Tabelle 15. Systemvoraussetzungen bei Ausführung unter Linux x86 (Forts.)

Datenbanken	• IBM DB2 Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 oder höher)
Datenbankclients	• DB2-Client Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • DB2-Client Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Client mit Oracle 12c beim Herstellen einer Verbindung zu Oracle 12c. • Client mit Oracle 11g Release 2 beim Herstellen einer Verbindung zu Oracle 11g Release 2.
JDBC-Clients (Java Database Connectivity) für die Konfigurationskonsole und Visualizer	• JDBC-Treiber des DB2-Clients Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • JDBC-Treiber des DB2-Clients Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • JDBC-Treiber für Oracle 12c beim Herstellen einer Verbindung zu Oracle 12c. • JDBC-Treiber für Oracle 11g beim Herstellen einer Verbindung zu Oracle 11g.
Web-Browser	• Mozilla Firefox
Unterstützte Software zur Steuerung von Nachrichtenwarteschlangen	• IBM WebSphere MQ

Systemvoraussetzungen bei Ausführung unter Linux for System x

In der folgenden Liste sind die Produkte aufgeführt, die unterstützt werden, wenn IBM InfoSphere Identity Insight unter dem Betriebssystem Linux for System x ausgeführt wird.

Tabelle 16. Systemvoraussetzungen bei Ausführung unter Linux for System x

Betriebssysteme	• Red Hat Enterprise Linux AS, Version 7.0 • Red Hat Enterprise Linux AS, Version 6.0
Hardwarevoraussetzungen	• Intel x86_64
Java	Folgendes wird mit dem Produkt installiert: • IBM Java Runtime Environment (64 Bit) Version 8

Tabelle 16. Systemvoraussetzungen bei Ausführung unter Linux for System x (Forts.)

Datenbanken	• IBM DB2 Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 oder höher)
Datenbankclients	• DB2-Client Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • DB2-Client Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Client mit Oracle 12c beim Herstellen einer Verbindung zu Oracle 12c. • Client mit Oracle 11g Release 2 beim Herstellen einer Verbindung zu Oracle 11g Release 2.
JDBC-Clients (Java Database Connectivity)	• JDBC-Treiber des DB2-Clients Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • JDBC-Treiber des DB2-Clients Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • JDBC-Treiber für Oracle 12c beim Herstellen einer Verbindung zu Oracle 12c. • JDBC-Treiber für Oracle 11g beim Herstellen einer Verbindung zu Oracle 11g.
Web-Browser	• Mozilla Firefox
Unterstützte Software zur Steuerung von Nachrichtenwarteschlangen	• IBM WebSphere MQ

Systemvoraussetzungen bei Ausführung unter Linux for System z

In der folgenden Liste sind die Produkte aufgeführt, die unterstützt werden, wenn IBM InfoSphere Identity Insight unter dem 64-Bit-Betriebssystem Linux for System z ausgeführt wird.

Tabelle 17. Systemvoraussetzungen bei Ausführung unter Linux on System z (64 Bit)

Betriebssysteme	• Red Hat Enterprise Linux AS, Version 7.0
Hardwarevoraussetzungen	• IBM System z
Java	Folgendes wird mit dem Produkt installiert: • IBM Java Runtime Environment (64 Bit) Version 8

Tabelle 17. Systemvoraussetzungen bei Ausführung unter Linux on System z (64 Bit) (Forts.)

Datenbanken	• IBM DB2 Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 oder höher)
Datenbankclients	• DB2-Client Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • DB2-Client Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle-Client der Version 10g Release 2 (10.2.0.2.0) beim Herstellen einer Verbindung zu Oracle 11g Release 1 (11.2.0.1) oder 11g Release 2 (11.2.0.2)
JDBC-Clients (Java Database Connectivity)	• JDBC-Treiber des DB2-Clients Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • JDBC-Treiber des DB2-Clients Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle-Client der Version 10g Release 2 (10.2.0.2.0) beim Herstellen einer Verbindung zu Oracle 11g Release 1 (11.2.0.1) oder 11g Release 2 (11.2.0.2)
Web-Browser	• Mozilla Firefox
Unterstützte Software zur Steuerung von Nachrichtenwarteschlangen	• IBM WebSphere MQ

Systemvoraussetzungen bei Ausführung unter Sun Solaris

In der folgenden Liste sind die Produkte aufgeführt, die unterstützt werden, wenn IBM InfoSphere Identity Insight unter dem Betriebssystem Sun Solaris ausgeführt wird.

Tabelle 18. Systemvoraussetzungen bei Ausführung unter Sun Solaris

Betriebssysteme	• Sun Solaris 10.0
Hardwarevoraussetzungen	• UltraSPARC T2 • UltraSPARC IV und höher
Java	Folgendes wird mit dem Produkt installiert: • IBM Java Runtime Environment (64 Bit) for Solaris, Java Technology Edition, Version 6

Tabelle 18. Systemvoraussetzungen bei Ausführung unter Sun Solaris (Forts.)

Java-Voraussetzungen für Client	Auf Maschinen mit unterstützten Clientplattformen, die eine Verbindung zur Konfigurationskonsole oder zu Visualizer herstellen, muss SUN Java SE Runtime Environment (JRE) Version 6 installiert sein.
Datenbanken	• IBM DB2 Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 oder höher)
Datenbankclients	• DB2-Client Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • DB2-Client Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Client mit Oracle 12c beim Herstellen einer Verbindung zu Oracle 12c. • Client mit Oracle 11g Release 2 beim Herstellen einer Verbindung zu Oracle 11g Release 2.
JDBC-Clients (Java Database Connectivity) für die Konfigurationskonsole und Visualizer	• JDBC-Treiber des DB2-Clients Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • JDBC-Treiber des DB2-Clients Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • JDBC-Treiber für Oracle 12c beim Herstellen einer Verbindung zu Oracle 12c. • JDBC-Treiber für Oracle 11g beim Herstellen einer Verbindung zu Oracle 11g.
Web-Browser	• Mozilla Firefox
Unterstützte Software zur Steuerung von Nachrichtenwarteschlangen	• IBM WebSphere MQ
Sonstige Software	• GNU Compiler Collection-Paket (gcc oder gcc_small) Version 3.3.2.

Systemvoraussetzungen bei Ausführung unter Microsoft Windows Server

In der folgenden Liste sind die Produkte aufgeführt, die unterstützt werden, wenn IBM InfoSphere Identity Insight unter dem 64-Bit-Betriebssystem Microsoft Windows Server ausgeführt wird.

Tabelle 19. Systemvoraussetzungen bei Ausführung unter Microsoft Windows Server

Betriebssysteme	• Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 R2
Hardwarevoraussetzungen	• Intel x86_64
Java	Folgendes wird mit dem Produkt installiert: • IBM Java Runtime Environment (64 Bit) Version 8
Datenbanken	• IBM DB2 Database for Linux, UNIX, and Windows 11.1 • IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 oder höher)
Datenbankclients	• DB2-Client Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • DB2-Client Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • Client mit Oracle 12c beim Herstellen einer Verbindung zu Oracle 12c. • Client mit Oracle 11g Release 2 beim Herstellen einer Verbindung zu Oracle 11g Release 2.
JDBC-Clients (Java Database Connectivity)	• JDBC-Treiber des DB2-Clients Version 11.1 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 11.1 • JDBC-Treiber des DB2-Clients Version 10.5 beim Herstellen einer Verbindung zu IBM DB2 Database for Linux, UNIX, and Windows 10.5 • JDBC-Treiber für Oracle 12c beim Herstellen einer Verbindung zu Oracle 12c. • JDBC-Treiber für Oracle 11g beim Herstellen einer Verbindung zu Oracle 11g.
Web-Browser	• Windows Internet Explorer 10 und höher • Mozilla Firefox
Unterstützte Software zur Steuerung von Nachrichtenwarteschlangen	• IBM WebSphere MQ

Definieren der Systemarchitektur

Erarbeiten Sie einen Entwurf der Datenbank- und Serverkonfigurationen für Ihre Produktinstallation.

Produktdatenbankkonfiguration

IBM InfoSphere Identity Insight-Installationen können bis zu drei separate Datenbanken für die Produktkonfiguration und Entitätsdatenspeicherung enthalten.

Folgende Datenbanken können vorhanden sein:

Entitätendatenbank
Die Datenbank, in der die Identitäten, Entitäten und Daten gespeichert werden, die für Beziehungen, Auflösungen und Alerts verwendet werden.

Konfigurationskonsolendatenbank (Configuration Console Database)
Die Datenbank, in der die Ressourcen für die Konfigurationskonsole gespeichert werden.

Anwendungsmonitordatenbank
Die Datenbank, die die Routing- und Überwachungsdaten für die Pipelines speichert.

Im Rahmen von Neuinstallationen können die Datenbanken (in Abhängigkeit der installierten Features) in einer einzelnen Datenbank konsolidiert werden. Die Option zur Konsolidierung der Datenbanken befindet sich in den jeweiligen Datenbankkonfigurationsanzeigen des Installationsprogramms. Eine einzelne Datenbank ist die bevorzugte Konfiguration.

Pipelinebereitstellungen

Pipelines können je nach Systemvoraussetzungen und Serverressourcen auf einem einzelnen Server oder auf mehreren Servern installiert werden.

Berücksichtigen Sie bei der Bereitstellung von Pipelines die folgenden Faktoren in Bezug auf das Leistungsverhalten:

- Pipelines können einzeln ausgeführt oder für die Ausführung gleichzeitig ablaufender Threads für die Parallelverarbeitung konfiguriert werden.
- Jede CPU kann 1,5 bis 2 Pipelines oder Pipeline-Threads für die Parallelverarbeitung verarbeiten.
- Pipelines für die Parallelverarbeitung sind in der Lage, gleichzeitig Daten aus mehreren Datenquellen zu empfangen, sodass Sie die Dateien nicht manuell entsprechend der Anzahl der einzelnen Pipelines aufteilen müssen.

Berücksichtigen Sie bei der Bereitstellung von Pipelines darüber hinaus die folgenden Faktoren:

- Pipelines können in jeder unterstützten Hardware- und Betriebssystemkonfiguration ausgeführt werden.
- Führen Sie die Pipelines nicht auf der Maschine aus, auf der sich die Datenbank befindet, auch wenn dies theoretisch möglich ist.
- Pipelines für die Parallelverarbeitung sind weniger aufwendig zu konfigurieren als Mehrfachpipelines.
- Konfigurationen mit mehreren Servern sind aufwendiger in der Verwaltung.
- Konfigurationen mit nur einem einzelnen Server erfordern eine kostenintensive Hardware (die Kosten steigen exponentiell mit der Anzahl CPUs).

Erstellen eines geschützten Benutzers für Nicht-Windows-Installationen

Erstellen Sie für alle anderen Plattformen als Windows einen geschützten Benutzer für das Ausführen des Produktinstallationsprogramms.

Informationen zu diesem Vorgang

Führen Sie das Produktinstallationsprogramm nicht als Rootbenutzer aus.

Benutzerrollen und -zuständigkeiten

Benutzerrollen helfen beim Kategorisieren der typischen Tasks, die abgeschlossen werden müssen, um IBM InfoSphere Identity Insight effektiv bereitstellen und verwenden zu können. Möglicherweise verwenden viele verschiedene Typen von Benutzern IBM InfoSphere Identity Insight für verschiedene Zwecke, d. h., Benutzer sind bei der Verwendung des Produkts für die Aufgaben mindestens einer Rolle zuständig.

Sie können basierend auf den verschiedenen Benutzerrollen und -zuständigkeiten Benutzergruppen definieren.

Die folgenden Rollen zählen zu den gängigsten Benutzerrollen:

Analyst
Analysiert die Daten und prüft Entitäten, Beziehungen und Alerts. Der Analyst definiert, welche Ergebnisse die nützlichsten sind, und stellt sicher, dass das System diese Ergebnisse zurückgibt. Der Analyst arbeitet eng mit dem Bediener und dem Anwendungsadministrator zusammen.

Bediener
Lädt Daten in das System, führt die Pipelines aus, prüft, dass das System ordnungsgemäß ausgeführt wird, und stellt bei Bedarf Berichte zur Qualität bei Ladevorgängen bereit. Der Bediener prüft auch die Ergebnisse, Ausnahmebedingungen und Ereignisse. Der Bediener arbeitet eng mit dem Analysten, dem Datenquellenadministrator und dem Anwendungsadministrator zusammen.

Datenquellenadministrator
Bereitet die Daten zum Laden in das System vor. Hierzu gehört das Konvertieren der Daten in eine UMF-Datei und das Prüfen dieser Datei. Der Datenquellenadministrator arbeitet eng mit den Bedienern, den Anwendungsadministratoren und den Datenbankadministratoren zusammen.

Anwendungsadministrator
Konfiguriert die Anwendung. Hierzu gehört die Konfiguration der Daten, des Entitätsmodells und der Regeln. Der Anwendungsadministrator arbeitet eng mit den Datenquellenadministratoren und den Bedienern zusammen, um das Entitätsmodell zu definieren, und koordiniert Konfigurationsänderungen mit dem Datenbankadministrator, dem Datenquellenadministrator und den Bedienern. Der Anwendungsadministrator koordiniert die Tätigkeit der für das Gesamtsystem verantwortlichen Administratoren (falls vorhanden) und berät sich mit diesen.

Datenbankadministrator
Stellt sicher, dass die Datenbank zur Verwendung mit der Anwendung entsprechend konfiguriert und optimiert ist. Der Datenbankadministrator arbeitet eng mit dem Bediener, dem Datenquellenadministrator und dem Anwendungsadministrator zusammen.

Systemarchitekt
Plant die Bereitstellung der Anwendung durch Schätzen der Hardware- und Softwareanforderungen. Der Systemarchitekt arbeitet eng mit dem Installationsverantwortlichen, dem Datenbankadministrator, dem Datenquellenadministrator und dem Anwendungsadministrator zusammen, um sicherzustellen, dass die Bereitstellung die Vision, Strategien und Zielsetzungen erfüllt und in Ihre Geschäftsprozesse integriert werden kann, sodass die erwarteten Ergebnisse erzielt werden.

Installationsverantwortlicher
Verwaltet die Installation und Erstkonfiguration der Anwendung. Der Installationsverantwortliche konfiguriert Erstbenutzer im System. Häufig arbeitet IBM Professional Services mit dem Systemarchitekten zusammen, um diese Aufgaben durchzuführen.

Programmierer
Entwirft und entwickelt grafische Oberflächen oder passt grafische Oberflächen für die verschiedenen Funktionen an, sodass die Bereitstellung der Anwendung nahtlos in Ihre Umgebung integriert werden kann. Der Programmierer arbeitet eng mit dem Systemarchitekten und dem Anwendungsadministrator zusammen, häufig, um Alerts auf die für Ihre Umgebung effektivste Art an die entsprechenden Benutzer zu verteilen.

Sicherheitsarchitekt
Stellt sicher, dass das Projektteam die Sicherheitsvorgaben einhält und ein sicheres System implementiert. Der Sicherheitsarchitekt arbeitet eng mit dem Systemarchitekten, dem Installationsverantwortlichen und dem Datenbankadministrator zusammen.

Kapitel 3. Konfigurieren der Datenbanken

Sie müssen die erforderlichen Datenbanken konfigurieren, bevor Sie das Produkt installieren.

Setzen der Umgebungsvariablen

Für DB2- oder Oracle-Datenbanken müssen Sie Umgebungsvariablen setzen.

DB2-Umgebungsvariablen

Setzen Sie auf der Zielmaschine alle nachfolgend aufgeführten erforderlichen Umgebungsvariablen für Ihr Betriebssystem.

AIX-Umgebungsvariablen

Anmerkung: Sie müssen sicherstellen, dass diese Umgebungsvariablenwerte allen vorhandenen Einträge dieser Umgebungsvariablen vorangestellt werden.

Alle Umgebungsvariablen müssen groß geschrieben werden.

Tabelle 20. AIX-Umgebungsvariablen für DB2-Datenbanken

Umgebungsvariable	Wert	Bedingungen
DB2DIR	Installationspfad der DB2-Software	Dabei ist *DB2DIR* die Position, an der die DB2-Client/Server-Software installiert ist.
DB2INSTANCE	Name der DB2-Datenbankinstanz	Dabei ist *DB2INSTANCE* der Name der von Ihnen erstellten DB2-Datenbankinstanz.
LIBPATH	$*DB2DIR*/lib64:*installationsverzeichnis*/lib	Dabei ist *DB2DIR* die Position, an der die DB2-Client/Server-Software installiert ist, und *INSTALLDIRECTORY* ist die Position, an der das Produkt installiert wird.

Linux-Umgebungsvariablen

Tabelle 21. Linux-Umgebungsvariablen für DB2-Datenbanken

Umgebungsvariable	Wert	Bedingungen
DB2DIR	Installationspfad der DB2-Software	Dabei ist *DB2DIR* die Position, an der die DB2-Client/Server-Software installiert ist.
DB2INSTANCE	Name der DB2-Datenbankinstanz	Dabei ist *DB2INSTANCE* der Name der von Ihnen erstellten DB2-Datenbankinstanz.
LD_LIBRARY_PATH	$*DB2DIR*/lib64:*installationsverzeichnis*/lib	Dabei ist *DB2DIR* die Position, an der die DB2-Client/Server-Software installiert ist, und *INSTALLDIRECTORY* ist die Position, an der das Produkt installiert wird.

Microsoft Windows-Umgebungsvariablen

Beim Konfigurieren von Umgebungsvariablen in einer Microsoft Windows-Umgebung müssen Sie die Microsoft Windows-Namenskonvention 8.3 beachten. Die Umgebungsvariablen dürfen keine Leerzeichen enthalten.

Tabelle 22. Microsoft Windows-Umgebungsvariablen für DB2-Datenbanken

Umgebungsvariable	Wert	Bedingungen
DB2DIR	Installationspfad der DB2-Software	Dabei ist *DB2DIR* die Position, an der die DB2-Instanz erstellt wurde. Bei einigen Versionen von DB2 ist stattdessen *DB2_HOME* oder *DB2PATH* eingestellt. Wenn *DB2DIR* nicht gefunden wird, sucht das Installationsprogramm daher nach diesen Umgebungsvariablen.
DB2INSTANCE	Name der DB2-Datenbankinstanz	Dabei ist *DB2INSTANCE* der Name der von Ihnen erstellten DB2-Datenbankinstanz.
DB2CODEPAGE	Ist auf den CODEPAGE-Wert der DB2-Datenbank gesetzt.	Eine Abweichung kann Codierungsprobleme beim Laden von Latin-1-/UTF-8-Daten verursachen.

Oracle-Umgebungsvariablen

Setzen Sie auf der Zielmaschine alle nachfolgend aufgeführten erforderlichen Umgebungsvariablen für Ihr Betriebssystem.

Anmerkung: Sie müssen sicherstellen, dass diese Umgebungsvariablenwerte allen vorhandenen Einträge dieser Umgebungsvariablen vorangestellt werden.

Alle Umgebungsvariablen müssen groß geschrieben werden.

AIX-Umgebungsvariablen

Tabelle 23. AIX-Umgebungsvariablen für Oracle-Datenbanken

Umgebungsvariable	Wert	Bedingungen
ORACLE_HOME	Installationsverzeichnis der Oracle-Client-Software	Dabei ist *ORACLE_HOME* die Position, an der die Oracle-Client-Software installiert wird.
LIBPATH	$*ORACLE_HOME*/lib:<*produktinstallationsverzeichnis*>/lib	Dabei ist *ORACLE_HOME* das Installationsverzeichnis der Oracle-Client-Software und <*produktinstallationsverzeichnis*> gibt die Position an, an der das Produkt installiert wird.

Linux-Umgebungsvariablen (64 Bit)

Tabelle 24. Linux-Umgebungsvariablen (64 Bit) für Oracle-Datenbanken

Umgebungsvariable	Wert	Bedingungen
ORACLE_HOME	Installationsverzeichnis der Oracle-Client-Software	Dabei ist *ORACLE_HOME* die Position, an der die Oracle-Client-Software installiert wird.
LD_LIBRARY_PATH	$*ORACLE_HOME*/lib:<*produktinstallations-verzeichnis*>/lib	Dabei ist *ORACLE_HOME* das Installationsverzeichnis der Oracle-Client-Software und <*produktinstallations-verzeichnis*> gibt die Position an, an der das Produkt installiert wird.

Microsoft Windows-Umgebungsvariablen

Beim Konfigurieren von Umgebungsvariablen in einer Microsoft Windows-Umgebung müssen Sie die Microsoft Windows-Namenskonvention 8.3 beachten. Die Umgebungsvariablen dürfen keine Leerzeichen enthalten.

Tabelle 25. Microsoft Windows-Umgebungsvariablen für Oracle-Datenbanken

Umgebungsvariable	Wert	Bedingungen
ORACLE_HOME	Installationsverzeichnis der Oracle-Client-Software	Dabei ist *ORACLE_HOME* die Position, an der die Oracle-Client-Software installiert wird.

Microsoft SQL Server-Umgebungsvariablen

Setzen Sie auf der Zielmaschine alle nachfolgend aufgeführten erforderlichen Umgebungsvariablen für Ihr Betriebssystem.

Microsoft Windows-Umgebungsvariablen

Beim Konfigurieren von Umgebungsvariablen in einer Microsoft Windows-Umgebung müssen Sie die Microsoft Windows-Namenskonvention 8.3 beachten. Die Umgebungsvariablen dürfen keine Leerzeichen enthalten.

Tabelle 26. Microsoft Windows-Umgebungsvariablen für Microsoft SQL Server-Datenbanken

Umgebungsvariable	Wert	Bedingungen
MSSQL_JDBC	Position des Microsoft-JDBC-Treibers.	Datei steht *MSSQL_JDBC* für die Position, an der sich der Microsoft-JDBC-Treiber mit den `.jar`-Dateien auf dem Server befindet. Dieser Pfad wird vom Produktinstallationsprogramm berücksichtigt.

Festlegen des ODBC-DSN für Microsoft SQL Server

Der Microsoft SQL Server-ODBC-DSN (DSN - Datenquellenname) muss auf genau denselben Wert wie der Microsoft SQL Server-Datenbankname gesetzt werden.

Informationen zu diesem Vorgang

Der Verbindungstyp des Datenquellennamens muss in Abhängigkeit des Authentifizierungsverfahrens festgelegt werden, für das Ihre Microsoft SQL Server-Instanz konfiguriert ist (Betriebssystembenutzer- oder SQL Server-Authentifizierung).

Aktivieren von XA-Transaktionen für Microsoft SQL Server

Sie müssen XA-Transaktionen aktivieren, um die Konfigurationskonsole und Visualizer ordnungsgemäß ausführen zu können.

Vorgehensweise

1. Aktivieren von XA-Transaktionen mit dem Tool zur Verwaltung der Komponentenservices von Windows.
2. Führen Sie den Service für den verteilten Transaktionskoordinator über den Microsoft SQL Server-Desktop aus.
3. Installieren Sie die gespeicherten JTA-Prozeduren (JTA - Java Transaction API) wie in der entsprechenden Microsoft SQL Server-Dokumentation beschrieben.
4. Legen Sie für Benutzer die Berechtigungen für das Ausführen der gespeicherten JTA-Prozeduren mithilfe von Microsoft SQL Server Enterprise Manager fest.

Erteilen von CREATE VIEW-Zugriffsrechten für Oracle-Benutzer

Damit das Produkt ordnungsgemäß ausgeführt wird, müssen Datenbankbenutzern von Oracle mit Grant CREATE VIEW-Zugriffsrechte erteilt werden.

Informationen zu diesem Vorgang

Die CREATE VIEW-Zugriffsrechte müssen dem Benutzer direkt und nicht über eine rollenbasierte Zuordnung zugeordnet werden.

Erstellen und Konfigurieren der Datenbanken

Sie erstellen eine einzelne Datenbank, die so genannte Entitätendatenbank, für alle Komponenten des zu verwendenden Produkts.

Erstellen der Entitätendatenbank

Sie müssen eine Datenbank erstellen, in der die Pipeline Identitäten, Entitäten, Beziehungen und Alerts, aber auch Konfigurationsinformationen für die Konfigurationskonsole und die Anwendungsüberwachungsinformationen speichern kann.

Informationen zu diesem Vorgang

Anweisungen zum Erstellen neuer Datenbanken finden Sie in der Dokumentation zu Ihrer Datenbank.

Verwenden Sie GROSSBUCHSTABEN für Datenbanknamen.

Konfigurieren der Clientauthentifizierung

Die Clientauthentifizierung ermöglicht es Benutzern, eine Verbindung zur Entitätendatenbank herzustellen, ohne in der INI-Datei der Pipeline weitere Berechtigungsnachweise durch Angabe von Benutzername und Kennwort anzugeben.

Informationen zu diesem Vorgang

Die Clientauthentifizierung wird auch als Datenbankauthentifizierung auf der Basis gesicherter Betriebssystemdaten bezeichnet. Die Clientauthentifizierung ermöglicht es, eine Verbindung über den Benutzernamen herzustellen, der zurzeit angemeldet ist. Bei diesem Authentifizierungsschema wird davon ausgegangen, dass der Benutzer bereits vom Betriebssystem ordnungsgemäß authentifiziert wurde. Die Clientauthentifizierung kann auf DB2- und Oracle-Datenbankplattformen verwendet werden. Die Pipelines und IBM WebSphere-Prozesse müssen von einem Betriebssystembenutzer ausgeführt werden, der in gesichertem Modus Zugriff auf die Entitätendatenbank hat. Müssen diese Prozesse von mehreren Benutzern ausgeführt werden, setzen Sie sich mit dem IBM Support in Verbindung, um weitere Informationen zu erhalten.

Konfigurieren der Clientauthentifizierung für DB2-Datenbanken

Richten Sie DB2 für die Verwendung der Clientauthentifizierung ein.

Vorgehensweise

1. Legen Sie die folgenden globalen Datenbankserverkonfigurationsoptionen fest:
   a. Setzen Sie **authentication** auf den Wert client.
   b. Setzen Sie **trust_allclnts** auf den Wert yes.
   c. Setzen Sie **trust_clntauth** auf den Wert server.
2. Katalogisieren Sie die Produktdatenbanken unter Verwendung des Parameters **authentication client** des Befehls **db2 catalog database**.
3. Synchronisieren Sie die Betriebssystem- und DB2-Datenbankbenutzernamen.
4. Stellen Sie sicher, dass neben dem DB2-JDBC-Standardtreiber des Typs 4 auch der DB2-JDBC-Treiber des Typs 2 vorhanden ist. Dieser sollte sich in der Datei db2java.zip befinden.
5. Aktivieren Sie während der Produktinstallation die gesicherte Authentifizierung.

Konfigurieren der Clientauthentifizierung für Oracle-Datenbanken

Richten Sie Oracle für die Verwendung der Clientauthentifizierung ein.

Vorgehensweise

1. Legen Sie die folgenden globalen Datenbankserverkonfigurationsoptionen fest:
   a. Setzen Sie **os_authent_prefix** auf den Wert OPS$.
   b. Setzen Sie **remote_os_authent** auf den Wert TRUE.
2. Erstellen Sie Oracle-Datenbankbenutzer so, dass der Benutzer sowohl externe Authentifizierungsverfahren als auch Datenbankauthentifizierungsverfahren verwenden kann. Beispielsyntax:

```
CREATE USER OPS$<benutzer> IDENTIFIED BY <db-kennwort> DEFAULT
TABLESPACE <tabellenbereich> TEMPORARY TABLESPACE <temp_tabellenbereich>
QUOTA UNLIMITED ON <tabellenbereich>;
GRANT CONNECT, RESOURCE TO OPS$<benutzer>;
```

3. Stellen Sie sicher, dass neben dem Oracle-JDBC-Standardtreiber des Typs 4 auch der Oracle-JDBC-Treiber des Typs 2 vorhanden ist. Bei Oracle sollte sich dieser in der Datei ojdbc16.zip befinden.

4. Aktivieren Sie während der Produktinstallation die gesicherte Authentifizierung. Wenn Sie vom Produktinstallationsprogramm zur Angabe der Datenbankberechtigungsnachweise aufgefordert werden, geben Sie einen Benutzernamen mit dem Präfix OPS$ an.

Konfigurieren der Clientauthentifizierung für Microsoft SQL Server-Datenbanken

Richten Sie Microsoft SQL Server für die Verwendung der Clientauthentifizierung ein.

Vorgehensweise

1. Stellen Sie sicher, dass der System-DSN (Data Source Name - Datenquellenname) die Windows NT-Authentifizierung und nicht die SQL Server-Authentifizierung verwendet. Erstellen Sie alternativ einen neuen System-DSN, der die Windows NT-Authentifizierung verwendet.
2. Stellen Sie sicher, dass der Datenbankbenutzer mit Administratorberechtigung in Microsoft SQL Server Enterprise Manager vorhanden ist. Erteilen Sie dem Administrator mit Grant für jede Produktdatenbank mindestens den Datenbankzugriff public und db_owner. Legen Sie als Standarddatenbank die Entitätendatenbank fest.
3. Stellen Sie sicher, dass der JDBC-ODBC-Bridge-Treiber des Typs 1 vorhanden ist.
4. Erstellen Sie einen Datenbankbenutzer (nicht den Betriebssystembenutzer), der Zugriff auf die Entitätendatenbank hat.
5. Aktivieren Sie während der Produktinstallation die gesicherte Authentifizierung. Wenn Sie vom Produktinstallationsprogramm zur Angabe der Datenbankberechtigungsnachweise aufgefordert werden, verwenden Sie den Datenbankbenutzer (nicht den Betriebssystembenutzer).

Dimensionierung des Oracle-Anweisungscache

Der Anweisungscache muss vom Oracle-Datenbankadministrator angemessen dimensioniert werden.

Informationen zu diesem Vorgang

Das Produkt kann sehr anweisungsintensiv sein, was zu einem raschen Anwachsen des Oracle-Anweisungscache und einem Überschreiten der Standardeinstellungen für die Oracle-Datenbank führen kann. Weitere Informationen zur Dimensionierung und Optimierung dieser Parameter finden Sie in der Oracle-Dokumentation.

Vorgehensweise

Konfigurieren Sie die folgenden Parameter auf der Serverebene unter Verwendung des Oracle-Befehls **ALTER SYSTEM SET**:

SESSION_CACHED_CURSORS
Ein guter Wert für diesen Parameter sind 20 gleichzeitig aktive Cursor pro Pipeline oder Thread für die parallele Pipelineverarbeitung.

OPEN_CURSORS
Ein guter Wert für diesen Parameter sind 20 gleichzeitig aktive Cursor pro Pipeline oder Thread für die parallele Pipelineverarbeitung.

CURSOR_SHARING
Dieser Parameter hat eine große Auswirkung auf die Leistung. Berücksichtigen

Sie beim Konfigurieren dieses Parameters, dass das Produkt in hohem Maße Gebrauch von Bindevariablen macht und die Anwendung von einer gemeinsamen Cursornutzung profitiert.

Kapitel 4. Verwaltung

Die Verwaltungstasks umfassen die Konfiguration und Verwaltung der Systemeinstellungen für die Benutzerschnittstellen sowie die Aktualisierung globaler Konfigurationseinstellungen. Administratoren können die Verwaltungstasks über die Konfigurationskonsole durchführen.

Verwalten der Konsole

Zur effektiven Verwendung der Konsole müssen Sie die Browser konfigurieren, Konten für die entsprechenden Benutzer einrichten und den Zugriff auf die Konfigurationskonsole verwalten.

Konfigurationskonsole

Die Konfigurationskonsole stellt eine taskorientierte Schnittstelle bereit, die Ihnen die Ausführung einiger der wichtigsten Tasks zum Einrichten von Identity Insight für den Betrieb erleichtert.

Die Konfigurationskonsole wird von IBM WebSphere Liberty gehostet.

Verwalten der Systemkonfiguration

Über die Konfigurationskonsole können Sie die meisten Systemparameter und -optionen in einer Gruppe vereinfachter und optimierter Schnittstellen konfigurieren. Die Konsole schreibt die Änderungen dann in die Konfigurationsdatenbank. Direkt an der Konfigurationsdatenbank vorgenommene Änderungen werden nicht unterstützt. Diese Änderungen führen sehr wahrscheinlich zu einem nicht ordnungsgemäß funktionierenden Produkt.

Benutzerrollen und -zuständigkeiten

Benutzerrollen helfen beim Kategorisieren der typischen Tasks, die abgeschlossen werden müssen, um IBM InfoSphere Identity Insight effektiv bereitstellen und verwenden zu können. Möglicherweise verwenden viele verschiedene Typen von Benutzern IBM InfoSphere Identity Insight für verschiedene Zwecke, d. h., Benutzer sind bei der Verwendung des Produkts für die Aufgaben mindestens einer Rolle zuständig.

Sie können basierend auf den verschiedenen Benutzerrollen und -zuständigkeiten Benutzergruppen definieren.

Die folgenden Rollen zählen zu den gängigsten Benutzerrollen:

Analyst
Analysiert die Daten und prüft Entitäten, Beziehungen und Alerts. Der Analyst definiert, welche Ergebnisse die nützlichsten sind, und stellt sicher, dass das System diese Ergebnisse zurückgibt. Der Analyst arbeitet eng mit dem Bediener und dem Anwendungsadministrator zusammen.

Bediener
Lädt Daten in das System, führt die Pipelines aus, prüft, dass das System ordnungsgemäß ausgeführt wird, und stellt bei Bedarf Berichte zur Qualität bei Ladevorgängen bereit. Der Bediener prüft auch die Ergebnisse, Aus-

nahmebedingungen und Ereignisse. Der Bediener arbeitet eng mit dem Analysten, dem Datenquellenadministrator und dem Anwendungsadministrator zusammen.

Datenquellenadministrator
Bereitet die Daten zum Laden in das System vor. Hierzu gehört das Konvertieren der Daten in eine UMF-Datei und das Prüfen dieser Datei. Der Datenquellenadministrator arbeitet eng mit den Bedienern, den Anwendungsadministratoren und den Datenbankadministratoren zusammen.

Anwendungsadministrator
Konfiguriert die Anwendung. Hierzu gehört die Konfiguration der Daten, des Entitätsmodells und der Regeln. Der Anwendungsadministrator arbeitet eng mit den Datenquellenadministratoren und den Bedienern zusammen, um das Entitätsmodell zu definieren, und koordiniert Konfigurationsänderungen mit dem Datenbankadministrator, dem Datenquellenadministrator und den Bedienern. Der Anwendungsadministrator koordiniert die Tätigkeit der für das Gesamtsystem verantwortlichen Administratoren (falls vorhanden) und berät sich mit diesen.

Datenbankadministrator
Stellt sicher, dass die Datenbank zur Verwendung mit der Anwendung entsprechend konfiguriert und optimiert ist. Der Datenbankadministrator arbeitet eng mit dem Bediener, dem Datenquellenadministrator und dem Anwendungsadministrator zusammen.

Systemarchitekt
Plant die Bereitstellung der Anwendung durch Schätzen der Hardware- und Softwareanforderungen. Der Systemarchitekt arbeitet eng mit dem Installationsverantwortlichen, dem Datenbankadministrator, dem Datenquellenadministrator und dem Anwendungsadministrator zusammen, um sicherzustellen, dass die Bereitstellung die Vision, Strategien und Zielsetzungen erfüllt und in Ihre Geschäftsprozesse integriert werden kann, sodass die erwarteten Ergebnisse erzielt werden.

Installationsverantwortlicher
Verwaltet die Installation und Erstkonfiguration der Anwendung. Der Installationsverantwortliche konfiguriert Erstbenutzer im System. Häufig arbeitet IBM Professional Services mit dem Systemarchitekten zusammen, um diese Aufgaben durchzuführen.

Programmierer
Entwirft und entwickelt grafische Oberflächen oder passt grafische Oberflächen für die verschiedenen Funktionen an, sodass die Bereitstellung der Anwendung nahtlos in Ihre Umgebung integriert werden kann. Der Programmierer arbeitet eng mit dem Systemarchitekten und dem Anwendungsadministrator zusammen, häufig, um Alerts auf die für Ihre Umgebung effektivste Art an die entsprechenden Benutzer zu verteilen.

Sicherheitsarchitekt
Stellt sicher, dass das Projektteam die Sicherheitsvorgaben einhält und ein sicheres System implementiert. Der Sicherheitsarchitekt arbeitet eng mit dem Systemarchitekten, dem Installationsverantwortlichen und dem Datenbankadministrator zusammen.

Optimale Browsereinstellungen für Verwendung der Konfigurationskonsole

Die Konfigurationskonsole ist eine webbasierte Anwendung, die bestimmte Einstellungen für den Browser erfordert, mit dem Sie auf die Konsole zugreifen.

Verwenden Sie die folgenden Browsereinstellungen, um die Konfigurationskonsole optimal anzuzeigen:

Tabelle 27. Optimale Browsereinstellungen

Einstellung	Wert	Beschreibung
Auflösung	Mindestens 800 x 600; 1024 x 768 oder höher wird empfohlen	
Textgröße	Mittel	
JavaScript	Ein	
Cookies	Ein	Zumindest Sitzungscookies der aktuellen Webseite müssen aktiviert sein.
Sicherheit - Vertrauenswürdige Website	HTTP-Adresse der Konfigurationskonsole	Stellen Sie sicher, dass sich die HTTP-Adresse der Konfigurationskonsole in der Liste der vertrauenswürdigen Internet-Websites befindet.
Sicherheit - Downloadoptionen	Aktiviert	Stellen Sie sicher, dass alle Downloadoptionen für vertrauenswürdige Internet-Websites aktiviert sind.
Popup-Blocker	Popups von der HTTP-Adresse der Konfigurationskonsole zulassen	Stellen Sie sicher, dass sich die HTTP-Adresse der Konfigurationskonsole in der Liste der Websites befindet, für die Popups zulässig sind.

Anmelden an der Konfigurationskonsole

Das Anmelden an der Konfigurationskonsole ermöglicht Ihnen die Anzeige und das Ändern von Systemkonfigurationseinstellungen.

Vorbereitende Schritte

Ihr Systemadministrator muss ein Benutzerkonto für Sie erstellt haben, das Sie zum Anmelden verwenden können.

Vorgehensweise

1. Öffnen Sie die Konfigurationskonsole:
   a. Öffnen Sie den Browser, in dem Sie die Konfigurationskonsole ausführen wollen.
   b. Geben Sie die URL für die Konfigurationskonsole mit der folgenden Syntax ein: `http://<servername>/console/`.
   c. Drücken Sie die Eingabetaste.
2. Geben Sie im Fenster **Anmelden** Ihren Benutzernamen und Ihr Kennwort ein.
3. Optional: Wenn Sie als Systemadministrator die aktuelle Systemkonfiguration bearbeiten müssen, wählen Sie die Option **Konfiguration bearbeiten** aus. Wenn Sie die aktuelle Systemkonfiguration bearbeiten, müssen Sie in der Regel alle Pipelines stoppen, damit neue Daten erst nach Abschluss der Konfigurationsänderungen bearbeitet werden.
4. Klicken Sie die Schaltfläche **Anmelden** an.

Nächste Schritte

Wenn Ihr Benutzername und Kennwort mit denen übereinstimmen, die für die Konfigurationskonsole festgelegt wurden, wird die Konfigurationskonsole geöffnet. Andernfalls tritt ein Fehler auf und Sie müssen sich erneut anmelden, nachdem Sie den entsprechenden Benutzernamen und das zugehörige Kennwort ermittelt haben.

Abmelden von der Konfigurationskonsole

Sie können sich von einer aktuellen Sitzung der Konfigurationskonsole abmelden, ohne die Anwendung zu beenden. Wenn 60 Minuten lang keine Aktivität erfolgt, meldet die Konfigurationskonsole den aktuellen Benutzer automatisch ab.

Vorgehensweise

Klicken Sie **Abmelden** in der rechten oberen Ecke eines beliebigen Konfigurationskonsolfensters an.

Nächste Schritte

Sie sind jetzt von der Konfigurationskonsolsitzung abgemeldet und müssen sich erneut anmelden, um mit der Verwendung der Konfigurationskonsole fortfahren zu können.

Benutzerkonten für die Konfigurationskonsole

Ihr Systemadministrator erstellt und übergibt Ihnen ein Benutzerkonto für die Anmeldung an der Konfigurationskonsole. Benutzerkonten bestehen aus einem Benutzernamen und einem Kennwort, das Sie ändern können.

Sie können sich mit demselben Benutzerkonto mehrmals anmelden. Wenn Sie ein Benutzerkonto mit anderen Benutzern gemeinsam nutzen, können Sie sich nicht zur selben Zeit an der Konfigurationskonsole anmelden. Wenn Sie versuchen, sich mit einem Benutzerkonto anzumelden, das zurzeit von einem anderen Benutzer verwendet wird, wird dessen Sitzung beendet und Ihre Sitzung gestartet.

Der Systemadministrator kann jederzeit zusätzliche Benutzerkonten erstellen. Der Systemadministrator kann zudem die Konfigurationskonsole erneut starten, um eine Zeitlimitüberschreitung zu erzwingen.

Verwalten des Zugriffs auf die Konfigurationskonsole

Jedem Benutzer der Konfigurationskonsole muss der Zugriff auf die Konfigurationskonsole erteilt werden, und zum Anmelden an der Konsole müssen ein Benutzername und das dazugehörige Kennwort verwendet werden. Sie können die Benutzernamen und Kennwörter mithilfe der anwendungsspezifischen Datei verwalten, die von der Konfigurationskonsole bereitgestellt wird. Falls Ihre Benutzer über Benutzerkonten des Verwaltungssystems für relationale Datenbanken verfügen, mit denen sie auf die Entitätendatenbank zugreifen können, können Sie den Zugriff der Benutzer auf die Konfigurationskonsole auch über diese Benutzerkonten und Datenbankverwaltungsprogramme verwalten. Diese Benutzernamen und Kennwörter sind unabhängig von den Benutzernamen und Kennwörtern, die für den Zugriff auf Visualizer konfiguriert sind, und nicht unbedingt mit den Visualizer-Benutzernamen und -Kennwörtern identisch.

Verwalten des Zugriffs auf die Konfigurationskonsole mithilfe von Datenbankanmeldeinformationen

Sie können den Zugriff auf die Konfigurationskonsole mit der Benutzer-ID und dem zugehörigen Kennwort für die Entitätendatenbank verwalten.

Vorbereitende Schritte

Stellen Sie zur Vermeidung von Konfigurationskonflikten sicher, dass niemand an der Konfigurationskonsole angemeldet ist.

Vorgehensweise

1. Starten Sie das Konfigurationsdienstprogramm, indem Sie zum Verzeichnis `<installationsposition>/installer/util/` wechseln und einen der folgenden Befehle eingeben:
   a. Geben Sie unter Windows `eacfg.bat –i –l ../logs/` ein.
   b. Geben Sie unter UNIX `eacfg –i –l ../logs/` ein.
2. Klicken Sie **Einstellungen der Konfigurationskonsole** im Navigationsteilfenster an.
3. Klicken Sie das Kontrollkästchen **Authentifizierung der Konfigurationskonsole modifizieren** an.
4. Klicken Sie das Optionsfeld **SQL-Authentifizierung** an.
5. Klicken Sie **OK** an.
6. Verwenden Sie Ihre Datenbankverwaltungsprogrammtools, um die Anmeldeinformationen für die Konfigurationskonsole (und die Entitätendatenbank) anzugeben.

Verwalten des Zugriffs auf die Konfigurationskonsole mithilfe des Kennwortmanagers

Sie können den Zugriff auf die Konfigurationskonsole mithilfe des Kennwortmanagers verwalten.

Vorbereitende Schritte

Stellen Sie sicher, dass niemand an der Konfigurationskonsole angemeldet ist.

Vorgehensweise

1. Starten Sie das Konfigurationsdienstprogramm, indem Sie zum Verzeichnis `<installationsposition>/installer/util/` wechseln und einen der folgenden Befehle eingeben:
   a. Geben Sie unter Windows `eacfg.bat –i –l ../logs/` ein.
   b. Geben Sie unter UNIX `eacfg –i –l ../logs/` ein.
2. Klicken Sie **Einstellungen der Konfigurationskonsole** im Navigationsteilfenster an.
3. Klicken Sie das Kontrollkästchen **Authentifizierung der Konfigurationskonsole modifizieren** an.
4. Klicken Sie das Optionsfeld **Dateiauthentifizierung** an.
5. Klicken Sie **OK** an.

Ergebnisse

Sie können jetzt den Kennwortmanager (pwdmgr.jar) im Verzeichnis `srd-home/console` verwenden, um Benutzer hinzuzufügen oder zu löschen oder

um Kennwörter von Benutzern in der Datei `console_password.properties` zurückzusetzen.

Anzeigen einer Liste der Benutzer und deren Status:

Sie können eine Liste der Benutzer und deren Status mit dem Kennwortmanagerbefehl anzeigen.

Vorgehensweise

1. Wechseln Sie in einem Befehlsfenster in das Verzeichnis \srd-home\console.
2. Geben Sie den folgenden Befehl ein. `pwdmgr console-passwords.properties console-principals.properties -l`

Beispiel

Wenn Sie z. B. den Befehl `pwdmgr console-passwords.properties console-principals.properties -l` eingeben, könnte die folgende Beispielausgabe angezeigt werden:

```
admin (super-user)
judy (super-user)
allen (super-user)
jose (super-user) *** NEVER LOGGED IN ***
```

Wenn Sie vor Kurzem ein Kennwort zurückgesetzt haben, wird eine Nachricht mit der Information angezeigt, dass der Benutzer mit diesem neuen Kennwort noch nicht an der Konfigurationskonsole angemeldet ist.

Hinzufügen eines neuen Benutzers:

Wenn Sie den Zugriff auf die Konfigurationskonsole verwalten, können Sie in der Datei console-passwords.properties über den Kennwortverwaltungsbefehl einen neuen Benutzer hinzufügen.

Vorgehensweise

1. Wechseln Sie in einem Befehlsfenster in das Verzeichnis \srd-home\console.
2. Geben Sie den `pwdmgr console-passwords.properties console-principals.properties -a benutzername` Befehl ein. Dabei ist *benutzername* der Benutzername, den Sie hinzufügen wollen.

Nächste Schritte

Ein Benutzer wird hinzugefügt. Diesem ist das Standardkennwort und der von Ihnen angegebene Benutzername zugeordnet. Der neue Benutzer kann sich jetzt an der Konfigurationskonsole anmelden.

Löschen eines vorhandenen Benutzers:

Wenn Sie den Zugriff auf die Konfigurationskonsole verwalten, können Sie in der Datei console-passwords.properties über den Befehl pwdmgr einen vorhanden Benutzer löschen.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie den Befehl über das Verzeichnis `\srd-home\console\` absetzen. Stellen Sie außerdem sicher, dass die Benutzer vorhanden sind, die Sie lö-

schen wollen. Beim Versuch, einen nicht vorhandenen Benutzer zu löschen, erhalten Sie eine Fehlernachricht.

Vorgehensweise

1. Wechseln Sie in einem Befehlsfenster in das Verzeichnis \srd-home\console.
2. Geben Sie den Befehl `pwdmgr console-passwords.properties console-principals.properties -d benutzername` ein, wobei *benutzername* der Benutzername ist, den Sie löschen wollen.

Nächste Schritte

Der Benutzer mit dem Benutzernamen, den Sie gerade gelöscht haben, kann sich nicht mehr an der Konfigurationskonsole anmelden.

Zurücksetzen eines Kennworts:

Wenn Benutzer ihr Kennwort für das Konfigurationskonsolenbenutzerkonto vergessen haben oder ein Kennwort aus Sicherheitsgründen geändert werden muss, können Systemadministratoren das Kennwort mit dem Kennwortmanagerbefehl (pwdmgr) zurücksetzen.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie den Befehl über das Verzeichnis `\srd-home\console\` absetzen.

Vorgehensweise

1. Wechseln Sie in einem Befehlsfenster in das Verzeichnis `\srd-home\console` .
2. Geben Sie den folgenden Befehl ein: `pwdmgr console-passwords.properties console-principals.properties -r benutzername`. Dabei ist *benutzername* der Benutzername des Benutzers, dessen Kennwort Sie zurücksetzen wollen.

Nächste Schritte

Das Kennwort des von Ihnen angegebenen Benutzernamens ist jetzt so zurückgesetzt, dass es mit dem Benutzernamen übereinstimmt. Wenn sich Benutzer, deren Kennwort zurückgesetzt wurde, das nächste Mal an der Konfigurationskonsole anmelden, werden sie vom System zum Zurücksetzen ihres Kennwort aufgefordert. Daher sollten Sie dem Benutzer nach dem Zurücksetzen eines Benutzerkennworts vorschlagen, sich so schnell wie möglich anzumelden und sein Kennwort zu ändern, um Sicherheitsprobleme zu minimieren.

Kennwortmanagerbefehl:

Mit dem Kennwortmanagerbefehl verwalten Sie den Zugriff auf die Konfigurationskonsole mithilfe einer Eigenschaftendatei. Sie können Benutzer hinzufügen, löschen und auflisten und ihre Kennwörter zurücksetzen.

Die Syntax für den Kennwortmanagerbefehl lautet:

`pwdmgr -option parameter`

Setzen Sie den Befehl über das Verzeichnis `\srd-home\console\` ab, um den Kennwortmanagerbefehl zu verwenden.

Optionen und Parameter

Jede Option und die zugehörigen Parameter für den Kennwortmanagerbefehl müssen als separate Befehle angegeben werden. Wird keine Option angegeben, wird die Hilfe für den Befehl angezeigt.

-a *benutzername*
Fügt jeweils einen Benutzer hinzu.

Der von Ihnen angegebene Name für den Benutzer ist der Standardwert für das Anfangskennwort. Der Benutzer wird bei der ersten Anmeldung an der Konfigurationskonsole aufgefordert, dieses Kennwort zu ändern.

Wenn Sie einen bereits vorhandenen Benutzer hinzufügen, erhalten Sie eine Fehlernachricht.

-d *benutzername*
Löscht jeweils einen Benutzer.

Wenn Sie einen nicht vorhandenen Benutzer zu löschen versuchen, erhalten Sie eine Fehlernachricht. Sie können eine Liste der Benutzer mit der Option zum Auflisten anzeigen, um zu überprüfen, ob der Benutzer erfolgreich gelöscht wurde.

-l
Zeigt eine Liste aller Benutzer und deren Status an.

-r *benutzername*
Setzt das Kennwort für den angegebenen Benutzer auf die Benutzer-ID zurück. Beispielsweise würde judy/sunflower auf judy/judy zurückgesetzt.

Für den Kennwortmanagerbefehl werden zwei Dateien verwendet:

- console-passwords.properties - In dieser Datei sind alle Benutzernamen und der Nachrichtenauszug der Kennwörter aufgezeichnet.
- console-principals.properties - Diese Datei ist für die zukünftige Verwendung reserviert, um verschiedene Benutzerebenen zu erstellen. Zurzeit werden alle Benutzer der Konfigurationskonsole als Superuser betrachtet und haben Zugriff auf alle Bereiche der Konfigurationskonsole.

Diese Dateien befinden sich im Verzeichnis **srd-home**. Sie dürfen sie jedoch nicht manuell ändern. Sie werden vom Programm zur Überwachung von Benutzeranmeldenamen verwendet und sind für einige andere Befehle erforderliche Parameter.

Kennwortmanagerbeispielbefehle

Geben Sie folgenden Befehl ein, um einen neuen Benutzer mit dem Anmeldenamen und dem Standardkennwort "judy" hinzuzufügen: `pwdmgr -a judy`

Geben Sie folgenden Befehl ein, um den vorhandenen Benutzer mit dem Namen "judy" und dem entsprechenden Kennwort zu löschen: `pwdmgr -d judy`

Geben Sie folgenden Befehl ein, um eine Liste der aktuellen Benutzer und ihren Statustyp anzuzeigen: `pwdmgr -l`

Wenn Sie den Befehl `pwdmgr -l` eingeben, kann beispielsweise die folgende Ausgabe angezeigt werden:

```
admin (super-user)
judy (super-user)
allen (super-user)
jose (super-user) *** NEVER LOGGED IN ***
```

Wenn Sie vor Kurzem ein Kennwort zurückgesetzt haben, wird eine Nachricht mit der Information angezeigt, dass der Benutzer mit diesem neuen Kennwort noch nicht an der Konfigurationskonsole angemeldet ist.

Soll das Kennwort eines Benutzers auf die Benutzer-ID zurückgesetzt werden, geben Sie folgenden Befehl ein: `pwdmgr -r benutzername`

Wenn Sie beispielsweise den Befehl `pwdmgr -r judy` eingeben, wird das Kennwort des vorhandenen Benutzers "judy" auf das Standardkennwort "judy" zurückgesetzt. Wenn die ursprüngliche Kombination Anmeldename/Kennwort "judy/sunflower" lautete, wird sie jetzt auf "judy/judy" zurückgesetzt.

Hilfethemen

Anmeldefenster der Konfigurationskonsole

Über dieses Fenster können Sie sich an der Konfigurationskonsole anmelden.

Benutzer-ID
Geben Sie Ihre Benutzer-ID für die Konfigurationskonsole ein.

Kennwort
Geben Sie Ihr Kennwort für die Konfigurationskonsole ein.

Konfiguration bearbeiten
Wählen Sie dieses Kontrollkästchen aus, um den Bearbeitungsmodus zu verwenden.

Anmelden
Klicken Sie diese Option an, um die Benutzer-ID und das Kennwort abzusenden und auf die Konfigurationskonsole Zugriff zu erhalten.

Inhalt löschen
Klicken Sie diese Option an, um die Einträge für die Benutzer-ID und das Kennwort zu löschen und die Auswahl des Kontrollkästchens **Konfiguration bearbeiten** zurückzunehmen.

Ausführen von Berichten über die Konfigurationskonsole

In der Konfigurationskonsole können Sie Berichte generieren, die Zusammenfassungen von Pipelinestatistikdaten nach Datenquelle anzeigen, oder einen Bericht anzeigen und drucken, der die aktuellen Einstellungen der Systemkonfiguration einschließlich die Konfiguration für die Entitätsauflösung auflistet. Die resultierenden Berichte werden im webbasierten Tool BIRT Report Viewer (Business Intelligence Reporting Tool) angezeigt. Stellen Sie sicher, dass Sie alle Popup-Blocker inaktiviert haben, da diese die Anzeige des Berichts in der Anzeigefunktion beeinträchtigen können.

Anzeigen von statistischen Berichten

Während das Produkt Daten ausführt, protokolliert es statistische Informationen zur Leistung und zu den Daten der eingehenden Datenquellendateien, die geladen wurden. Diese Informationen werden für Sie in zwei Berichten zusammengefasst: **Datenquelle - Ergebnisbericht** und **Laden - Ergebnisbericht**.

Informationen zu diesem Vorgang

Anhand der Statistikdaten zu diesen Berichten können Sie schnell überprüfen, ob das Produkt alle eingehenden Datensätze verarbeitet, operative Entscheidungen zur Produktleistung treffen, die Qualität der eingehenden Daten bewerten und die Anzahl der neuen Identitäten, Entitäten, Beziehungen und Alerts anzeigen, die aus der Verarbeitung der Datendateien resultieren.

Vorgehensweise

1. Wählen Sie in der Konfigurationskonsole **Status** > **Berichte** aus.
2. Erforderlich: Wählen Sie in der Liste **Bericht** einen statistischen Bericht aus:
   - **Datenquelle - Ergebnisbericht** - Dieser Bericht enthält eine nach Datenquelle sortierte statistische Kurzzusammenfassung der geladenen und verarbeiteten Datensätze. Verwenden Sie den Bericht, um die Gesamtzahl geladener Datensätze nach Datenquellendatei, die Gesamtzahl verarbeiteter neuer Identitätsdatensätze nach Datenquellendatei und die Gesamtzahl neuer Entitäten basierend auf den Daten in dieser Datenquellendatei anzuzeigen. Der Bericht **Datenquelle - Ergebnisbericht** ist nach Ladedatum, Lade-ID, Datenquelle und Datenquellendatei sortiert.
   - **Laden - Ergebnisbericht** - Dieser Bericht fasst Statistiken und Qualitätsmerkmale für eine oder mehrere Datenquellen zusammen. Verwenden Sie den Bericht, um Informationen zur Ladeleistung, die Qualität der Datenquellendatei und Zusammenfassungen von Datenwerten anzuzeigen, die zum Auflösen von Entitäten, Erkennen von Beziehungen und Generieren von Alerts verwendet wurden. Dieser Bericht kann Ihnen helfen, die Qualität der aus einer bestimmten Datenquelle geladenen Daten zu ermitteln. Daten von schlechterer Qualität können darauf hinweisen, dass für die Daten in dieser Datenquelle eine zusätzliche Bereinigung erforderlich ist, entweder vor dem Laden in das Produkt oder während der Entitätsauflösung durch Anwenden bestimmter DQM-Regeln (Data Quality Management - Datenqualitätsmanagement) auf die Daten. Der Bericht **Laden - Ergebnisbericht** ist nach Lade-ID sortiert.
3. Geben Sie in das Feld **Anfangsdatum** das Startdatum für den Bericht im Format **mm/tt/jjjj** ein. Standardmäßig enthält dieses Feld das aktuelle Datum.

   Dieses Feld kann leer bleiben. Dies bedeutet dann, dass das Produkt alle Daten für sämtliche angegebenen Kriterien ab dem Datum meldet, an dem das Produkt in Betrieb genommen wurde.
4. Geben Sie in das Feld **Enddatum** das Enddatum für den Bericht im Format **mm/tt/jjjj** ein. Standardmäßig enthält dieses Feld das aktuelle Datum.

   Dieses Feld kann leer bleiben. Dies bedeutet dann, dass das Produkt alle Daten für sämtliche angegebenen Kriterien bis zum aktuellen Datum meldet.
5. Optional: Geben Sie in **Datenquellencode** den Datenquellencode ein, zu dem ein Bericht erstellt werden soll. Der von Ihnen eingegebene Datenquellencode muss genau mit einem konfigurierten Datenquellencode übereinstimmen.

   Dieses Feld kann leer bleiben. Dies bedeutet dann, dass das Produkt Statistikdaten von allen Datenquellen für sämtliche angegebenen Kriterien meldet.
6. Erforderlich: Klicken Sie **Bericht ausführen** an, um den ausgewählten Bericht zu generieren.

Ergebnisse

Das Produkt generiert den ausgewählten statistischen Bericht auf der Basis aller angegebenen Kriterien und zeigt den Bericht in einem separaten Web-Browser-

Fenster für BIRT Report Viewer an. Wenn es keine aufzulistenden Daten gibt, werden im BIRT Report Viewer-Fenster abhängig von den von Ihnen ausgewählten Kriterien der Name des Berichts, Datum und Uhrzeit der Berichtsgenerierung und oben im Fenster **Seite 1/1** angezeigt. Der Datenabschnitt ist leer.

Nächste Schritte

Verwenden Sie die statistischen Informationen in diesem Bericht, um die Optimierung der Produkt- oder der Datendateien zu unterstützen.

Datenquelle - Ergebnisbericht

Der Ergebnisbericht für Datenquellen enthält eine kurze statistische Zusammenfassung nach der Datenquelle der Datensätze, die zur Verarbeitung in das System geladen wurden. Dieser Bericht zeigt die Gesamtzahl der verarbeiteten Datensätze nach Lade-ID. Für diese Gesamtanzahl der geladenen Datensätze zeigt der Bericht, wie viele dieser Datensätze neue Identitäten oder neue Entitäten darstellten, und der Prozentsatz der jeweiligen Datensätze (neue Identitäten bzw. neu erstellte Entitäten) wird berechnet.

Statistik nach Ladevorgang innerhalb einer Datenquelle

Ladedatum
Zeigt das Datum an, an dem diese Datenquellendatei geladen wurde.

Lade-ID
Zeigt die vom System zugeordnete Lade-ID-Nummer an.

Datenquelle
Zeigt den Datenquellencode und die Datenquellenbeschreibung (getrennt durch einen Strich) der geladenen Datenquellendatei an.

Geladene UMF-Datensätze
Gibt die Gesamtanzahl der geladenen Identitätsdatensätze in dieser Datenquellendatei an.

Neue Identitäten
Gibt die Gesamtanzahl der in der geladenen Datendatei erkannten neuen Identitäten an. (Diese Zahl weist auf eine Identität hin, die das System noch nicht verarbeitet hat.)

Neue Identität %
Gibt den Prozentsatz der Gesamtanzahl geladener Datensätze an (neue Identitäten geteilt durch geladene UMF-Datensätze), die neue Identitäten darstellen.

Neue Entitäten
Gibt die Gesamtanzahl der neuen Entitäten an, die aus diesem Datenladevorgang erstellt wurden.

Neue Entitäten %
Gibt den Prozentsatz der Gesamtanzahl geladener Datensätze an (neue Entitäten geteilt durch geladene Datensätze), die neue Entitäten darstellen.

Statistikdiagramme nach Datenquelle

Geladene Datensätze nach Datenquelle
Zeigt ein Balkendiagramm an, in dem die Anzahl der von jeder Datenquelle in das System geladenen Datensätze gemäß den anderen angegebenen Berichtskriterien grafisch dargestellt wird. Sie sehen, welche Datenquellen

die meisten Datensätze oder die wenigsten Datensätze beigesteuert haben, und Sie können dieses Ergebnis mit Ihren geschätzten Ladezahlen vergleichen.

- Die vertikale Achse zeigt die Datenquellen nach Datenquellencode an.
- Die horizontale Achse zeigt die Anzahl der geladenen Datensätze.

Werden für eine bestimmte Datenquelle weniger Datensätze als erwartet geladen, können Sie die Datendateien für diese Datenquelle überprüfen. (Sie könnten auch einen Ladeergebnisbericht ausführen, um die Datenqualität der Dateien anzuzeigen, die für diese Datenquelle geladen wurden. Die Datenqualität wirkt sich unmittelbar auf die Anzahl der geladenen Datensätze aus.)

Neue Entitäten nach Datenquelle
Zeigt ein Balkendiagramm an, in dem grafisch dargestellt wird, welche Datenquellen die größte Anzahl neuer Entitäten gemäß den anderen angegebenen Berichtskriterien geliefert haben.

- Die vertikale Achse zeigt die Datenquellen nach Datenquellencode an.
- Die horizontale Achse zeigt die Anzahl der neu erstellten Entitäten.

Laden - Ergebnisbericht

Der Ladeergebnisbericht fasst Statistiken und Qualitätsmerkmale nach Datenquelle zusammen. Er enthält Informationen zu den Datenquellendateien. Mit diesem Bericht können Sie Statistikdaten zur Ladeleistung, die Anzahl der von diesem Ladevorgang erstellten Entitäten und Alerts, allgemeine Informationen zur Datenqualität der geladenen Daten, eine Zusammenfassung der Aktionen bezüglich der UMF-Datensätze nach Ladevorgang und alle von dem Ladevorgang generierten UMF-Ausnahmenbedingungen ermitteln. Der Bericht ist nach Lade-ID sortiert.

Der Bericht unterteilt die Statistikdaten für jeden Ladevorgang in verschiedene Abschnitte:

- Ladezusammenfassung
- Rollenalertzusammenfassung
- Beziehungszusammenfassung
- Qualitätszusammenfassung
- UMF-Dokumentzusammenfassung
- Zusammenfassung der Ausnahmebedingung

Ladezusammenfassung

Mit diesem Abschnitt können Sie feststellen, wie lange die Verarbeitung einer bestimmten Datei gedauert hat, und er gibt Ihnen eine allgemeine Vorstellung von der Brauchbarkeit dieser Datenquellendatei für die Entitätsauflösung und Erkennung von Beziehungen insgesamt.

Startdatum und -zeit
Gibt das Anfangsdatum und die Anfangszeit des Datenladevorgangs an.

Abschlussdatum und -zeit
Gibt das Enddatum und die Endzeit des Datenquellendateiladevorgangs an.

Anzahl UMF-Datensätze
Gibt die Gesamtanzahl der Datensätze an, die im Zeitraum zwischen **Startdatum und -zeit** und **Abschlussdatum und -zeit** aus dieser Datenquellendatei geladen wurden.

Die Differenz zwischen **Abschlussdatum und -zeit** und **Startdatum und -zeit** gibt die Minuten an, die zum Laden dieser Datenquellendatei benötigt wurden. Dieser Wert kann Ihnen eine Vorstellung von der Systemleistung geben. Außerdem kann er anzeigen, dass eine große Datenquellendatei zur schnelleren Verarbeitung in kleinere Dateien aufgeteilt werden muss.

Neue Identitäten
Gibt die Gesamtanzahl neuer Identitäten an, die im Zeitraum zwischen **Startdatum und -zeit** und **Abschlussdatum und -zeit** geladen wurden.

Neue Identität %
Gibt den Prozentsatz der Gesamtanzahl der Identitäten in diesem Datenladevorgang an, die (für die Entitätendatenbank) neue Identitäten sind.

Neue Entitäten
Gibt die Gesamtanzahl der Entitäten an, die im Zeitraum zwischen **Startdatum und -zeit** und **Abschlussdatum und -zeit** neu erstellt wurden.

Neue Entitäten %
Gibt den Prozentsatz der Gesamtzahl der Entitäten an, die als Ergebnis dieses Datenquellenladevorgangs neu erstellte Entitäten sind.

Die Anzahl der neuen Identitäten und der neuen Entitäten kann Ihnen eine allgemeine Vorstellung von der Brauchbarkeit dieser Datenquelle für die Entitätsauflösung und Erkennung von Beziehungen insgesamt geben. Bleiben diese Werte über einen Zeitraum hinweg niedrig, könnte dies bedeuten, dass diese Datenquelle für die Ziele Ihres Unternehmens in Bezug auf die Entitätsauflösung nicht geeignet ist.

Rollenalertzusammenfassung

In diesem Abschnitt sehen Sie die Auflösungsregeln und die Auflösungsbewertungen, die den erkannten Beziehungen gemein sind, die zu Rollenalerts führten. Jede Zeile stellt die Anzahl der generierten Rollenalerts auf der Basis der aufgelisteten Kriterien dar.

Auflösungsregel
Zeigt den Namen der Auflösungsregel an, die verwendet wird, um die Identität und die Entität während der Entitätsauflösung und der Beziehungserkennung auszuwerten.

Alertbeschreibung
Zeigt den Namen der Rollenalertregel an, die den Rollenalert auslöste.

Wertigkeit
Zeigt einen benutzerdefinierten Anzeiger zur Messung der Priorität oder Bedeutung dieses Rollenalerts an.

Auflösungsbewertung
Zeigt eine Beziehungsbewertung (0 - 100) für die Auflösungsregel an, die der Identität und der Entität in diesem Rollenalert zugeordnet wird. Diese Bewertung zeigt den Grad der Ähnlichkeit zwischen der Identität und der Entität an. Eine Bewertung von 100 bedeutet, dass der Identitätsdatensatz in die Entität aufgelöst wurde.

Alertanzahl
Gibt die Gesamtanzahl der Rollenalerts an, die gemäß der Beschreibung der Rollenalertregel, der Auflösungsregel und der Auflösungsbewertung generiert wurden.

Beziehungszusammenfassung

In diesem Abschnitt sehen Sie die Attribute, die den erkannten Beziehungen gemein sind, die keinen Rollenalert generierten. Jede Zeile stellt die Anzahl der erkannten Beziehungen auf der Basis der aufgelisteten Kriterien dar.

Auflösungsregel
Zeigt den Namen der Auflösungsregel an, die verwendet wird, um die eingehenden Identitätsdatensätze und die vorhandenen Entitäten während der Entitätsauflösung und der Beziehungserkennung auszuwerten.

Auflösungsbewertung
Zeigt eine Auflösungsbewertung (0 - 100) für die Auflösungsregel an, die der Identität und der Entität während der Entitätsauflösung zugeordnet wird. Diese Bewertung zeigt den Grad der Ähnlichkeit zwischen der Identität und der Entität an. Eine Bewertung von 100 bedeutet, dass der Identitätsdatensatz in die Entität aufgelöst wurde.

Beziehungsbewertung
Zeigt eine Beziehungsbewertung (0 - 100) für die Auflösungsregel an, die der Identität und der Entität während der Beziehungsauflösung zugeordnet wird. Diese Bewertung zeigt den Grad der Beziehung zwischen der Identität und der Entität an.

Je höher die Beziehungsbewertung, umso enger ist die Beziehung zwischen der Identität und der Entität (auf der Basis der übereinstimmenden Attribute).

Beziehungsanzahl
Gibt die Gesamtanzahl der Beziehungen an, die auf der Basis der Auflösungsregel, der Auflösungsbewertung und der Beziehungsbewertung erkannt werden.

Qualitätszusammenfassung

Mit den Informationen in diesem Abschnitt können Sie die Qualität der Daten in jeder Datenquellendatei bewerten. Der Abschnitt zeigt die Qualität nach Attributtyp innerhalb eines UMF-Segments und UMF-Dokumenttyps an. Anhand der Qualitätszusammenfassung und der Zusammenfassung der UMF-Ausnahmebedingungen können Sie erkennen, bei welchen Datenquellendateien Qualitätsprobleme oder UMF-Fehler vorliegen, die behoben werden müssen. Normalerweise können Sie diese Probleme durch ETL oder DQM/Datenquellenkonfiguration vor Verarbeitung der Datenquellendatei lösen.

In einigen Fällen kann dieser Abschnitt zeigen, dass die Qualität einer Datenquelle so schlecht ist, dass Sie diese Datenquelle nicht für die Entitätsauflösung verwenden wollen.

Dokumenttyp
Zeigt den Namen des UMF-Dokumenttyps an, der den in **Datentyp** aufgeführten Datentyp enthält. In der Regel lautet dieser Wert UMF_ENTITY.

Tabellenname
Zeigt den Namen der Datenbanktabelle an, in der die Daten aus UMF-Segmenten mit ähnlichem Namen gespeichert werden. Daten aus dem Segment NUMBER werden beispielsweise in der Tabelle NUMS gespeichert.

Datentyp
Gibt den Datentyp an, wie in den UMF-Tags für den Attributtyp der eingehenden Datensätze aufgelistet. Dieser Typ entspricht einem in **Tabellenna-**

me aufgeführten UMF-Segment. Lautet der Tabellenname beispielsweise *ADDRESS* und der aufgeführte Datentyp *H*, werten die Qualitätsinformationen den Adresstyp *Home* aus.

Wenn Sie einen Datentyp nicht erkennen, kann dies bedeuten, dass die Datenquellendatei der entsprechenden Kombination aus UMF-Dokumenten, -Segmenten und -Tags nicht ordnungsgemäß zugeordnet ist. Überprüfen Sie den Abschnitt mit der Zusammenfassung der Ausnahmebedingungen, um festzustellen, ob Segmentausnahmebedingungen durch übereinstimmende UMF-Segmente und -Tags verursacht wurden. Wird das Problem durch ein ungültiges UMF verursacht, stimmen die Zahlen für **Zähler für schlechte Qualität** im Abschnitt mit der Qualitätszusammenfassung und für **Anzahl Segmentausnahmebedingungen** im Abschnitt mit den UMF-Ausnahmebedingungen häufig überein.

Datensatzanzahl
Gibt die Gesamtzahl der eingehenden Identitätsdatensätze für den Dokumenttyp, den Tabellennamen und den Datentyp an.

Generische Anzahl
Gibt die Gesamtzahl der eingehenden Identitätsdatensätze mit dem angegebenen Dokumenttyp, Tabellennamen und Datentyp an, die Werte enthalten, die als generisch betrachtet werden.

Zähler für schlechte Qualität
Gibt die Gesamtzahl der eingehenden Identitätsdatensätze mit dem angegebenen Dokumenttyp, Tabellennamen und Datentyp an, deren Qualität als schlecht betrachtet wird. Dieser Wert kann auf einen Datenerfassungs- oder ETL-Umsetzungsfehler in der Datenquellendatei hinweisen.

Verwendbar %
Gibt den Prozentsatz der eingehenden Identitätsdatensätze mit dem angegebenen Dokumenttyp, Tabellennamen (dieses UMF-Segments) und Datentyp an, die für die Entitätsauflösung und das Erkennen von Beziehungen verwendet werden können. ('Datensatzanzahl' minus 'Generische Anzahl' minus 'Zähler für schlechte Qualität') geteilt durch 'Datensatzanzahl' ist gleich 'Verwendbar %'.

Identität (%)
Gibt den Prozentsatz der eingehenden Identitätsdatensätze an, die den Dokumenttyp, Tabellennamen und Datentyp enthielten.

Attributzusammenfassung

In diesem Abschnitt sehen Sie die Attribute in der Datenquellendatei, die bei der Erkennung von Beziehungen und der Generierung von Rollenalerts beteiligt waren. Jedes Attribut ist einem bestimmten UMF-Segment zugeordnet und dieser Abschnitt zeigt die Anzahl der erkannten Beziehungen und der generierten Rollenalerts auf der Basis der Daten im eingehenden UMF-Segment.

Segmentname
Zeigt den Namen des UMF-Segments an, das unmittelbar einem Attribut zugeordnet ist.

Datentyp
Zeigt den Attributtyp (oder Datentyp) innerhalb des UMF-Segments, der der Genauigkeitsbeschreibung entspricht. Der Bericht könnte einen bestimmten Attributtyp oder *ALL* auflisten. *ALL* steht für alle Attributtypen im UMF-Segment.

Genauigkeitsbeschreibung
Beschreibt den Übereinstimmungsschwellenwert zwischen einem Attribut aus einer eingehenden Identität und einem Attribut aus einer vorhandenen Entität.

Rollenalerts
Gibt die Gesamtanzahl der Rollenalerts an, die gemäß diesem UMF-Segment, Datentyp und dieser Genauigkeitsbeschreibung generiert wurden.

Beziehungen
Gibt die Gesamtanzahl der Beziehungen an, die gemäß diesem UMF-Segment, Datentyp und dieser Genauigkeitsbeschreibung erkannt wurden.

UMF-Dokumentzusammenfassung

Sie können in diesem Abschnitt die Gesamtanzahl der eingehenden Datensätze in einer Datenquellendatei prüfen. Als Basis dient die Aktion, die für den Datensatz ausgeführt werden soll. Sie können diese Zahlen mit der Datensatzanzahl im Abschnitt mit der Ladezusammenfassung abgleichen.

Dokumenttyp
Zeigt den Namen des UMF-Eingangsdokumenttyps an. In der Regel lautet dieser Wert UMF_ENTITY.

Aktion
Gibt den Typ der Aktion für den eingehenden Identitätsdatensatz an. Nachfolgend finden Sie eine Liste der am häufigsten verwendeten Aktionen:

- *A* für Hinzufügen (Add)
- *C* für Ändern (Change)
- *D* für Löschen (Delete)

Als Teil des ETL-Prozesses verwenden Identitätsdatensätze in der Regel UMF-Tagging, um anzuzeigen, wie bei dem jeweiligen eingehenden Datensatz während der Systemverarbeitung verfahren werden soll.

Anzahl UMF-Datensätze
Gibt die Gesamtanzahl der für jeden Aktionstyp innerhalb des Dokumenttyps verarbeiteten Datensätze an.

Prozent
Gibt den Prozentsatz der Gesamtanzahl geladener Datensätze an, die die Datensatzanzahl darstellt. (Die Summe darf 100 % nicht überschreiten.)

Zusammenfassung der Ausnahmebedingung

Diese Informationen helfen beim Identifizieren von fehlerhaften Identitätsdatensätzen, z. B. Datensätzen mit UMF-Fehlern. Die Ausnahmebedingung beschreibt den Fehler und der Tabellenname und das Element zeigen, welches Segment und welcher Datensatz fehlerhaft sind. Die Anzahl zeigt, wie viele der Datensätze in der Datei diesen UMF-Fehler enthielten.

Dokumenttyp
Zeigt den Namen des UMF-Eingangsdokumenttyps an. In der Regel lautet dieser Wert UMF_ENTITY.

Aktion
Gibt den Typ der Aktion für den eingehenden Identitätsdatensatz an:

- *A* für Hinzufügen (Add)

- *C* für Ändern (Change)
- *D* für Löschen (Delete)

Als Teil des ETL-Prozesses verwenden Identitätsdatensätze in der Regel UMF-Tagging, um anzuzeigen, wie bei dem jeweiligen eingehenden Datensatz während der Systemverarbeitung verfahren werden soll.

Segment
Zeigt den Namen des UMF-Segments an, in dem die Ausnahmebedingung aufgetreten ist.

UMF-Tag
Zeigt den Wert des UMF-Tags an, der die UMF-Ausnahmebedingung verursacht hat.

Ausnahmebedingung
Zeigt die Nachrichten-ID oder einen anderen Ausnahmecode an, die bzw. der den Typ der aufgetretenen UMF-Ausnahmebedingung angibt und Informationen zur Behebung der Ausnahmebedingung liefert. Diese Informationen befinden sich auch in der Tabelle UMF_EXCEPT.

Anzahl Segmentausnahmebedingungen
Gibt die Gesamtanzahl der UMF-Ausnahmebedingungen dieses Typs an.

Überprüfen Sie den Zähler für schlechte Qualität im Abschnitt mit der Qualitätszusammenfassung, um festzustellen, ob ein entsprechender Datentyp mit schlechter oder unbrauchbarer Qualität gemeldet ist. Wird das Problem durch UMF-Fehler verursacht, stimmen die Zahlen bei **Zähler für schlechte Qualität** im Abschnitt mit der Qualitätszusammenfassung und bei **Anzahl Segmentausnahmebedingungen** im Abschnitt mit den UMF-Ausnahmebedingungen für dasselbe UMF-Segment und dieselben UMF-Tags häufig überein.

Ausführen des Konfigurationsberichts

Der Konfigurationsbericht enthält eine einheitliche Übersicht aller Systemeinstellungen, die Sie mithilfe der Konfigurationskonsole konfigurieren können. Wenn Sie ein Konfigurationsproblem lösen oder unterschiedliche Konfigurationseinstellungen vergleichen, zeigen Sie diesen Bericht an, um die aktuellen Produktkonfigurationseinstellungen zu sehen, bevor Sie die aktuelle Systemkonfiguration ändern.

Vorgehensweise

1. Klicken Sie in der Konfigurationskonsole **Konfiguration** > **Berichte** an.
2. Wählen Sie in **Berichte** den Eintrag **Konfigurationsbericht** aus.
3. Klicken Sie **Bericht ausführen** an.

Ergebnisse

Das Produkt generiert den ausgewählten statistischen Bericht auf der Basis aller angegebenen Kriterien und zeigt den Bericht in einem separaten Web-Browser-Fenster für BIRT Report Viewer an. Wenn es keine aufzulistenden Daten gibt, werden im BIRT Report Viewer-Fenster abhängig von den von Ihnen ausgewählten Kriterien der Name des Berichts, Datum und Uhrzeit der Berichtsgenerierung und oben im Fenster **Seite 1/1** angezeigt. Der Datenabschnitt ist leer.

Konfigurationsbericht

Der Konfigurationsbericht enthält eine einheitliche Sicht der Systemeinstellungen, die Sie mithilfe der Konfigurationskonsole konfigurieren. Mit diesem Bericht können Sie die aktuelle Systemkonfiguration anzeigen oder drucken, bevor Sie die Sys-

temkonfiguration ändern, wenn Sie einen Konfigurationsfehler beheben oder wenn Sie verschiedene Konfigurationseinstellungen vergleichen.

In dem Bericht sind die aktuellen Konfigurationseinstellungen nach Kategorie aufgelistet:

Datenquellen
Konfigurationseinstellungen für Datenquellen anzeigen. Hierzu gehören die ID und der Code für Datenquelle, der der Datenquelle zugeordnete Rollencode, die der Datenquelle zugeordnete Entitätsauflösungskonfiguration und der aktuelle Status des Datenquellencodes (aktiv oder inaktiv).

Wählen Sie **Konfiguration** > **Quellen** > **Datenquellen** aus, um Datenquellen zu konfigurieren.

Nummerntypen
Konfigurationseinstellungen für Nummerntypen anzeigen. Hierzu gehören die Nummerntypen-ID, der Nummerntyp, die Mindestlänge und die maximale Länge des Nummerntyps, alle dem Nummerntyp zugeordneten Masken, Informationen darüber, wie der Nummerntyp in der Entitätsauflösung verwendet wird und ob der Nummerntyp aktiv oder inaktiv ist.

Wählen Sie **Konfiguration** > **Quellen** > **Nummern** aus, um Nummerntypen zu konfigurieren.

Merkmaltypen
Konfigurationseinstellungen für Merkmaltypen anzeigen. Hierzu gehören die Merkmaltyp-ID, der Name des Merkmaltyps, der dem Merkmal zugeordnete Datentyp (z. B. Zeichen oder Datum), Informationen darüber, wie der Merkmaltyp in der Entitätsauflösung verwendet wird und ob der Merkmaltyp aktiv oder inaktiv ist.

Wählen Sie **Konfiguration** > **Quellen** > **Merkmale** aus, um Merkmaltypen zu konfigurieren.

Plug-in
Konfigurationseinstellungen für die Attribut- und Bewertungsanpassung anzeigen. Hierzu gehören die Plug-in-ID, der Name, der Typ, die Version sowie der Kurzname für die Bibliothek.

Wählen Sie **Konfiguration** > **Allgemein** > **Plug-ins** aus, um die Plug-ins für die Attribut- und Bewertungsanpassung zu konfigurieren.

Ereignistypen
Konfigurationseinstellungen für Ereignistypen anzeigen. Hierzu gehört die Maßeinheit, die dem Wert für dieses Ereignis zugeordnet ist. Ereignistypen sind Teil des Ereignismanagers.

Wählen Sie **Konfiguration** > **Quellen** > **Ereignistypen** aus, um Ereignistypen zu konfigurieren.

Regeln für das Datenqualitätsmanagement
Die Liste der Regeln für das Datenqualitätsmanagement (DQM-Regeln) und die zugehörigen Parameter anzeigen, die für einen bestimmten UMF-Tag in einem UMF-Segment konfiguriert sind. Hierzu gehören die Angabe, welchem UMF-Segment und UMF-Tagnamen die DQM-Regel zugeordnet ist, die Reihenfolge, in der die DQM-Regel in diesem UMF-Segment und -Tag verwendet wird, zugeordnete Parameter für die DQM-Regel in diesem UMF-Segment und -Tag, ob die DQM-Regel eingehende Daten für dieses UMF-Segment und diesen UMF-Tag korrigiert und ob die DQM-Regel in diesem UMF-Segment und -Tag aktiviert ist.

Wählen Sie **Konfiguration** > **UMF** > **DQM-Regeln** aus, um ein UMF-Segment und einen UMF-Tag für die Verwendung von DQM-Regeln zu konfigurieren.

Zuordnung laden
Die Konfigurationsdaten für die Zuordnung der UMF-Daten in die entsprechenden Tabellen und Tabellenspalten in der Entitätendatenbank anzeigen. Hierzu gehören der UMF-Segmentname, der UMF-Datenpfad, der Name der Entitätendatenbanktabelle, der Feldname und -typ in dieser Entitätendatenbanktabelle, der Datentyp dieses Felds und die Angabe, ob die Zuordnung aktiviert ist.

Wählen Sie **Konfiguration** > **UMF** > **Datenzuordnung** aus, um Daten aus einem UMF-Segment einer Tabelle in der Entitätendatenbank zuzuordnen.

Entitätsauflösungsregeln
Die Konfigurationseinstellungen für jede Entitätsauflösungsregel anzeigen. Hierzu gehören die ID der Entitätsauflösungsregel, die Reihenfolge der Regel, die Mindestauflösungsbewertung und die Beziehungsbewertung für die Regel und die Angabe, ob die Regel Zurückweisungen enthält.

Wählen Sie **Konfiguration** > **Auflösung** > **Auflösungsregeln** aus, um Entitätsauflösungsregeln zu konfigurieren.

Bestätigung/Zurückweisung der Entitätsauflösung
Die Einstellungen der Bewertungen anzeigen, die den Bestätigungs- und Zurückweisungsprozess der Entitätsauflösung beeinflussen. Hierzu gehören die zugeordnete Entitätsauflösungs-ID und Konfigurations-ID, die Priorität jeder Bewertung, die Beschreibung und der Attributname jeder Bewertung sowie der numerische Wert der Bewertung.

Wählen Sie **Konfiguration** > **Auflösung** > **Bestätigungen und Zurückweisungen** aus, um Einstellungen für Entitätsauflösungsbestätigungen und -zurückweisungen zu konfigurieren.

Entitätsauflösungsmerkmale
Die Einstellungen für Merkmaltypen anzeigen, die für die während der Entitätsauflösung verwendeten Bestätigungs- und Zurückweisungsgewichtungen konfiguriert wurden. Hierzu gehören die Priorität, die Bestätigungsgewichtung und die Zurückweisungsgewichtung.

Wählen Sie **Konfiguration** > **Auflösung** > **Merkmale** aus, um Bestätigungs- und Zurückweisungsgewichtungen für Merkmaltypen zu konfigurieren.

Rollencodes
Die Liste der konfigurierten Rollencodes und die zugehörigen Einstellungen anzeigen. Hierzu gehören die ID und die Beschreibung des Rollencodes, die Rollencodeklasse und der aktuelle Status des Rollencodes (aktiv oder inaktiv).

Wählen Sie **Konfiguration** > **Beziehungen** > **Rollen** aus, um Rollencodes zu konfigurieren.

Rollenalertregeln
Die Liste der konfigurierten Rollenalertregeln und die zugehörigen Einstellungen anzeigen. Hierzu gehören die ID und Beschreibung der Rollenalertregel, Wertigkeit, Mindestgrenzwert für Alerts und die Rollencode-IDs der beiden Rollen, die diese Rollenalertregel auslösen.

Wählen Sie **Konfiguration** > **Beziehungen** > **Rollenalertregeln** aus, um Rollenalertregeln zu konfigurieren.

Name Manager-Konfiguration
Die konfigurierten Einstellungen für die Komponente Name Manager anzeigen, die die Namensgenauigkeit während der Entitätsauflösung erweitert.

Wählen Sie **Konfiguration** > **Auflösung** > **Name Manager-Abgleichkonfiguration** aus, um die Einstellungen für Name Manager zu konfigurieren.

Abgrenzungskonfiguration
Die konfigurierten Einstellungen für die Komponente Degrees of Separation der Pipeline anzeigen, die Beziehungen mit einem, zwei oder mehr Abgrenzungsgraden erkennen kann.

Wählen Sie **Konfiguration** > **Beziehungen** > **Abgrenzungskonfiguration** aus, um die Einstellungen für Abgrenzungsgrade zu konfigurieren.

Systemreihenfolgen
Die Konfigurationseinstellungen für Reihenfolgennummern anzeigen, die angeben, wie das System Daten lädt und verarbeitet. Die Systemreihenfolgennummern verringern die Systembelastung auf zwei Arten. Erstens, weil sie jeder Pipeline ermöglichen, eine Abfrage abzusetzen, die eine sequenzielle Nummernreihe abruft, und diese Nummern dann im Cache gespeichert werden, bis sie verbraucht sind. Und zweitens, weil die Reihenfolgennummern verhindern, dass mehrere Pipelines, die vom System generierte IDs erstellen, dieselbe ID-Nummer für mehrere Datensätze verwenden.

Jedes Mal, wenn die Pipeline beispielsweise eine neue Entität während der Entitätsauflösungsverarbeitung erstellt, generiert das System eine eindeutige Entitäts-ID. Mit Systemreihenfolgen kann die Pipeline eine Abfrage senden, um die nächsten 1000 verfügbaren Entitäts-ID-Nummern anzufordern. So kann die Pipeline für die nächsten 1000 neu erstellten Entitäten die verfügbaren in ihrem Speicher gespeicherten Entitäts-ID-Nummern verwenden. Die alternative (langsamere) Methode ist, dass jede Pipeline für jede neu erstellte Entität eine Abfrage an die Entitätendatenbank sendet und eine neue Entitäts-ID anfordert.

Wählen Sie **Konfiguration** > **UMF** > **Ladefolge** aus, um Systemreihenfolgen zu konfigurieren.

Schwellenwerte für generische Daten
Die nach Attribut konfigurierten Einstellungen der Schwellenwerte für generische Daten anzeigen. Hierzu gehören Attributname, Attributtyp und die Zahl für den Schwellenwert, die festlegt, wann ein bestimmter Wert für dieses Attribut generisch wird.

Wählen Sie **Konfiguration** > **UMF** > **Schwellenwert für generische Daten** aus, um generische Schwellenwerte nach Attributtyp zu konfigurieren.

Tabellenverzeichnis
Die Verzeichniseinstellungen nach Entitätendatenbanktabelle anzeigen. Hierzu gehören Tabellenname, Beschreibung und der Tabellentyp.

Wählen Sie **Konfiguration** > **UMF** > **Wörterverzeichnis** aus, um das Tabellenverzeichnis zu konfigurieren.

Referenztabellen
Die Einstellungen für die Liste der Tabellen anzeigen, die das System als Referenztabellen während der Verarbeitung verwendet. Hierzu gehören der

Tabellenname, der Schlüsselfeldname, der ID-Feldname und die Angabe, ob die Tabelle während der Verarbeitung in den Speicher geladen werden soll.

Wählen Sie **Konfiguration** > **UMF** > **Suchfunktion** aus, um anzugeben, welche Tabellen das System als Referenztabellen verwendet.

Übereinstimmende Konfiguration
Die Einstellungen für jede Auflösungskonfiguration anzeigen, die in Ihrem System konfiguriert ist. Hierzu gehören der Konfigurationsname und die Konfigurations-ID, der Übereinstimmungstyp und der Name des UMF-Segments.

Wählen Sie **Konfiguration** > **Auflösung** > **Kandidatenerstellungsregel** aus, um übereinstimmende Konfigurationen zu konfigurieren.

Dokumenttypen
Die Einstellungen für UMF-Eingabedokumente anzeigen. Hierzu gehören der Dokumenttyp, die Angabe, ob für diesen Dokumenttyp Datenqualitätsmanagement ausgeführt werden soll, ob die durch diesen Dokumenttyp verarbeiteten Daten in die Entitätsauflösungsdatenbank geladen werden sollen sowie die Entitätsauflösungsebene, die für diesen Typ des UMF-Eingabedokuments ausgeführt werden soll.

Wählen Sie **Konfiguration** > **UMF** > **Eingabedokumente** aus, um UMF-Eingabedokumente zu konfigurieren.

UMF-Ausgabeformat
Die Formateinstellungen für UMF-Ausgabedokumente anzeigen. Hierzu gehören Format-ID und Formatcode, die Weiterleitungsrichtung und die Angabe, ob die Einstellung des Ausgabeformats aktiviert ist.

Wählen Sie **Konfiguration** > **UMF** > **Ausgabedokumente** aus, um Formate für UMF-Ausgabedokumente zu konfigurieren.

GEM-Ereignistypen
Die Formateinstellungen für Ereignismanagerereignisse anzeigen. Hierzu gehören die Ereignis-ID, der Typ, die Beschreibung, die Kategorie, die Maßeinheit sowie das Erstellungsdatum und die Erstellungzeit.

Wählen Sie **Konfiguration** > **Quellen** > **Ereignistyp** aus, um Ereignistypen zu konfigurieren.

Systemparameter
Die Liste der Systemparametereinstellungen nach Parametergruppe anzeigen. Hierzu gehören der Wert und der Standardwert des Systemparameters sowie der Gültigkeitstyp und -wert des Parameters.

Wählen Sie **Konfiguration** > **Allgemein** > **Systemparameter** aus, um Systemparameter zu konfigurieren.

Anwendungsaktivitätscodes
Die Liste der für Visualizer konfigurierten Aktivitätscodes nach Aktivitätstyp (Rollenalert, Attributalert oder Ereignisalert) anzeigen. Hierzu gehören der Aktivitätscode, gültige Statuswerte für den Aktivitätscode und die Angabe, ob der Aktivitätscode aktiv oder inaktiv ist.

Wählen Sie **Konfiguration** > **Visualizer** > **Aktivitätscodes** aus, um Aktivitätscodes zu konfigurieren, die in Visualizer verwendet werden.

Benutzergruppen
Die Einstellungen der für Visualizer konfigurierten Benutzergruppen anzeigen. Hierzu gehören die zugeordneten Visualizer-Benutzernamen, das Er-

stellungsdatum und die Erstellungszeit für die Benutzergruppe und die Angabe, ob die Benutzergruppe aktiv oder inaktiv ist.

Wählen Sie **Konfiguration** > **Visualizer** > **Codes** und dann **ANALYZER-_GROUP** aus, um Aktivitätscodes zu konfigurieren, die in Visualizer verwendet werden.

Rollenalertgruppen
Die Einstellungen für konfigurierte Rollenalertgruppen anzeigen. Hierzu gehören die zugeordnete Anwendungsgruppe, die zugeordnete Rollenalertregel-ID und -beschreibung, das Erstellungsdatum und die Erstellungszeit für die Rollenalertgruppe und die Angabe, ob die Rollenalertgruppe aktiv oder inaktiv ist.

Wählen Sie **Konfiguration** > **Beziehungen** > **Rollenalertregeln** aus und bearbeiten Sie dann das Feld **Alertgruppe**, um Rollenalertgruppen zu konfigurieren, die in Visualizer verwendet werden.

Benutzer
Die Einstellungen für die Benutzer anzeigen, die für die Anmeldung an Visualizer konfiguriert sind. Hierzu gehören Benutzeranmeldenamen, die Angabe, ob der Visualizer-Benutzer mithilfe von Berechtigungsnachweisen der Entitätendatenbank authentifiziert werden soll und ob der Visualizer-Benutzer aktiv oder inaktiv ist.

Wählen Sie **Konfiguration** > **Visualizer** > **Visualizer-Benutzer** aus, um die Benutzer zu konfigurieren.

Exportieren von Berichten

BIRT Report Viewer bietet Ihnen die Möglichkeit, die Daten des Konfigurationskonsolenberichts in andere Anwendungen wie Microsoft Excel, Microsoft PowerPoint, Microsoft Word oder Adobe Acrobat zu exportieren. Sie können den gesamten Bericht oder bestimmte Daten aus einem Bericht exportieren.

Exportieren von Konfigurationskonsolenberichten

Wenn Sie einen Bericht vollständig (Daten und Format) in eine andere Anwendung, beispielsweise in Microsoft PowerPoint, oder in ein anderes Format, beispielsweise als Adobe Acrobat-PDF exportieren wollen, verwenden Sie die Option **Berichte exportieren** in BIRT Report Viewer. Der Export ganzer Berichte funktioniert gut bei Berichten, die mehrere Seiten umfassen, und in Fällen, in denen Sie die Daten nach dem Export nicht bearbeiten wollen.

Informationen zu diesem Vorgang

Für einen in eine mit Microsoft Word bearbeitbare DOC-Datei exportierten Konfigurationskonsolenbericht ist Microsoft Word Version 2003 oder höher erforderlich.

Wenn Sie kleine Änderungen am exportierten Bericht vornehmen oder diesem etwas hinzufügen wollen, exportieren Sie den Bericht in Microsoft Word oder Microsoft Excel. Diese Anwendungen behalten die Berichtsformatierung bei, die Daten werden jedoch in der Regel in Spalten oder Tabellen angezeigt, wodurch die Daten in gewissem Umfang bearbeitet werden können. Da der exportierte Bericht eine schreibgeschützte Datei ist, müssen Sie die Datei unter einem neuen Namen speichern, um Ihre Änderungen zu sichern.

Vorgehensweise

1. Klicken Sie nach dem Generieren des Berichts **Bericht exportieren** im BIRT Report Viewer-Fenster an. Das Symbol **Bericht exportieren** ist das vierte Symbol links neben der BIRT Report Viewer-Symbolleiste.
2. Wählen Sie in **Bericht exportieren** das Format oder die Anwendung aus, mit dem bzw. in die Sie die Daten exportieren wollen:
   - **PDF**
   - **PowerPoint**
   - **Word**
   - **PostScript**
   - **Excel**
3. Wählen Sie die Seiten oder den Seitenbereich für den Export aus.
4. Optional: Wählen Sie die Größe des resultierenden Berichts aus: Diese Option ist nur verfügbar, wenn Sie die Option **PDF**, **PowerPoint** oder **PostScript** ausgewählt haben.
   - **Automatisch**: Jede Seite des Berichts wird als separate Seite exportiert.
   - **Tatsächliche Größe**: Alle Seiten des Berichts werden in eine einzige lange Seite eingefügt.
   - **Auf Seitengröße anpassen**: Alle Seiten des Berichts werden verkleinert, damit sie ungefähr auf ein Drittel einer einzelnen Seite passen. Wenn Sie die Option **PowerPoint** ausgewählt haben, wird der Bericht als Bild in die Seite eingefügt, sodass Sie die Größe des Bilds ändern können.
5. Klicken Sie **OK** an.

Ergebnisse

Wenn Sie den Bericht im PDF- oder PostScript-Format exportiert haben, wird die resultierende Datei in der Regel in den Ordner gestellt, in den die Dateien auf dem Client heruntergeladen werden. Beispiel: C:\Dokumente und Einstellungen\Administrator\Eigene Dateien\Downloads.

Wenn Sie die Daten in PowerPoint, Word oder Excel exportiert haben, werden sie in eine schreibgeschützte Datei exportiert, die in der Regel den Namen *berichtsname.erweiterung_für_ausgewählte_anwendung* erhält.

- *berichtsname* ist der Name des von Ihnen exportierten Konfigurationskonsolenberichts.
- *erweiterung_für_ausgewählte_anwendung* ist die für die ausgewählte Anwendung geeignete Dateiformaterweiterung.

Wenn Sie beispielsweise den Bericht **Laden - Ergebnisbericht** in Word exportiert haben, erhält die Datei in der Regel den Namen `Laden - Ergebnisbericht.doc`. Ein Dialog wird angezeigt, in dem Sie wählen können, ob Sie die Datei in der ausgewählten Anwendung öffnen oder sie speichern wollen.

Exportieren von Daten aus den Konfigurationskonsolenberichten

Wenn Sie Berichtsdaten in eine CSV-Datei (Comma Separated Values) exportieren wollen, um die Daten in einer anderen Anwendung wie Microsoft Excel anzuzeigen und zu bearbeiten, verwenden Sie die Option **Daten exportieren** in BIRT Report Viewer. Sie können einen Abschnitt des Berichts, die zu exportierenden Felder und das Exportdatenformat auswählen.

Informationen zu diesem Vorgang

BIRT Report Viewer exportiert jeweils einen Datenabschnitt eines Berichts, d. h., die Anzeigefunktion erstellt für jeden Abschnitt im Bericht eine separate Ergebnismenge. Die exportierten Daten sind Rohdaten ohne Formatierung.

Wenn Sie den gesamten Bericht exportieren wollen, verwenden Sie stattdessen die Option **Bericht exportieren**. Diese Exportoption exportiert jedoch sowohl die Daten als auch die Berichtsformatierung. Aus diesem Grund können Sie die Daten nach dem Export nicht mehr bearbeiten.

Vorgehensweise

1. Klicken Sie nach dem Generieren des Berichts in BIRT Report Viewer das Symbol **Daten exportieren** an. Das Symbol **Daten exportieren** ist das dritte Symbol von links auf der BIRT Report Viewer-Symbolleiste.
2. Erforderlich: Wählen Sie in **Verfügbare Ergebnismengen** des Bereichs **Daten exportieren** den Berichtsabschnitt aus, den Sie exportieren wollen. Die Namen der Berichtsabschnitte werden nach Element angezeigt, beispielsweise ELEMENT_2041. Sie sehen in der Regel an den in der Liste der verfügbaren Spalten aufgeführten Spaltennamen, welchen Abschnitt Sie gerade auswählen.
3. Erforderlich: Wählen Sie die zu exportierenden Spalten in der Liste der verfügbaren Spalten aus. Die Spaltennamen, die für den in der Liste der ausgewählten Berichtsgruppen ausgewählten Berichtsabschnitt gelten, sind in der Liste der ausgewählten Spalten aufgeführt. Möglicherweise wollen Sie die Daten nicht in allen für diesen Berichtsabschnitt verfügbaren Spalten anzeigen.
4. Optional: Legen Sie die Reihenfolge der Spalten in der Liste der ausgewählten Spalten fest. Mit dieser Option können Sie die Daten nach Spalte neu ordnen, bevor Sie sie exportieren.
5. Optional: Wählen Sie in **Trennzeichen** ein Trennzeichen aus, wenn Sie das Standardtrennzeichen, ein **Komma**, nicht verwenden wollen:
   - **Semikolon**
   - **Doppelpunkt**
   - **Vertikale Linie**
   - **Tabulatortaste**
6. Klicken Sie **OK** an. Wählen Sie im angezeigten Dialog aus, ob Sie die exportierten Daten öffnen oder die Datei speichern wollen. Die Datei wird standardmäßig in Microsoft Excel geöffnet. Sie können jedoch auch eine beliebige andere Anwendung auswählen, vorausgesetzt, diese kann eine CSV-Datei exportieren.

Ergebnisse

Die Daten werden in eine Datei exportiert, die in der Regel den Name *berichtsname*.csv erhält. Dabei ist *berichtsname* der Name des Konfigurationskonsolenberichts, aus dem Sie die Daten exportiert haben.

Verwalten von Visualizer

Zur effektiven Verwendung von Visualizer müssen Sie die Browser konfigurieren, Konten für die entsprechenden Benutzer einrichten und den Zugriff auf Visualizer verwalten.

Visualizer

Visualizer ist eine grafische Benutzerschnittstelle, die Analysten und Prüfer zum Analysieren der Ergebnisse von Alerts, Beziehungen und Entitätsauflösungen verwenden.

Visualizer wird von einer integrierten Version von IBM WebSphere Application Server gehostet. Sie konfigurieren Visualizer über die Konfigurationskonsole und die Auswahl **Benutzervorgaben** im Menü **Datei** von Visualizer.

Visualizer-Benutzer können verschiedene Analysetasks ausführen:

Ausführen von Analysen und Dispositionen für Alerts
Von der Entitätsauflösungsverarbeitung generierte Alerts stellen Beziehungs- und Entitätsauflösungen dar, die für ein Unternehmen von Interesse sind. In der Regel überprüfen Analysten Alerts und entscheiden auf Grundlage der Alertinformationen, welche Maßnahme ergriffen werden soll oder dass keine Maßnahme erforderlich ist. Es gibt die folgenden drei Alerttypen: Rollenalerts, Attributalerts und Ereignisalerts.

Visualizer zeigt die Alerts an und stellt Analysten Textsichten und grafisch orientierte Sichten der Alerts und der an den Alerts beteiligten Entitäten bereit. Analysten können die Details abrufen und anschließend den Dispositionsstatus des Alerts entsprechend festlegen.

Erstellen und Verwalten von Attributalertgeneratoren
Mit Visualizer können Analysten über die Komponente 'Attributalertgenerator' persistente Suchen erstellen und verwalten sowie die Anzeige und den Emfpang von Attributalerts verwalten. Analysten können Attributalertgeneratoren basierend auf Attributdaten erstellen, um Identitäten zu suchen, die basierend auf diesen Attributdaten in Entitäten aufgelöst wurden. Analysten können auch einen Attributalertgenerator erstellen, um eine persistente Suche nach einer bestimmten Entität in der Entitätendatenbank durchzuführen.

Suchen von Entitäten
Visualizer-Benutzer können auch nach verschiedenen Methoden Entitäten für die weitere Analyse suchen:

- Nach Attributen
- Nach Datenquellenbenutzerkonto
- Nach Entitäts-ID
- Nach Auflösung (wie stark das eingegebene Kriterium mit den Identitäten und Entitäten in der Entitätendatenbank basierend auf den Schwellenwerten für die Mindestauflösungsbewertung übereinstimmt)

Hinzufügen von Entitäten und offengelegten Beziehungen
Mit Visualizer können Analysten Datensätze für Entitätsauflösung und Beziehungserkennung hinzufügen. Sie können einen einzelnen Identitätsdatensatz hinzufügen oder eine UMF-Datei laden, die Tausende von Identitätsdatensätzen enthält. Wie beim Hinzufügen von Identitäten durch Übernahmeprogramme werden durch Visualizer hinzugefügte Datensätze von einer Pipeline für Entitätsauflösung und Beziehungserkennung verarbeitet. Die Verarbeitungsergebnisse werden in die Entitätendatenbank geschrieben und Alerts werden in Visualizer veröffentlicht.

Analysten können auch Beziehungen zwischen Entitäten (nach Identität) offenlegen, wenn sie eine Verknüpfung zwischen den Identitäten kennen. Offengelegte Beziehungen sind beispielsweise das Zuordnen von Entitäten

zu einander auf der Grundlage von Kontaktdaten für den Notfall oder von in einer Bewerbung aufgelisteten Referenzen. Diese Beziehungen wurden von der Entität in der Anwendung offengelegt.

Generieren und Drucken von Berichten
Visualizer enthält auch mehrere Berichte, die Analysten anzeigen und drucken können, damit sie ihre Arbeit mit Visualizer einfacher verwalten und überwachen können.

Benutzerrollen und -zuständigkeiten

Benutzerrollen helfen beim Kategorisieren der typischen Tasks, die abgeschlossen werden müssen, um IBM InfoSphere Identity Insight effektiv bereitstellen und verwenden zu können. Möglicherweise verwenden viele verschiedene Typen von Benutzern IBM InfoSphere Identity Insight für verschiedene Zwecke, d. h., Benutzer sind bei der Verwendung des Produkts für die Aufgaben mindestens einer Rolle zuständig.

Sie können basierend auf den verschiedenen Benutzerrollen und -zuständigkeiten Benutzergruppen definieren.

Die folgenden Rollen zählen zu den gängigsten Benutzerrollen:

Analyst
Analysiert die Daten und prüft Entitäten, Beziehungen und Alerts. Der Analyst definiert, welche Ergebnisse die nützlichsten sind, und stellt sicher, dass das System diese Ergebnisse zurückgibt. Der Analyst arbeitet eng mit dem Bediener und dem Anwendungsadministrator zusammen.

Bediener
Lädt Daten in das System, führt die Pipelines aus, prüft, dass das System ordnungsgemäß ausgeführt wird, und stellt bei Bedarf Berichte zur Qualität bei Ladevorgängen bereit. Der Bediener prüft auch die Ergebnisse, Ausnahmebedingungen und Ereignisse. Der Bediener arbeitet eng mit dem Analysten, dem Datenquellenadministrator und dem Anwendungsadministrator zusammen.

Datenquellenadministrator
Bereitet die Daten zum Laden in das System vor. Hierzu gehört das Konvertieren der Daten in eine UMF-Datei und das Prüfen dieser Datei. Der Datenquellenadministrator arbeitet eng mit den Bedienern, den Anwendungsadministratoren und den Datenbankadministratoren zusammen.

Anwendungsadministrator
Konfiguriert die Anwendung. Hierzu gehört die Konfiguration der Daten, des Entitätsmodells und der Regeln. Der Anwendungsadministrator arbeitet eng mit den Datenquellenadministratoren und den Bedienern zusammen, um das Entitätsmodell zu definieren, und koordiniert Konfigurationsänderungen mit dem Datenbankadministrator, dem Datenquellenadministrator und den Bedienern. Der Anwendungsadministrator koordiniert die Tätigkeit der für das Gesamtsystem verantwortlichen Administratoren (falls vorhanden) und berät sich mit diesen.

Datenbankadministrator
Stellt sicher, dass die Datenbank zur Verwendung mit der Anwendung entsprechend konfiguriert und optimiert ist. Der Datenbankadministrator arbeitet eng mit dem Bediener, dem Datenquellenadministrator und dem Anwendungsadministrator zusammen.

Systemarchitekt
Plant die Bereitstellung der Anwendung durch Schätzen der Hardware- und Softwareanforderungen. Der Systemarchitekt arbeitet eng mit dem Installationsverantwortlichen, dem Datenbankadministrator, dem Datenquellenadministrator und dem Anwendungsadministrator zusammen, um sicherzustellen, dass die Bereitstellung die Vision, Strategien und Zielsetzungen erfüllt und in Ihre Geschäftsprozesse integriert werden kann, sodass die erwarteten Ergebnisse erzielt werden.

Installationsverantwortlicher
Verwaltet die Installation und Erstkonfiguration der Anwendung. Der Installationsverantwortliche konfiguriert Erstbenutzer im System. Häufig arbeitet IBM Professional Services mit dem Systemarchitekten zusammen, um diese Aufgaben durchzuführen.

Programmierer
Entwirft und entwickelt grafische Oberflächen oder passt grafische Oberflächen für die verschiedenen Funktionen an, sodass die Bereitstellung der Anwendung nahtlos in Ihre Umgebung integriert werden kann. Der Programmierer arbeitet eng mit dem Systemarchitekten und dem Anwendungsadministrator zusammen, häufig, um Alerts auf die für Ihre Umgebung effektivste Art an die entsprechenden Benutzer zu verteilen.

Sicherheitsarchitekt
Stellt sicher, dass das Projektteam die Sicherheitsvorgaben einhält und ein sicheres System implementiert. Der Sicherheitsarchitekt arbeitet eng mit dem Systemarchitekten, dem Installationsverantwortlichen und dem Datenbankadministrator zusammen.

Optimale Browsereinstellungen für die Verwendung von Visualizer

Visualizer ist eine Java-basierte Anwendung, auf die Sie über das Internet zugreifen. Die Leistung dieser Anwendung kann mit bestimmten Einstellungen für den Browser, mit dem Sie auf Visualizer zugreifen, optimiert werden.

Verwenden Sie die folgenden Browsereinstellungen, um Visualizer optimal anzuzeigen:

Tabelle 28. Optimale Browsereinstellungen für Visualizer

Einstellung	Wert	Beschreibung
Textgröße	Mittel	
JavaScript	Ein	
Cookies	Ein	Zumindest Sitzungscookies der aktuellen Webseite müssen aktiviert sein.
Sicherheit - Vertrauenswürdige Website	HTTP-Adresse für Visualizer	Stellen Sie sicher, dass sich die HTTP-Adresse für Visualizer in der Liste der vertrauenswürdigen Internet-Websites befindet.
Sicherheit - Downloadoptionen	Aktiviert	Stellen Sie sicher, dass alle Downloadoptionen für vertrauenswürdige Internet-Websites aktiviert sind.

Popup-Blocker	Popups von der HTTP-Adresse für Visualizer zulassen	Stellen Sie sicher, dass sich die HTTP-Adresse für Visualizer in der Liste der Websites befindet, für die Popups zulässig sind.

Anmelden an Visualizer

Sie müssen über ein Visualizer-Benutzerkonto (Benutzername und Kennwort) verfügen, bevor Sie sich an Visualizer anmelden. Ihr Systemadministrator kann Ihnen die Informationen zu Ihrem Visualizer-Benutzerkonto bereitstellen.

Vorgehensweise

1. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie das Visualizer-Symbol auf Ihrer Arbeitsoberfläche doppelt an.
   - Oder öffnen Sie Ihren Internet-Browser und geben Sie die URL (Uniform Resource Locator) für Visualizer in die Adresszeile ein.

   Die URL zum Starten von Visualizer lautet:

   `http://server:installationsport`

   Beispiel: `http://localhost:13510`. Wenn Visualizer installiert ist, ist der *installationsport* standardmäßig 13510, die Portnummer kann jedoch geändert werden. Setzen Sie sich mit Ihrem Systemadministrator in Verbindung, wenn Sie sich bezüglich des richtigen Servernamens oder der richtigen Portnummer nicht sicher sind.
2. Melden Sie sich an, indem Sie Ihren Benutzernamen und Ihr Kennwort eingeben.

   Anmerkung: Bei den Feldern für den Benutzernamen und das Kennwort muss die Groß-/Kleinschreibung beachtet werden. Verwenden Sie bei Ihrer ersten Anmeldung das Kennwort, das Ihnen Ihr Systemadministrator zugewiesen hat. Nach der ersten erfolgreichen Anmeldung ändern Sie normalerweise Ihr Visualizer-Kennwort, um die Sicherheit Ihres Visualizer-Benutzerkontos zu wahren.
3. Klicken Sie **Anmelden** an.

Schließen von Visualizer

Wenn Sie Ihre Arbeit mit Visualizer beendet haben, schließen Sie die Anwendung. Beim Schließen von Visualizer melden Sie sich gleichzeitig ab. Wenn Sie ein Pause machen und Ihre Workstation lediglich für einige Minuten sichern wollen, können Sie Visualizer auch sperren.

Vorgehensweise

Gehen Sie wie folgt vor, um Visualizer zu schließen und sich abzumelden:

- Wählen Sie **Datei** > **Beenden** aus.
- Oder drücken Sie **Strg** + **Q**.

Verwalten des Zugriffs auf Visualizer

Visualizer-Benutzer müssen über ein registriertes Konto verfügen, bevor sie sich an Visualizer anmelden können. Diese Benutzerkonten sind nicht mit den Benutzerkonten für die Konfigurationskonsole identisch, sondern sie sind speziell für die Verwendung von Visualizer berechtigt.

Erstellen neuer Visualizer-Benutzer

Damit ein Benutzer auf Visualizer zugreifen und Visualizer verwenden kann, muss ein Systemadministrator in der Konfigurationskonsole ein Visualizer-Benutzerkonto für den Benutzer erstellen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Visualizer** an.
3. Klicken Sie die Registerkarte **Visualizer-Benutzer** an.
4. Klicken Sie die Schaltfläche **Neu** an.
5. Wählen Sie in der Dropdown-Liste **Datenbankanmeldung** einen der folgenden Werte aus:
   - Wählen Sie **Ja** aus, wenn der Benutzer über ein Benutzerkonto verfügt, das ihm den Zugriff auf die Entitätendatenbank gestattet, und wenn Sie diese Datenbankanmeldeinformationen verwenden wollen.
   - Wählen Sie **Nein** aus, wenn Sie die Anmeldeinformationen in der Standarddatei verwenden wollen. Bei dieser Auswahl wählt ein Systemadministrator das erste Kennwort aus, mit dem sich der Benutzer an Visualizer anmeldet. Und ein Systemadministrator kann die Kennwörter von Visualizer-Benutzern bei Bedarf zurücksetzen.
6. Geben Sie in das Feld **Benutzername** den Benutzernamen ein, der hinzugefügt werden soll. Wenn Sie **Ja** in der Dropdown-Liste **Datenbankanmeldung** ausgewählt haben, muss dieser Benutzername dem Namen für diesen Benutzer in der Entitätendatenbank entsprechen.
7. Für das Feld **Kennwort** gilt Folgendes:
   a. Wenn Sie **Ja** in der Dropdown-Liste **Datenbankanmeldung** ausgewählt haben, muss dieser Wert dem Kennwort entsprechen, das in den Anmeldeinformationen für die Datenbank gespeichert ist.
   b. Wenn Sie **Nein** in der Dropdown-Liste **Datenbankanmeldung** ausgewählt haben, geben Sie das Anfangskennwort für den Benutzer ein.

      Anmerkung: Fordern Sie aus Sicherheitsgründen Ihre Visualizer-Benutzer auf, das Anfangskennwort zu ändern, nachdem sie sich zum ersten Mal erfolgreich angemeldet haben.
8. Optional: Wählen Sie in der Dropdown-Liste des Felds **Gruppe** die Analysegruppe aus, der dieser Benutzer angehört.
9. Klicken Sie die Schaltfläche **Speichern** an.

Nächste Schritte

Der Benutzer kann diesen Benutzernamen und dieses Kennwort sofort verwenden, um sich an Visualizer anzumelden.

Inaktivieren von Visualizer-Benutzern

Für Benutzer, die keinen Zugriff mehr auf Visualizer benötigen, können Sie Visualizer-Benutzerkonten inaktivieren.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Visualizer** an.
3. Klicken Sie die Registerkarte **Visualizer-Benutzer** an.

4. Klicken Sie den Benutzernamen an, dessen Benutzerkonto Sie inaktivieren wollen.
5. Wählen Sie in der Dropdown-Liste **Status** den Eintrag **Inaktiv** aus.
6. Klicken Sie die Schaltfläche **Speichern** an.

Ergebnisse

Der von Ihnen inaktivierte Benutzer kann sich nicht mehr an Visualizer anmelden.

Zurücksetzen von Visualizer-Kennwörtern

Wenn Visualizer-Benutzer ihr Kennwort vergessen haben und ihre Anmeldeinformationen über die Konfigurationskonsole und nicht über die Anmeldeoption der zugrunde liegenden Datenbank konfiguriert wurden, können Sie ihr Kennwort in der Konfigurationskonsole zurücksetzen. Andernfalls müssen Sie ihr Kennwort mit der Anmeldekonfiguration der zugrunde liegenden Datenbank zurücksetzen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Visualizer** an.
3. Klicken Sie die Registerkarte **Visualizer-Benutzer** an.
4. Klicken Sie den Benutzernamen des Benutzers an, dessen Kennwort Sie bearbeiten wollen.
5. Geben Sie in das Feld **Kennwort** ein neues Kennwort für den Benutzer ein.

   Anmerkung: Fordern Sie aus Sicherheitsgründen die Benutzer auf, ihr Kennwort zu ändern, nachdem sie sich zum ersten Mal erfolgreich angemeldet haben, sodass es nur noch ihnen bekannt ist.
6. Klicken Sie die Schaltfläche **Speichern** an.

Nächste Schritte

Der Benutzer kann dieses neue Kennwort unverzüglich zum Anmelden an Visualizer verwenden. Fordern Sie die Benutzer nach dem Zurücksetzen von Kennwörtern aus Sicherheitsgründen auf, ihr Kennwort zu ändern, nachdem sie sich erfolgreich angemeldet haben.

Erstellen von Gruppen von Visualizer-Benutzern

In Visualizer sind Alerts Gruppen von Analysten zugeordnet. Wenn Sie einem Projekt eine neue Gruppe von Analysten hinzufügen, können Sie die neue Analystengruppe mithilfe der Konfigurationskonsole erstellen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Codes** an.
4. Klicken Sie in der Dropdown-Liste **Typ** den Eintrag **ANALYZER_GROUP** an.
5. Klicken Sie die Schaltfläche **Neu** an.
6. Geben Sie in das Feld **Code** den Namen der Analystengruppe ein.
7. Wählen Sie **Aktiv** in der Dropdown-Liste **Status** aus.
8. Klicken Sie die Schaltfläche **Speichern** an.

Hilfethemen

Visualizer-Benutzer - Registerkarte 'Allgemein':

Über diese Registerkarte können Sie neue Visualizer-Benutzer hinzufügen oder vorhandene Benutzerkennwörter ändern.

Datenbankanmeldung
Wählen Sie eine Option aus, um anzugeben, ob die Anmeldeinformationen der zugrunde liegenden Entitätendatenbank (Benutzername und Kennwort) für den Visualizer-Zugriff verwendet werden sollen.

- Ja - Verwenden Sie diese Einstellung nur, wenn dieser Visualizer-Benutzer bereits über ein Benutzerkonto verfügt, mit dem der Benutzer auf die Entitätendatenbank zugreifen kann. Verwenden Sie bei der Auswahl dieser Option den Benutzernamen und das Kennwort für die Anmeldung an der Entitätendatenbank als Visualizer-Benutzernamen und -Kennwort. (Wenn diese Informationen nicht übereinstimmen, kann sich der Visualizer-Benutzer nicht anmelden.)
- Nein - Die auf dieser Registerkarte eingegebenen Anmeldeinformationen werden verwendet.

Benutzername
Geben Sie den Benutzernamen für diesen Visualizer-Benutzer ein. Wenn dieser Benutzer eine Datenbankanmeldung verwendet, muss dieser Benutzername mit dem entsprechenden Benutzernamen für die Entitätendatenbank übereinstimmen.

Kennwort
Geben Sie das neue Kennwort für diesen Visualizer-Benutzer ein. Wenn dieser Benutzer eine Datenbankanmeldung verwendet, muss dieses Kennwort genau mit dem entsprechenden Datenbankkennwort übereinstimmen.

Gruppe
Wählen Sie die Visualizer-Gruppe aus, zu der dieser Benutzer gehört. Die Visualizer-Gruppe legt fest, welche Alerts und Benachrichtigungen dem Benutzer im Visualizer-Fenster **Alertzusammenfassung** angezeigt werden. (Wenn es in Ihrem Unternehmen beispielsweise eine Visualizer-Gruppe "Sicherheit" und eine Gruppe "Reservierung" gibt, können den Benutzern in den jeweiligen Gruppen unterschiedliche Alerttypen in Visualizer angezeigt werden.).

Status Wählen Sie einen Status aus, um anzugeben, ob dieser Visualizer-Benutzer zurzeit aktiv ist (d. h., ob er sich an Visualizer anmelden kann).

Konfigurieren von Aktivitätscodes für Visualizer

Visualizer stellt verschiedene Standardaktivitätscodes für die Behandlung von Alerts bereit. Über die Konfigurationskonsole können Sie neue Aktivitätscodes hinzufügen und vorhandene Aktivitätscodes löschen.

Erstellen von Aktivitätscodes für Suchen

Visualizer stellt Aktivitätscodes für Suchergebnisalerts bereit. Wenn Sie zusätzliche Aktivitäten in Bezug auf die Alerthandhabung protokollieren müssen, können Sie mithilfe der Konfigurationskonsole neue Aktivitätscodes hinzufügen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Visualizer** an.

3. Klicken Sie die Registerkarte **Aktivitätscodes** an.
4. Klicken Sie **SUCHE** in der Dropdown-Liste **Aktivitätstyp** an.
5. Klicken Sie die Schaltfläche **Neu** an.
6. Geben Sie in das Feld **Aktivitätscode** den Namen des Aktivitätscodes ein.
7. Wählen Sie in der Dropdown-Liste **Aktivitätenstatuscode** den intern anerkannten Aktivitätenstatuscode aus, dem der neue Aktivitätscode entspricht.
8. Wählen Sie **Aktiv** in der Dropdown-Liste **Status** aus.
9. Klicken Sie die Schaltfläche **Speichern** an.

Löschen von Aktivitätscodes für Suchen

Visualizer stellt Aktivitätscodes für Suchergebnisalerts bereit. Wenn Sie Aktivitätscodes in Bezug auf die Alerthandhabung löschen müssen, können Sie mithilfe der Konfigurationskonsole vorhandene Aktivitätscodes löschen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Visualizer** an.
3. Klicken Sie die Registerkarte **Aktivitätscodes** an.
4. Klicken Sie **SUCHE** in der Dropdown-Liste **Aktivitätstyp** an.
5. Wählen Sie das Kontrollkästchen neben dem Aktivitätscode aus, den Sie löschen wollen.
6. Klicken Sie die Schaltfläche **Löschen** an. Ein Bestätigungsfenster wird geöffnet.
7. Klicken Sie **OK** an.

Erstellen von Aktivitätscodes für Rollenalerts

Visualizer stellt Aktivitätscodes für Rollenalerts bereit. Wenn Sie zusätzliche Aktivitäten in Bezug auf die Alerthandhabung protokollieren müssen, können Sie mithilfe der Konfigurationskonsole neue Aktivitätscodes hinzufügen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Visualizer** an.
3. Klicken Sie die Registerkarte **Aktivitätscodes** an.
4. Klicken Sie **CONFLICT** in der Dropdown-Liste **Aktivitätstyp** an.
5. Klicken Sie die Schaltfläche **Neu** an.
6. Geben Sie in das Feld **Aktivitätscode** den Namen des Aktivitätscodes ein.
7. Wählen Sie in der Dropdown-Liste **Aktivitätenstatuscode** den intern anerkannten Aktivitätenstatuscode aus, dem der neue Aktivitätscode entspricht.
8. Wählen Sie **Aktiv** in der Dropdown-Liste **Status** aus.
9. Klicken Sie die Schaltfläche **Speichern** an.

Löschen von Aktivitätscodes für Rollenalerts

Visualizer stellt Aktivitätscodes für Rollenalerts bereit. Wenn Sie Aktivitätscodes in Bezug auf die Alerthandhabung löschen müssen, können Sie mithilfe der Konfigurationskonsole vorhandene Aktivitätscodes löschen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Visualizer** an.
3. Klicken Sie die Registerkarte **Aktivitätscodes** an.

4. Klicken Sie **CONFLICT** in der Dropdown-Liste **Aktivitätstyp** an.
5. Wählen Sie das Kontrollkästchen neben dem Aktivitätscode aus, den Sie löschen wollen.
6. Klicken Sie die Schaltfläche **Löschen** an. Ein Bestätigungsfenster wird geöffnet.
7. Klicken Sie **OK** an.

Erstellen von Aktivitätscodes für Ereignisalerts

Visualizer stellt Aktivitätscodes für Ereignisalerts bereit, die über die Ereignisverarbeitung generiert werden, wenn in Ihrem System der Ereignismanager aktiviert ist. Mithilfe von Codes für Ereignisalerts können Sie zusätzliche Aktivitäten in Bezug auf die Handhabung von Ereignisalerts protokollieren. Das System stellt drei vordefinierte Codes für Ereignisalerts bereit, über die Konfigurationskonsole können Sie jedoch auch neue Aktivitätscodes für Ereignisalerts hinzufügen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Visualizer** an.
3. Klicken Sie die Registerkarte **Aktivitätscodes** an.
4. Wählen Sie **EVENT** in der Dropdown-Liste **Aktivitätstyp** aus.
5. Klicken Sie die Schaltfläche **Neu** an.
6. Geben Sie in das Feld **Aktivitätscode** einen eindeutigen Namen für den neuen Aktivitätscode ein.
7. Wählen Sie in der Dropdown-Liste **Aktivitätenstatuscode** den intern anerkannten Aktivitätenstatuscode aus, dem der neue Aktivitätscode entspricht.
8. Wählen Sie **Aktiv** in der Dropdown-Liste **Status** aus, damit dieser Aktivitätscode zur Verwendung in Visualizer verfügbar ist.
9. Klicken Sie die Schaltfläche **Speichern** an.

Vordefinierte Aktivitätscodes für Ereignisalerts:

Aktivitätscodes für Ereignisse werden von Analysten in Visualizer verwendet, um die Disposition von Ereignisalerts festzulegen. Das System stellt drei vordefinierte Aktivitätscodes für Ereignisse bereit.

Die vordefinierte Gruppe von Aktivitätscodes für Ereignisalerts stellt die folgenden Aktivitätscodes für Ereignisalerts bereit:

ASSIGNED
: Wenn Analysten sich selbst oder einer anderen Analystengruppe einen Ereignisalert zuordnen, wird das System standardmäßig auf den Aktivitätscode ASSIGNED gesetzt.

CLOSED
: Wenn Analysten einen Ereignisalert schließen, wird das System standardmäßig auf den Aktivitätscode CLOSED gesetzt.

PENDING
: Bevor ein Analyst die Disposition von Ereignisalerts festlegt, ordnet das System ihnen automatisch die Aktivität PENDING zu. Das bedeutet, dass der Ereignisalert für alle Analysten in der zugeordneten Gruppe zur Überprüfung oder Disposition offen ist.

Bearbeiten von vordefinierten Aktivitätscodes für Ereignisalerts

Sie können vorhandene Aktivitätscodes bearbeiten, die zum Festlegen der Disposition von Ereignisalerts in Visualizer verwendet werden. Sie können einen vorhan-

denen Aktivitätscode nicht umbenennen, aber Sie können seine zugehörige Beschreibung, seinen Aktivitätsstatuscode oder seinen Status ändern.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Visualizer** an.
3. Klicken Sie die Registerkarte **Aktivitätscodes** an.
4. Wählen Sie **EVENT** in der Dropdown-Liste **Aktivitätstyp** aus.
5. Klicken Sie den Aktivitätscode an, den Sie bearbeiten wollen.
6. Nehmen Sie auf der Registerkarte **Aktivitätscodes - Allgemein** Ihre Änderungen vor. Wenn Sie beispielsweise einen Aktivitätscode konfigurieren wollen, dieser aber nicht zur Auswahl in Visualizer angezeigt werden soll, wählen Sie den Status **Inaktiv** aus. Auf diese Weise müssen Sie den Aktivitätscode nicht löschen, falls Sie ihn später aktivieren wollen.
7. Klicken Sie die Schaltfläche **OK** an.

Löschen von Aktivitätscodes für Ereignisalerts

Visualizer stellt Aktivitätscodes für Dispositionsereignisalerts bereit. Wenn Sie Aktivitätscodes in Bezug auf die Handhabung von Ereignisalerts löschen müssen, können Sie mithilfe der Konfigurationskonsole vorhandene Aktivitätscodes löschen, einschließlich der vordefinierten Aktivitätscodes für Ereignisalerts. Wenn die Aktivitätscodes gelöscht werden, können sie in Visualizer nicht mehr zur Handhabung von Ereignisalerts verwendet werden.

Informationen zu diesem Vorgang

Wenn Sie die Informationen für den Aktivitätscode nur ändern wollen, können Sie den Aktivitätscode bearbeiten, ohne ihn zu löschen und erneut zu erstellen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Visualizer** an.
3. Klicken Sie die Registerkarte **Aktivitätscodes** an.
4. Wählen Sie **EVENT** in der Dropdown-Liste **Aktivitätstyp** aus.
5. Wählen Sie das Kontrollkästchen neben den Aktivitätscodes aus, die Sie löschen wollen.
6. Klicken Sie die Schaltfläche **Löschen** an. Ein Bestätigungsfenster wird geöffnet.
7. Klicken Sie die Schaltfläche **OK** an.

Visualizer-Aktivitätscodes - Registerkarte 'Allgemein'

Aktivitätscodes werden von Analysten in Visualizer verwendet, um die Disposition von Rollenalerts, Ereignisalerts und Suchen festzulegen.

Aktivitätstyp
Wird vom System ausgefüllt. Wählen Sie den Aktivitätstyp aus, um Aktivitätscodes anzuzeigen, hinzuzufügen oder zu löschen:

- **CONFLICT** wird für Rollenalerts verwendet
- **EVENT** wird für Ereignisalerts verwendet
- **SEARCH** wird für Visualizer-Suchen verwendet

Aktivitätscode
Geben Sie den eindeutigen Namen für diesen Aktivitätscode ein.

Beschreibung
Geben Sie eine Beschreibung dieses Aktivitätscodes ein.

Aktivitätenstatuscode
Wählen Sie den internen Statuscode aus, dem dieser Benutzeraktivitätscode entspricht:

- **Offen**
- **Zugeordnet**
- **Geschlossen**
- **Gefiltert**

Status Gibt an, ob dieser Aktivitätscode zurzeit aktiv ist. Sie können beispielsweise einen Aktivitätscode konfigurieren, bevor Sie den Code in Visualizer implementieren, indem Sie den Aktivitätscode inaktivieren. Unmittelbar vor der Implementierung des Aktivitätscodes können Sie ihn dann bearbeiten und aktivieren.

Verwalten der Systemkonfigurationseinstellungen

Die Systemkonfiguration kann über die folgenden Prozesse modifiziert werden:

Kapitel 5. Konfigurieren des Systems für Daten

Damit IBM InfoSphere Identity Insight effektiv genutzt werden kann, müssen Sie die Entitätendatenbank, die Entitätsauflösung und die Systemparameter konfigurieren.

Konfigurieren von Daten im System

Bevor Sie IBM InfoSphere Identity Insight verwenden, müssen Sie zunächst die Entitätendatenbank für die Verwendung Ihrer Quellendaten konfigurieren.

Konfigurieren von Merkmaltypen

Sie können Merkmaltypen für Daten konfigurieren, die nicht als Namens-, Zahlen-, Adress- oder E-Mail-Adresstyp klassifiziert werden können. Wenn einer Datenquelle neue Daten hinzugefügt werden und Sie die Daten als einen Merkmaltyp klassifizieren wollen, der nicht bereits im System konfiguriert ist, müssen Sie einen neuen Merkmaltyp für die neuen Daten erstellen.

Merkmale

Merkmale sind benutzerdefinierte Eigenschaften, die einer Identität zugeordnet sind und die in der Regel nicht als Name, Nummer, Adresse oder E-Mail-Adresse ausgedrückt werden.

Dieses Attribut ermöglicht Benutzern, das Produkt zu erweitern, indem sie anpassbare Entitätsattribute definieren, die für ihre Datenquellen aussagekräftig sind.

Merkmaltypen:

Merkmaltypen organisieren die in der Entitätendatenbank gespeicherten Daten und geben diese Daten an. Das Geburtsdatum und Geschlecht sind Beispiele für Standardmerkmaltypen, die bereits in der Entitätendatenbank konfiguriert sind.

Wenn Sie über Daten verfügen, die nicht durch einen Standardmerkmaltyp definiert sind, müssen Sie für diese Daten einen neuen Merkmaltyp erstellen.

Beispiel

Second National Banker's Trust hat seinen Kundentypen kürzlich eine neue Datenkategorie hinzugefügt. Die Daten kommen mithilfe dieser UMF-Tags zum Übernahmeknoten:

```
<attribute>
  <attr_type>cust_type</attr_type>
  <attr_value>merchant</attr_value>
</attribute>
```

In diesem Fall müssen Sie einen neuen Merkmaltyp namens 'cust_type' konfigurieren.

Vom System erstellte Merkmaltypen:

Wenn eine UMF-Nachricht mit einem nicht konfigurierten Merkmaltyp verarbeitet wird, erstellt das System automatisch einen neuen Merkmaltyp.

Der Wert der UMF-Nachricht wird mithilfe des neu erstellten Merkmaltyps in der Datenbank erfasst und es wird eine UMF-Ausnahmebedingung geschrieben.

Wenn das System automatisch ein neues Merkmal erstellt, führt dies zu einem unvollständigen Datenbanksatz, der nur Folgendes enthält:

- Die neuen Typinformationen auf der Basis der UMF-Nachricht
- Einen Statuswert `Vom System erstellt`

Anzeigen von Merkmaltypen

Merkmaltypen werden für Daten verwendet, die nicht als Namens-, Zahlen-, Address- oder E-Mail-Adresstyp klassifiziert werden können. Möglicherweise wollen Sie vorhandene Merkmaltypen anzeigen, wenn Sie darüber nachdenken, einen neuen Merkmaltyp hinzuzufügen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Registerkarte **Merkmale** an.
4. Wählen Sie den Merkmaltyp aus, den Sie anzeigen wollen.

Erstellen eines Merkmaltyps

Merkmale von Entitäten werden im System nach Typ verwaltet.

Vorbereitende Schritte

Bevor Sie einen neuen Merkmaltyp erstellen, sollten Sie die eingehenden Merkmaldaten prüfen, um festzustellen, ob sie mit einem der vorhandenen Merkmaltypen beschrieben werden können.

Informationen zu diesem Vorgang

Um neue Merkmaldaten effektiv verwenden zu können, müssen Sie über die Konfigurationskonsole einen neuen Merkmaltyp konfigurieren. Wenn Sie einen neuen Merkmaltyp mit dem Datentypwert DATE erstellen, erhalten Sie die Möglichkeit, eine neue DQM-Regel zu erstellen, um den neuen Merkmaltyp auszuwerten.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Registerkarte **Merkmale** an.
4. Klicken Sie die Schaltfläche **Neu** an.
5. Geben Sie auf der Registerkarte **`Allgemein`** den Typ, die Beschreibung, den Datentyp, die Klasse, die Auflösungsverwendung, den Status und die Anzeigeebene für diesen Merkmaltyp an. Geben Sie zudem an, ob das Protokoll beibehalten werden soll.
6. Klicken Sie die Schaltfläche **Speichern** an. Wenn Sie einen neuen Merkmaltyp mit dem Datentypwert DATE und eine neue DQM-Regel erstellen, um den neuen Merkmaltyp zu validieren, wird die Seite zur Erstellung von DQM-Regeln angezeigt, auf der die Werte auf der Basis des neuen Merkmaltyps bereits ausgefüllt sind.

Ergebnisse

Das System kann nun Daten in einer UMF-Datei verarbeiten, die für <CHARACTERISTIC_TYPE> angegeben ist.

Löschen von Merkmaltypen

Sie können einen vorhandenen Merkmaltyp löschen, wenn er von der Entitätendatenbank nicht mehr verwendet wird.

Informationen zu diesem Vorgang

Wenn Sie eine DQM-Regel für den Merkmaltyp erstellt haben, empfiehlt es sich möglicherweise, auch diese DQM-Regel zu löschen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Registerkarte **Merkmale** an.
4. Wählen Sie das Kontrollkästchen neben dem Merkmaltyp aus, den Sie löschen wollen.
5. Klicken Sie die Schaltfläche **Löschen** an.

Hilfethemen

Merkmale - Registerkarte 'Allgemein':

Über die Registerkarte **Allgemein** können Sie die Details für den Merkmaltyp angeben.

Typ Geben Sie den Namen des Merkmaltyps ein, den Sie erstellen wollen.

Beschreibung
Geben Sie die Beschreibung des Merkmaltyps ein, den Sie erstellen wollen.

Datentyp
Wählen Sie in der Dropdown-Liste den Datentyp des Merkmaltyps aus, den Sie erstellen wollen.

CHAR
Wählen Sie diesen Feldtyp aus, um den Datentyp CHAR für den Merkmaltyp anzugeben.

CLOB Wählen Sie diesen Feldtyp aus, um den Datentyp CLOB für den Merkmaltyp anzugeben.

CLOB muss für Merkmaltypen verwendet werden, die aus großen Datenmengen bestehen.

Anmerkung: Wenn der Datentyp auf CLOB gesetzt ist, kann sich dies negativ auf die Leistung auswirken. Verwenden Sie nach Möglichkeit VARCHAR (LVARCHAR für Informix), um mögliche Leistungsprobleme zu reduzieren.

DATE Wählen Sie diesen Feldtyp aus, um den Datentyp DATE für den Merkmaltyp anzugeben.

`DQM-Regel erstellen`
Wenn Sie einen neuen Merkmaltyp mit dem Datentypwert DATE erstellen, erhalten Sie die Möglichkeit, eine neue DQM-

Regel zu erstellen, um den neuen Merkmaltyp auszuwerten. Sie werden zu der Seite für die Erstellung von DQM-Regeln umgeleitet, wo die Werte bereits auf der Basis des neuen Merkmaltyps angegeben sind.

VARCHAR
Wählen Sie diesen Feldtyp aus, um den Datentyp VARCHAR für den Merkmaltyp anzugeben.

Klasse Wählen Sie in der Dropdown-Liste die Klasse für den Merkmaltyp aus, den Sie erstellen wollen.

LC Wählen Sie diesen Feldtyp aus, um den Merkmaltyp als persönliche Daten zu definieren (LC - Life Characteristic) anzugeben.

Beispiel: Größe oder Gewicht.

SC Wählen Sie diesen Feldtyp aus, um den Merkmaltyp als Systemdaten zu definieren (SC - System Characteristic) anzugeben.

Beispiele: der bevorzugte Sitzplatz in einem Flugzeug oder der Saldo eines guten Kunden.

Auflösungsverwendung
Wählen Sie in der Dropdown-Liste aus, ob dieses Merkmal für die Entitätsauflösung verwendet werden soll.

Keine Wählen Sie diesen Feldtyp aus, um anzugeben, dass der Merkmalwert nicht für die Entitätsauflösung verwendet wird.

Bestätigen/Zurückweisen
Wählen Sie diesen Feldtyp aus, um anzugeben, dass der Merkmalwert für die Entitätsauflösung verwendet wird.

Kandidaten
Wählen Sie diesen Feldtyp aus, um anzugeben, dass der Merkmalwert zum Erstellen einer Kandidatenliste und zum Erhöhen der Bewertung eines Kandidaten verwendet wird.

Kandidaten/Keine Bewertung
Wählen Sie diesen Feldtyp aus, um anzugeben, dass der Merkmalwert zum Erstellen einer Kandidatenliste, jedoch nicht zum Erhöhen der Bewertung eines Kandidaten verwendet wird.

Status Wählen Sie in der Dropdown-Liste **Aktiv** aus, um anzugeben, dass dieses Merkmal aktiv ist. Wählen Sie andernfalls **Inaktiv** aus.

Protokoll beibehalten
Wählen Sie in der Dropdown-Liste **Ja** aus, um den Langzeitstatus des Merkmaltypwerts aufzuzeichnen. Diese Option sollte nur für Merkmaltypen verwendet werden, deren Werte sich nur selten ändern. Wählen Sie andernfalls **Nein** aus.

Anzeigeebene
Wählen Sie in der Dropdown-Liste aus, ob dieses Merkmal für Diagramme und Berichte verwendet werden soll.

Keine Wählen Sie diesen Feldtyp aus, um den Wert dieses Merkmaltyps bei Diagrammen und Berichten auszuschließen.

Alle Wählen Sie diesen Feldtyp aus, um den Wert dieses Merkmaltyps bei allen Diagrammen und Berichten einzuschließen.

Konfigurieren von Nummerntypen

Sie können Nummerntypen für Daten konfigurieren, die als Nummern klassifiziert werden können. Wenn einer Datenquelle neue Daten hinzugefügt werden und Sie die Daten als eine Nummer klassifizieren wollen, die noch nicht im System konfiguriert ist, müssen Sie einen neuen Nummerntyp für die neuen Daten erstellen.

Nummern

Nummern sind benutzerdefinierte Eigenschaften, die einer Identität zugeordnet sind, die als Nummer klassifiziert werden kann.

Nummerntypen

Nummerntypen organisieren die in der Entitätendatenbank gespeicherten und geben Nummerndaten und geben diese Daten an. Die Telefon- und Sozialversicherungsnummer sind Beispiele für Standardnummerntypen, die bereits in der Entitätendatenbank konfiguriert sind.

Wenn Sie über Nummerndaten verfügen, die nicht durch einen Standardnummerntyp definiert sind, müssen Sie für diese Daten einen neuen Nummerntyp erstellen.

Beispiel

Second National Banker's Trust verfügt über Daten, zu denen auch die Nummern von Kundengirokonten gehören, und will der Entitätendatenbank diese neuen Daten hinzufügen. Die Daten kommen mithilfe dieser UMF-Tags zum Übernahmeknoten:

```
<number>
  <num_type>ca</num_type>
  <num_value>41510155060</num_value>
</number>
```

In diesem Fall müssen Sie einen neuen Nummerntyp namens ca konfigurieren.

Anzeigen von Nummerntypen

Nummerntypen sind für Daten, die als Nummern klassifiziert werden können. Möglicherweise wollen Sie vorhandene Nummerntypen anzeigen, wenn Sie planen, einen neuen Nummerntyp hinzuzufügen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Registerkarte **Nummern** an.
4. Wählen Sie den Nummerntyp aus, den Sie anzeigen wollen.

Erstellen von Nummerntypen

Sie müssen einen neuen Nummerntyp erstellen, wenn neue Daten in einem Quellensystem hinzugefügt werden und Sie diese Daten als einen Nummerntyp klassifizieren wollen, der noch nicht konfiguriert ist.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Registerkarte **Nummern** an.
4. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie die Schaltfläche **Neu** an, um einen vollständig neuen Nummerntyp zu erstellen.
- Wählen Sie einen Nummerntyp in der Liste aus und klicken Sie anschließend die Schaltfläche **Klonen** an, um einen Nummerntyp auf der Basis eines vorhandenen Nummerntyps zu erstellen.

5. Geben Sie auf der Registerkarte **Allgemein** den Wert für Typ, Beschreibung, Klasse, Eindeutig, Auflösungsverwendung, Status, Protokoll beibehalten, Bestätigungsgewichtung für Ausstellungsort und Zurückweisungsgewichtung für Ausstellungsort sowie sonstige Konfigurationsdaten für den Nummerntyp an.
6. Geben Sie auf der Registerkarte **Format** die Mindestlänge, die maximale Länge, die Maske, die Maskenfüllung, das Füllzeichen, die Hashlänge und sonstige Konfigurationsdaten für den Nummerntyp an.
7. Klicken Sie die Schaltfläche **Speichern** an.

Löschen von Nummerntypen

Sie können einen vorhandenen Nummerntyp löschen, wenn er nicht mehr vom System verwendet wird.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Registerkarte **Nummern** an.
4. Wählen Sie in der Liste einen Nummerntyp aus und klicken Sie anschließend die Schaltfläche **Löschen** an.

Hilfethemen

Nummern - Registerkarte 'Allgemein':

Über die Registerkarte **Allgemein** können Sie die Details für den Nummerntyp angeben.

Typ Geben Sie den Namen des Nummerntyps an, den Sie erstellen wollen.

Beschreibung
Geben Sie die Beschreibung des Nummerntyps an, den Sie erstellen wollen.

Klasse Wählen Sie in der Dropdown-Liste die Klasse für den Nummerntyp aus, den Sie erstellen wollen.

CC Wählen Sie diesen Feldtyp aus, um den Nummerntyp 'Kreditkarte' (Credit Card) anzugeben.

MISC Wählen Sie diesen Feldtyp aus, um den Nummerntyp 'Verschiedenes' (Miscellaneous) anzugeben.

Beispiel: Frequent-Flyer-Nummer.

OTHER
Wählen Sie diesen Feldtyp aus, um den Nummerntyp 'Sonstiges' anzugeben.

Beispiel: eine unbekannte Nummer in einer Datenquelle.

PHONE
Wählen Sie diesen Feldtyp aus, um den Nummerntyp 'Telefonnummer' anzugeben.

PID Wählen Sie diesen Feldtyp aus, um den Nummerntyp als persönliche Identifikationsnummer anzugeben.

Beispiel: eine Führerschein- oder Sozialversicherungsnummer.

SYSID

Wählen Sie diesen Feldtyp aus, um den Nummerntyp 'Systemkennung' (System ID) anzugeben.

Beispiel: eine IP-Adresse.

Auflösungsverwendung
Wählen Sie in der Dropdown-Liste aus, ob dieser Nummerntyp für die Entitätsauflösung verwendet werden soll.

Keine Wählen Sie diesen Feldtyp aus, um anzugeben, dass der Nummernwert nicht für die Entitätsauflösung verwendet wird.

Kandidaten
Wählen Sie diesen Feldtyp aus, um anzugeben, dass der Nummernwert zum Erstellen einer Kandidatenliste und zum Erhöhen der Bewertung eines Kandidaten verwendet wird.

Status Wählen Sie in der Dropdown-Liste **Aktiv** aus, um anzugeben, dass diese Nummer aktiv ist. Wählen Sie andernfalls **Inaktiv** aus.

Protokoll beibehalten
Wählen Sie in der Dropdown-Liste **Ja** aus, um den Langzeitstatus des Nummerntypwerts aufzuzeichnen. Diese Option sollte nur für Nummerntypen verwendet werden, deren Werte sich nur selten ändern. Wählen Sie andernfalls **Nein** aus.

Anzeigeebene
Wählen Sie in der Dropdown-Liste aus, ob diese Nummer für Diagramme und Berichte verwendet werden soll.

Keine Wählen Sie diesen Feldtyp aus, um den Wert dieses Nummerntyps bei Diagrammen und Berichten auszuschließen.

Alle Wählen Sie diesen Feldtyp aus, um den Wert dieses Nummerntyps bei allen Diagrammen und Berichten einzuschließen.

Konfigurieren von Namensdaten

Die Namensdaten sind die im Segment <NAME> eines eingehenden UMF-Dokuments enthaltenen Daten. Während des Entitätsauflösungsprozesses werden Namensdaten analysiert, mit den Namensdaten vorhandener Entitäten in der Entitätendatenbank verglichen und auf der Basis des Grads der Namensdatenübereinstimmung bewertet.

Erweitertes Namenshashing mit IBM Global Name Recognition Name Hasher

Name Hasher verwendet die IBM Global Name Recognition-Technologie zum Erweitern des Namenshashings durch Erstellen von Variantenhashes für jeden eingehenden Namen. Dank der Variantennamenhashes kann die Entitätsauflösung eine grobe Namensübereinstimmung während der Namensanalyse und -bewertung verwenden.

Die folgenden Szenarios zeigen die Fälle, in denen die Verwendung von Name Hasher Vorteile bietet:

- Wenn ein Großteil der Daten nur für das Segment `<NAME>` abgeglichen werden kann.

- Wenn ein Großteil der Daten nur für das Segment <NAME> abgeglichen werden kann und die Mehrheit der Daten nicht der anglo-amerikanischen Schreibweise von Vorname, zweiter Vorname und Nachname entspricht.

Wird Name Hasher mit dem Namensbewertungsalgorithmus von Name Manager verwendet, besteht die Möglichkeit, Namen für die Kultur zu klassifizieren. Außerdem lassen sich hiermit Namen auf der Kandidatenliste in einem kulturspezifischen Kontext vergleichen und bewerten.

Name Hasher ist standardmäßig nicht aktiviert. Aktivieren Sie Name Hasher und die zugehörigen DQM-Funktionen über die Konfigurationskonsole.

Achtung: Wenden Sie sich an den IBM Kundendienst oder an den IBM Support, wenn Sie ein Upgrade für Name Hasher von der Produktversion 8.0 oder 4.2 durchführen und Sie ein bestehender Kunde sind, der Name Hasher erstmalig aktiviert. In beiden Fällen schlägt die Entitätsauflösung für neue Daten fehl, wenn diese mit den in der Entitätendatenbank vorhandenen Daten verglichen werden und Sie keine Unterstützung des IBM Kundendiensts oder des IBM Support haben.

Aktivieren des Features 'IBM Global Name Recognition Name Hasher':

Durch Aktivieren der Datenqualitätsverarbeitung des Features 'IBM Global Name Recognition Name Hasher' für das UMF-Segment <NAME> können Sie das Namensparsing, die Klassifizierung von Kulturen und die Hashwertgenerierung für Namen verbessern.

Vorbereitende Schritte

Wenn Sie Name Hasher für eine vorhandene Installation erstmalig aktivieren, wenden Sie sich an den IBM Kundendienst oder den IBM Support. Es müssen alle vorhandenen Daten aus allen Datenquellen erneut geladen werden, um zu verhindern, dass die Entitätsauflösung der neuen Daten im Hinblick auf die in der Entitätendatenbank vorhandenen Daten fehlschlägt.

Informationen zu diesem Vorgang

Diese Anweisungen stellen Zusammenfassungen der Tasks dar, die ausgeführt werden müssen, um Name Hasher zu aktivieren. Alle Schritte werden mithilfe der Konfigurationskonsole ausgeführt. Klicken Sie die Verknüpfung an, um schrittweise Anleitungen für jede Task aufzurufen.

Vorgehensweise

1. Aktivieren Sie die DQM-Funktion 282, um Namenshashes zu erstellen. Diese Funktion aktiviert die Name Hasher-Funktion in den Pipelines. Wenn Sie von Name Hasher eine frühere Produktversion als Version 8.0 Fixpack 2 verwendet haben, lesen Sie die Anweisungen in Migrieren auf das aktualisierte Feature 'IBM Global Name Recognition Name Hasher'. Sie wollen möglicherweise mehrere von DQM 282 verwendete Parameter wiederverwenden.
2. Aktivieren Sie die DQM-Funktion 610, damit Name Hasher Hashattribute für zusammengesetzte Namen erstellen kann.
3. Konfigurieren Sie die Kandidatenerstellungsregel 'Default w/ Name only' für erweitertes Namenshashing.
4. Konfigurieren Sie alle Datenquellen für erweitertes Namenshashing.

5. Inaktivieren Sie das Parsing für vollständige Namen in DQM-Funktion 252. Name Hasher erstellt für alle Namensteile Namenshashvarianten, nicht nur für den vollständigen Namen.
6. Konfigurieren Sie DQM-Regel 255 für erweitertes Namenshashing. Durch Ausführen dieses Schritts wird die Namensstandardisierungsfunktion von DQM 255 beibehalten. Sie inaktivieren jedoch das Standardnamenshashing für die Verwendung des erweiterten Namenshashings von Name Hasher. Sie stellen außerdem sicher, dass die Pipeline-Gültigkeitsprüfung, bei der geprüft wird, ob DQM 255 aktiviert ist, nicht fehlschlägt und die Pipelines abschaltet.
7. Aktivieren Sie die DQM-Funktion 260 für das UMF-Segment <NAME>. Diese DQM-Funktion ordnet eingehenden Namensdaten Namenskulturen zu. Für Name Hasher ist eine Namenskultur erforderlich, die kulturübergreifendes Fachwissen auf das erweiterte Namenshashing anwendet. Stellen Sie sicher, dass Name Manager aktiviert ist. (Name Manager ist in der Regel aktiviert.) Wenn Sie die DQM-Regel 260 aktivieren und Name Manager nicht aktiviert ist, schlägt die DQM-Regel 260 fehl und die Pipelines werden abgeschaltet.
8. Legen Sie die Systemparameter für Name Hasher fest. Durch Ausführen dieses Schritts konfigurieren Sie die erforderlichen Systemparameter für die Pipelines, die während des erweiterten Namenshashings verwendet werden.

Konfigurieren von Systemparametern für erweitertes Namenshashing:

Damit eine ordnungsgemäße Ausführung von Name Hasher während der Entitätsauflösung gewährleistet ist, muss der Standardwert des MM-Systemparameters HASHLESS_NAMES_ARE_GENERIC inaktiviert sein. Ist dieser Wert inaktiviert, wird die Name Hasher-Funktion auf alle eingehende Namensdaten angewendet.

Inaktivieren des Parsing für vollständige Namen für erweitertes Namenshashing:

Für eine ordnungsgemäße Funktionsweise von Name Hasher müssen Sie die auf dem Segment <NAME> vorhandene DQM-Regel 252 inaktivieren.

Konfigurieren der DQM-Regel 255 für das Feature 'IBM Global Name Recognition Name Hasher':

Für eine ordnungsgemäße Funktionsweise von Name Hasher müssen Sie den Wert des Parameters **UMF-Ausschluss** in der DQM-Funktion 255 konfigurieren.

Informationen zu diesem Vorgang

- Inaktivieren Sie das Standardnamensparsing und die Namenshashing-Funktion der DQM-Regel 255 zugunsten der von Name Hasher bereitgestellten erweiterten Parsing- und Hashing-Funktionen.
- Stellen Sie sicher, dass die DQM-Regel 255 aktiviert ist, um die Anforderungen der Gültigkeitsprüfung für die Pipeline zu erfüllen, laut der die DQM-Regel 255 aktiviert sein muss.

Konfigurieren von Kandidatenerstellungsregeln für erweitertes Namenshashing:

Für eine ordnungsgemäße Funktionsweise von Name Hasher müssen Sie sicherstellen, dass die Konfiguration **Default w/ Name Only** der Kandidatenerstellungsregeln den Abgleichtyp **Merkmal** enthält.

Konfigurieren von Datenquellen für erweitertes Namenshashing:

Wenn Sie das erweiterte Namenshashing verwenden, müssen Sie jede Datenquelle so konfigurieren, dass sie die Erstellung von Namensattributen für Kandidatenlisten zulässt. Setzen Sie dazu die Konfiguration für Kandidatenerstellungsregeln auf die Kandidatenerstellungsregel **Default w/ Name Only**.

Erstellen von Hashattributen für zusammengesetzte Namen:

Die DQM-Funktion 610 erstellt aus verschiedenen kleineren, im eingehenden UMF-Dokument enthaltenen Werten neue Attribute. Name Hasher verwendet DQM 610, um Hashwerte für zusammengesetzte Namen zu erstellen und diese in den UMF-Segmenten <NAME> und <ATTRIBUTE> als Attribute zu speichern.

Informationen zu diesem Vorgang

Die resultierenden Hashattribute für zusammengesetzte Namen enthalten stets GNR_HASH als Attributtyp (<ATTR_TYPE>). Wenn diese Hashattribute für Namen erstellt werden, kann die Entitätsauflösung während der Namensanalyse und -bewertung die Funktion für grobe Namensübereinstimmung verwenden. Die Funktion für grobe Namensübereinstimmung erhöht die möglichen Identitäts- und Entitätsübereinstimmungen bei Namensdaten.

Migrieren auf das aktualisierte Feature 'IBM Global Name Recognition Name Hasher':

Wenn Ihr Produkt eine ältere Version von Name Hasher als Version 8.0 Fixpack 2 verwendet hat, führen Sie neben den Standardtasks auch diese Tasks aus, die zum Durchführen eines Upgrades auf die aktuellste Name Hasher-Funktion erforderlich sind.

Vorgehensweise

1. Führen Sie mithilfe des Produktinstallationsprogramms das Standardproduktupgrade aus.
2. Inaktivieren Sie in der Konfigurationskonsole die DQM-Funktion 660 für das UMF-Segment `<NAME>`. Kopieren oder notieren Sie die aktuellen Werte für die im HTTP-URL-Parameter enthaltenen Parameter **`maxVariants`** und **`variantScoreThreshold`**. In den Produktversionen vor Version 8.0 Fixpack 2 hat die erweiterte Namenshashing-Funktion ein Name Hasher-Servlet verwendet, das auf einem Webanwendungsserver ausgeführt wurde. Ab Produktversion 8.0 Fixpack 2 ist die Name Hasher-Funktion in die Pipeline integriert. Durch Inaktivieren der DQM-Funktion 660 für das Segment `<NAME>` inaktivieren Sie auch das vorhandene Name Hasher-Servlet.
3. Aktivieren Sie DQM-Regel 282 (Namenshashvarianten) in der Konfigurationskonsole für das UMF-Segment `<NAME>` und fügen Sie die folgenden Funktionsparameterwerte ein oder konfigurieren Sie sie manuell:

   `maxVariants`
   Setzen Sie diesen Wert auf den Wert, der auch zuvor für den Parameter **`maxVariants`** der DQM-Funktion 660 verwendet wurde.

   `variantScoreThreshold`
   Setzen Sie diesen Wert auf den Wert, der auch zuvor für den Parameter **`variantScoreThreshold`** der DQM-Funktion 660 verwendet wurde.

Anmerkung: Wenn die DQM-Funktion 660 keine Werte für diese Parameter in der URL enthält, verwenden Sie die Standardwerte für die DQM-Funktion 282. Durch Ausführen dieses Schritts aktivieren Sie die Name Hasher-Funktion in der Pipeline.

4. Konfigurieren Sie die Systemparameter für Name Hasher in der Konfigurationskonsole. Durch Ausführen dieses Schritts nehmen Sie eine globale Konfiguration der erforderlichen Parameter vor, die von der Pipeline als Teil der Name Hasher-Funktion verwendet werden.

Alternativnamensparsing

Durch das Erstellen von Alternativnamensparses für einen eingehenden vollständigen Namen werden die Namensbewertungs- und Namensabgleichsfunktionen der Entitätsauflösung erweitert.

Das Parsen von Namen in Namensteile stellt einen der ersten Schritte im Namensabgleich dar. Alternativnamensparses stellen mögliche Variationen des Namens dar. Wenn Sie Alternativnamensparses für eingehende Namensdaten generieren, können Sie dadurch die Wahrscheinlichkeit erhöhen, dass der eingehende Name korrekt analysiert und bewertet wird.

Verwenden Sie die DQM-Funktion 289, um Alternativnamensparses zu generieren. Diese Funktion ist standardmäßig nicht aktiviert. Sie müssen die DQM-Funktion 289 für das Segment <NAME> in der Konfigurationskonsole konfigurieren, um Alternativnamensparses generieren zu können.

Möglicherweise gibt es nicht für alle Namen einen Alternativparse. Wenn ein Alternativnamensparse für den Namen vorhanden ist und sich dieser Alternativparse vom Primärnamensparse unterscheidet, generiert die DQM-Funktion ein zweites Segment <NAME>, das den Alternativparse einschließt.

Berücksichtigen Sie beispielsweise die folgenden eingehenden Namensdaten:

```
<UMF_ENTITY>
 <NAME>
    <NAME_TYPE>M</NAME_TYPE>
    <FULL_NAME>ALLEN CRAIG</FULL_NAME>
    </NAME>
....
</UMF_ENTITY>
```

In diesem Beispiel kann der vollständige Name mindestens zwei verschiedene Parses aufweisen. "Allen" und "Craig" können sowohl Vor- als auch Familiennamen darstellen. Durch das Generieren von Alternativparses dieses Namens ist der Entitätsauflösungsprozess in der Lage, den Namen zu analysieren und ihn anhand eines Vergleichs mit weiteren Entitäten in der Entitätendatenbank zu bewerten.

Wenn die DQM-Funktion 289 für den UMF-Tag <FULL_NAME> des Segments <NAME> konfiguriert ist, wird während der Namensverarbeitung einen Alternativnamensparse erstellt und dem UMF-Datensatz hinzugefügt. Der resultierende Datensatz ähnelt dem folgenden Datensatz:

```
<UMF_ENTITY>
 <NAME>
    <NAME_TYPE>M</NAME_TYPE>
    <FIRST_NAME>ALLEN</FIRST_NAME>
    <LAST_NAME>CRAIG</LAST_NAME>
  </NAME>
  <NAME>
    <NAME_TYPE>ALT</NAME_TYPE>
    <FIRST_NAME>CRAIG</FIRST_NAME>
```

```
    <LAST_NAME>ALLEN</LAST_NAME>
    </NAME>
....
</UMF_ENTITY>
```

Das erste Segment <NAME> enthält den Primärnamensparse und den ursprünglichen Wert <NAME_TYPE>. Das zweite Segment <NAME> enthält den generierten Alternativparse, der durch den <NAME_TYPE>-Wert ALT angegeben ist. (Bei diesem Beispiel wird davon ausgegangen, dass der Wert für den Alternativparsenamenstyp der Standardwert ist.)

Konfigurieren von Namen zum Erstellen von Alternativnamensparses:

Sie können Namen konfigurieren, um Alternativnamensparses zu erstellen, die zur Generierung mehrerer Namenshashes verwendet werden können. Wenn Sie das Feature 'IBM Global Name Recognition Name Hasher' verwenden, kann die Erstellung von Alternativnamensparses die Funktionen für grobe Namensübereinstimmungen erweitern, um die Entitätsauflösung für Namensdaten zu verbessern.

Vorbereitende Schritte

- Stellen Sie sicher, dass Name Manager aktiviert ist und dass der Pfad zu den Unterstützungsdateien in den Systemparametern festgelegt ist. Ist diese DQM-Funktion aktiviert, ohne dass ein gültiger Pfad zu den Name Manager-Unterstützungsdateien angegeben ist, protokolliert die Pipeline einen Fehler und wird beendet.
- Wenn Sie die DQM-Funktion für das Feature für das Parsing von Alternativnamen aktivieren, ändern Sie die Systemkonfiguration. Wie bei allen anderen Konfigurationsänderungen müssen Sie auch hier sicherstellen, dass alle aktiven Pipelines gestoppt wurden, bevor Sie die Konfiguration ändern. Starten Sie die Pipelines anschließend neu, um sie mit den Konfigurationsänderungen zu reinitialisieren.

Informationen zu diesem Vorgang

- Bei neuen Produktinstallationen mit Version 8.0 Fixpack 2 oder später ist diese DQM-Funktion bereits konfiguriert und aktiv.
- Bei Produktversionen, für die ein Upgrade auf Version 8.0 Fixpack 2 oder später durchgeführt wurde, ist diese DQM-Funktion konfiguriert, aber inaktiv. Wenn Sie Alternativnamensparses generieren wollen, müssen Sie den Status der vorhandenen DQM-Funktion in **Aktiv** ändern.

Vorgehensweise

1. Wählen Sie in der Konfigurationskonsole **Konfiguration** > **UMF** > **DQM-Regeln** aus.
2. Wählen Sie NAME in der Liste **Segment** aus.
3. Wählen Sie den UMF-Tagnamen aus, für den **289 - Parser für Alternativnamen** in **Funktion** aufgelistet ist.
4. Stellen Sie sicher, dass Aktiv in **Status** ausgewählt ist.
5. Prüfen Sie auf der Registerkarte **Parameter** die folgenden Parameterwerte oder legen Sie diese fest:
   - **Schwellenwert für Parsing-Bewertung**: Setzen Sie diesen Wert auf eine Zahl zwischen 0 und 100. Je höher die Bewertung ist, desto weniger Alternativparses werden erstellt. Dieser Wert legt den Schwellenwert für den Mindestwert für die Übereinstimmungswahrscheinlichkeit fest, die der Namensparser verwendet, um zu ermitteln, ob ein Alternativparse für den eingehenden Namen

erstellt werden muss. Wenn kein Alternativparse mit einer höheren Übereinstimmungswahrscheinlichkeit gefunden wird oder die Bewertung des ursprünglich bereitgestellten eingehenden Parse bereits über dem Schwellenwert liegt, wird kein Alternativparse erstellt.

- **Typ des Alternativnamen**: Geben Sie den Wert für NAME_TYPE ein, um anzugeben, dass dieser Name ein Alternativparse ist. Dieser Wert ist der UMF-Tag, der dem Segment <NAME> für jeden erstellten Alternativnamensparse hinzugefügt wird. Dieser Wert ist standardmäßig auf ALT gesetzt. Zum Sicherstellen der vollständigen Zurückführung der Entitätsauflösung dürfen Sie diesen Wert nicht auf einen vorhandenen, in der Konfigurationskonsole konfigurierten eingehenden Namenstyp (NAME_TYPE) setzen. Sie dürfen diesen Wert insbesondere nicht auf **M** oder **A** setzen.

6. Klicken Sie **Speichern** an.

Geschlechtsbestimmung

Bei der Verarbeitung eingehender Namensdaten kann das Geschlecht eines persönlichen Namens manchmal ein Bestimmungsfaktor für die Übereinstimmung zweier Entitäten sein. Das Geschlecht fügt der Entitätsauflösungsbewertung Bestätigungs- oder Zurückweisungsgewichtung hinzu, wenn zwei Identitäten dieselbe Entität darstellen.

Die DQM-Funktion 258 gibt das Geschlecht des Segments <NAME> in einem eingehenden UMF-Datensatz dynamisch an, erstellt ein Geschlechtsmerkmal und fügt es dem eingehenden UMF-Datensatz hinzu. Das Geschlechtsmerkmal wird mithilfe des Segments <ATTRIBUTE> hinzugefügt.

- Wenn der eingehende UMF-Datensatz bereits ein Geschlechtsmerkmal in seinen Daten enthält, generiert die DQM-Funktion 258 kein weiteres Geschlechtsmerkmal.
- Wenn der UMF-Datensatz mehr als ein Segment <NAME> enthält, erstellt die DQM-Funktion 258 nur ein Geschlechtsmerkmal für den gesamten Eingabedatensatz. In diesem Fall kann die Generierung mehrerer Geschlechtsattribute redundant sein oder Konflikte verursachen.

Wenn Sie das Geschlecht eines Namens dynamisch ermitteln wollen, stellen Sie sicher, dass mindestens ein UMF-Tag im Segment <NAME> für die Verwendung der DQM-Funktion 258 konfiguriert ist.

- Bei neuen Produktinstallationen mit Version 8.0 Fixpack 2 oder später ist diese DQM-Funktion bereits konfiguriert und aktiv.
- Bei Produktversionen, für die ein Upgrade auf Version 8.0 Fixpack 2 oder später durchgeführt wurde, ist diese DQM-Funktion konfiguriert, aber inaktiv. Wenn Sie diese verbesserte Geschlechtsfunktionalität verwenden wollen, müssen Sie den Status in **Aktiv** ändern. Wenn Sie das Geschlecht bisher über den Parameter **Geschlechtsmerkmaltyp** der DQM-Funktion 255 zugeordnet haben, setzen Sie den Wert dieses Parameters auf KEINE zurück. Sie können DQM 255 weiterhin für alle UMF-Tags <NAME> verwenden, um Namen zu standardisieren.

Möglicherweise wollen Sie auch die folgenden Konfigurationen in der Konfigurationskonsole überprüfen:

- Stellen Sie sicher, dass das Geschlechtsmerkmal als Bestätigung oder Zurückweisung in der Entitätsauflösung nach Datenquelle konfiguriert ist. Sie zeigen diese Einstellung im Feld **Auflösungsverwendung** an oder konfigurieren sie, indem Sie **Konfiguration** > **Quellen** > **Merkmale** auswählen.
- Stellen Sie sicher, dass das Geschlechtsmerkmal mit den korrekten Anpassungswerten für die Entitätsauflösung konfiguriert ist. Sie zeigen diese Einstellung an

oder konfigurieren Sie, indem Sie **Konfiguration** > **Auflösung** > **Merkmale** auswählen. Überprüfen Sie die dem Geschlechtsmerkmal zugeordneten Werte der Bestätigungs- und Zurückweisungsgewichtungen, um sicherzustellen, dass sie Ihren Anforderungen entsprechen.

.

Betrachten Sie das Beispielsegment <NAME> im folgenden eingehenden UMF-Datensatz:

```
<UMF_ENTITY>
 <NAME>
    <NAME_TYPE>M</NAME_TYPE>
    <LAST_NAME>RASUL</LAST_NAME>
    <FIRST_NAME>KARIM</FIRST_NAME>
    </NAME>
.....
</UMF_ENTITY>
```

Wenn DQM 258 für den UMF-Tag <FIRST_NAME> des Segments <NAME> aktiviert ist, ähnelt der eingehende UMF-Datensatz nach der Analyse und Erstellung des Geschlechts dem folgenden Datensatz:

```
<UMF_ENTITY>
 <NAME>
    <NAME_TYPE>M</NAME_TYPE>
    <LAST_NAME>RASUL</LAST_NAME>
    <FIRST_NAME>KARIM</FIRST_NAME>
    </NAME>
 <ATTRIBUTE>
    <ATTR_TYPE>GENDER</ATTR_TYPE>
    <ATTR_VALUE>M</ATTR_TYPE>
  </ATTRIBUTE>
.....
</UMF_ENTITY>
```

Konfigurieren von Namen für die Geschlechtszuordnung:

Sie können die Entitätsauflösung verbessern, indem Sie einer Entität anhand eines Namens ein Geschlecht zuordnen. Sie können Bewertungen für Bestätigungen und Zurückweisungen festlegen, die darauf basieren, ob das Geschlecht der verglichenen Entitäten übereinstimmt. Sie können Namen konfigurieren, um ein Geschlecht dynamisch zuzuordnen und das Geschlechtsmerkmal den eingehenden UMF-Datensätzen hinzuzufügen.

Vorbereitende Schritte

- Stellen Sie sicher, dass Name Manager aktiviert ist und dass der Pfad zu den Name Manager-Unterstützungsdateien in den Systemparametern festgelegt ist. Ist diese DQM-Funktion aktiviert, ohne dass ein gültiger Pfad zu den Name Manager-Unterstützungsdateien angegeben ist, protokolliert die Pipeline einen Fehler und wird beendet.
- Wenn Sie das Geschlechtsfeature dieser DQM-Funktion aktivieren, ändern Sie die Systemkonfiguration. Wie bei allen anderen Konfigurationsänderungen müssen Sie auch hier sicherstellen, dass alle aktiven Pipelines gestoppt wurden, bevor Sie die Konfiguration ändern. Starten Sie die Pipelines anschließend neu, um sie mit den Konfigurationsänderungen zu reinitialisieren.

Informationen zu diesem Vorgang

- Bei neuen Produktinstallationen mit Version 8.0 Fixpack 2 oder später ist diese DQM-Funktion bereits konfiguriert und aktiv.

- Bei Produktversionen, für die ein Upgrade auf Version 8.0 Fixpack 2 oder später durchgeführt wurde, ist diese DQM-Funktion konfiguriert, aber inaktiv. Wenn Sie diese verbesserte Geschlechtsfunktionalität verwenden wollen, müssen Sie den Status der vorhandenen DQM-Funktion in **Aktiv** ändern. Wenn Sie das Geschlecht bisher über den Parameter **Geschlechtsmerkmaltyp** der DQM-Funktion 255 zugeordnet haben, setzen Sie den Wert dieses Parameters auf `KEINE` zurück. Sie können DQM 255 weiterhin für alle UMF-Tags `<NAME>` verwenden, um Namen zu standardisieren.

Vorgehensweise

1. Wählen Sie in der Konfigurationskonsole **Konfiguration** > **UMF** > **DQM-Regeln** aus.
2. Wählen Sie **NAME** in der Liste **Segment** aus.
3. Wählen Sie den UMF-Tagnamen **FIRST_NAME** aus, in dem auch **258 - Namensbasierte GNR-Geschlechtszuordnung** als Funktion aufgelistet ist. Diese Konfiguration wertet nur den ersten Namen im eingehenden Datensatz für persönliche Namen aus. Ist die Funktion zur Namenskategorisierung von Name Manager aktiviert, müssen Sie den vollständigen Namen im UMF-Tag `LAST_NAME` des Segments `NAME` angeben.
4. Stellen Sie in **Status** sicher, dass **Aktiv** ausgewählt ist.
5. Stellen Sie in **Regelfilter** sicher, dass der Feldwert `NAME_TYPE=M` lautet. Dieser Wert stellt sicher, dass nur der Hauptname jedes Eingabedatensatzes ausgewertet wird, um ein Geschlecht zuzuordnen.
6. Stellen Sie auf der Registerkarte **Parameter** sicher, dass der Mindestwert für die Geschlechtsübereinstimmungswahrscheinlichkeit auf eine Zahl zwischen 0 und 100 gesetzt ist. Die Standardbewertung ist auf 90 gesetzt, was bedeutet, dass das Geschlecht nur zugeordnet wird, wenn bei der Geschlechtszuordnung eine Übereinstimmungswahrscheinlichkeit von 90 % vorliegt. Seien Sie vorsichtig beim Herabsetzen dieser Bewertung, denn eine unter 90 % liegende Mindestbewertung kann sich auf die Entitätsauflösung während der Geschlechtsbestätigung oder -zurückweisung auswirken.
7. Klicken Sie **Speichern** an.

Kategorisierung von Namen

Ist der Name Manager-Systemparameter **`NAMESIFTER`** aktiviert, kategorisiert das Produkt die Namen nach Typ. Durch die Kategorisierung von Namen nach Typ kann die Entitätsauflösung während der Namensanalyse, der Bewertung und des Abgleichs die entsprechenden linguistischen und Referenzdatenressourcen anwenden:

Namen werden als persönlicher Namenstyp oder als Unternehmensnamentyp kategorisiert.

Persönliche Namen
: Ein persönlicher Name enthält keine Indikatoren dafür, dass er zu einer anderen Kategorie gehören könnte. (Beispiel: "Linda K. Schmidt".) Als persönliche Namen kategorisierte Namen werden in Namensteile geparst. Die Namensteile werden anschließend nach Kultur kategorisiert, wodurch beim Analyse- und Bewertungsprozess eine höhere Genauigkeit erzielt wird.

Unternehmensnamen
: Ein Geschäfts- oder Unternehmensname enthält einen gewissen unpersönlichen Indikator. Beispiel: "Schmidt & Co.") Den als Unternehmensnamen kategorisierten Namen wird automatisch die Kultur "Unternehmen" zugeordnet.

Unbekannte Namen

Ein als "unbekannt" kategorisierter Name enthält ein bestimmtes Element, das als Rechtschreibfehler oder als anderes Konstrukt betrachtet wird, welches normalerweise nicht in persönlichen oder Geschäftsnamen vorkommt. (Beispiel: "SCHMI".)

Kategorisieren von Namen nach Typ:

Der Name Manager-Systemparameter **NAMESIFTER** bietet die Möglichkeit, Namen nach Typ zu kategorisieren. Die häufigsten Namenstypen sind persönliche Namen und Geschäftsnamen. Durch die Kategorisierung von Namen können bei der Namensanalyse und Namensbewertung des Entitätsauflösungsprozesses genauere Ergebnisse erzielt werden.

Kategorisieren persönlicher Namen nach Kultur:

Die DQM-Funktion 260 wurde erstellt, um die Kultur für den Namen zu ermitteln und diesen Wert an das UMF-Segment <NAME> anzuhängen. Die Segmentkonfiguration <NAME> enthält eine DQM-Regel 260 für den UMF-Tag <LAST_NAME> . Verwenden Sie diese Anweisungen, um die DQM-Regel 260 einem anderen UMF-Tag im Segment <NAME> hinzuzufügen oder um die vorhandene Regel für den UMF-Tag <LAST_NAME> zu aktualisieren.

Name Manager - Übersicht

Name Manager

Name Manager erhöht die Namensgenauigkeit für Problemstellungen bei der erweiterten Namensbestätigung wie z. B. bei verschiedenen Transliterationen von Namen, bei Rechtschreibfehlern innerhalb der Kulturen, bei Schreibvarianten innerhalb von Kulturen oder zwischen Kulturen und bei Namen mit patronymischen (Vatersname) oder Ehrenbezeichnungen. Das Produkt verwendet die Komponentenbibliotheken von IBM InfoSphere Global Name Recognition, die eine Wissensbasis mit über einer Milliarde kulturübergreifender Namen und eindeutiger linguistischer Informationen enthalten und dem Produkt kulturspezifische Namensabgleichfunktionen bereitstellen.

Name Manager bewertet Namen mithilfe des folgenden Prozesses:

- Kategorisieren von Namen nach Namenstyp (persönliche Namen oder Geschäftsnamen)
- Parsen persönlicher Namen in Namensteile
- Klassifizieren von Namen nach Kultur (unterstützt über 20 Kulturen, einschließlich Afghanisch, Arabisch, Farsi, Han, Japanisch, Koreanisch, Thailändisch, Vietnamesisch und Yoruba)
- Normalisieren persönlicher Namen (wenn der Name als anglo-amerikanisch, arabisch, chinesisch, deutsch, französisch, indisch, koreanisch, russisch spanisch, oder thailändisch klassifiziert wird)

Konfigurieren von Name Manager

Die Name Manager-Namensbewertung ist bereits standardmäßig aktiviert und konfiguriert, wenn Sie IBM InfoSphere Identity Insight installieren. Sie können die Name Manager-Konfigurationseinstellungen jedoch über die Konfigurationskonsole prüfen oder ändern, einschließlich der folgenden Einstellungen:

- Name Manager-Systemparameter, einschließlich des Unterstützungspfads für die Name Manager-Komponentenbibliotheken (globale Parameter, die von der Pipeline zum Ausführen der Entitätsauflösung verwendet werden)
- Schwellenwerte für die Name Manager-Namensbewertung, die beim Namensabgleich verwendet werden (Bestätigungen und Zurückweisungen)

Konfigurieren von Systemparametern für Name Manager:

Die Systemparameter für die Name Manager-Namensbewertung werden standardmäßig beim Installieren des Produkts konfiguriert. Sie können die Standardsystemparameter jedoch bei Bedarf aktualisieren. Es kann beispielsweise sein, dass Sie die Position der Name Manager-Unterstützungsbibliotheken ändern müssen.

Informationen zu diesem Vorgang

Sie legen den Pfad der Name Manager-Unterstützungsbibliotheken fest und aktivieren über die Name Manager-Systemparameter die Kategorisierung von Namen nach Typ. Sie legen außerdem den Systemparameter **CROSSCHECKCULTURE** fest, um die Namensverarbeitung zwischen verschiedenen Namenskulturen zu konfigurieren.

Vorgehensweise

1. Wählen Sie in der Konfigurationskonsole **Konfiguration** > **Allgemein** > **Systemparameter** aus.
2. Wählen Sie die Parametergruppe **NAMEMANAGER** in der Liste **Parametergruppe** aus.
3. Wählen Sie im linken Teilfenster den zu konfigurierenden Systemparameter von Name Manager aus:

Name Manager-Systemparameter	Beschreibung
SUPPORTPATH	Gibt die Position der Name Manager-Unterstützungsdateien an. Der Standardwert lautet ./data und gibt den relativen Pfad zum übergeordneten Produktverzeichnis an. Ändern Sie diesen Wert in den absoluten Pfad der neuen Position, wenn die Unterstützungsdateien während der Installation an eine andere Position verschoben werden.
NAMESIFTER	Gibt an, ob die Funktion für die Namenskategorisierung nach Namenstyp (persönliche Namen oder Unternehmensnamen) aktiviert ist. Geben Sie den Wert 1 (neuer Standardwert für die Installation) in **Aktueller Wert** ein, um die Kategorisierung von Namen nach Typ (Name Sifter-Funktion) zu aktivieren. Geben Sie den Wert 0 (Standardwert für das Upgrade) in **Aktueller Wert** ein, um die Kategorisierung von Namen nach Typ (Name Sifter-Funktion) zu inaktivieren.

Name Manager-Systemparameter	Beschreibung
CROSSCHECKCULTURE	Gibt an, ob eine Name Manager-Namensbewertung zwischen Namenskulturen ausgeführt werden soll, wenn sich die Namenskulturen voneinander unterscheiden. Wenn Sie nur den eingehenden Namenskulturwert vor dem Bewerten beider Namen prüfen wollen, geben Sie `0` in **Aktueller Wert** ein. Wenn Sie die Namenskulturwerte vor dem Bewerten prüfen wollen (neuer Standardwert für die Installation), geben Sie den Wert 1 in **Aktueller Wert** ein.

Achtung: Der Systemparameter **CROSSCHECKCULTURE** hat Einfluss darauf, wie die Entitätsauflösung die Namensbewertung nach Kultur in den Pipelines ausführt. Wenden Sie sich an den IBM Kundendienst oder den IBM Support, bevor Sie den aktuellen Wert dieses Systemparameters ändern.

4. Klicken Sie **Speichern** an.

Konfigurieren von Name Manager-Schwellenwerten für Bestätigungen und Zurückweisungen:

Sie können die Schwellenwerte für die Namensbewertung festlegen, die Name Manager während der Entitätsauflösung nach Auflösungsregel verwendet. Nach der Erstellung der Kandidatenliste vergleicht die Entitätsauflösung die Name Manager-Namensbewertung auf der Basis des Namensteils und der für jeden Namensteil festgelegten Kultur mit diesen Schwellenwerten. Wenn die Name Manager-Bewertung die konfigurierte Schwellenwertbewertung für den Namensteil erfüllt oder übersteigt, werden die Namen als übereinstimmend betrachtet.

Informationen zu diesem Vorgang

Wichtig: Die Schwellenwerte für die Name Manager-Namensteilbewertung werden standardmäßig für die optimale Name Manager-Bewertung und -Leistung konfiguriert. Die Änderung der Standardwerte ist eine Konfigurationstask für Fortgeschrittene, da sich diese Werte negativ auf die Entitätsauflösung für Regeln einschließlich der Namensbewertung auswirken können. Wenden Sie sich an den IBM Kundendienst oder den IBM Support, bevor Sie diese Standardwerte ändern.

Vorgehensweise

1. Wählen Sie in der Konfigurationskonsole **Konfiguration** > **Auflösung** > **Auflösungsregeln** aus.
2. Wählen Sie die Auflösungskonfiguration in der Liste **Auflösungskonfigurationen** aus.
3. Wählen Sie die Auflösungsregel aus.
4. Klicken Sie **Schwellenwerte für Bestätigung/Zurückweisung** an.
5. Geben Sie unter **Name Manager** die Mindestbewertung für jeden Schwellenwert für Namensteile ein, die zwischen 0.0 und 1.0 betragen kann. Je höher die Bewertung, desto genauer muss die Übereinstimmung der Namensteile sein. Eine Bewertung unter 0.7 ist in der Regel nicht für einen Abgleich von Namensteilen geeignet.

Name Manager-Namensbewertung:

Der Name Manager-Algorithmus bewertet eingehende Namensdaten, indem er den Namen in Namensteile aufspaltet und anschließend die Kultur für jeden Namensteil bestimmt. Der Algorithmus bewertet anschließend jeden Namensteil und die resultierenden Bewertungen werden während der Entitätsauflösung verwendet.

Obwohl der Name Manager-Algorithmus von den Name Comparator-Algorithmen (NC1 und NC2) getrennt ist, müssen Sie weiterhin NC1 oder NC2 auswählen. Während des Entitätsauflösungsprozesses werden Namen zunächst auf Basis der ausgewählten Name Comparator-Algorithmen bewertet. Wenn der Name als exakte Übereinstimmung bewertet wird, überspringt die Entitätsauflösung die Name Manager-Bewertung, da die exakte Übereinstimmung den Namensbewertungsteil der Auflösungsregel erfüllt. Wenn der eingehende Name eine Bewertung erhält, die unter einer exakten Übereinstimmung liegt, wird der Name vom Entitätsauflösungsprozess mithilfe des Name Manager-Algorithmus bewertet.

Zunächst parst der Algorithmus den Namen in Namensteile (Vorname, Familienname und vollständiger Name) und ermittelt anschließend die Kultur für jeden Namensteil. Zuletzt weist der Algorithmus jedem Namensteil eine Bewertung zu und vergleicht die Bewertungen mit den Name Manager-Bewertungsschwellenwerten, um zu ermitteln, wie hoch die Übereinstimmung der Namen ist. Je höher der Bewertungsschwellenwert ist, desto höher muss die Übereinstimmung zwischen den eingehenden Namensdaten und den Namensteilen aus der vorhandenen Entität in der Entitätendatenbank sein.

Auswählen von Kulturen für die Name Manager-Namensbewertung:

Sie können konfigurieren, welche Methoden für die Namensbewertung während des Namensbewertungsprozesses der Entitätsauflösung von der Kultur verwendet werden sollen. Name Manager kann nur die Namenskultur und die Bewertungsnamen für die Kulturen ermitteln, die für die Verwendung des Name Manager-Namensabgleichs konfiguriert sind.

Informationen zu diesem Vorgang

Standardmäßig sind alle unterstützten Kulturen bereits auf der Grundlage der aktuellsten bewährten Verfahren für die typische Namensbewertung konfiguriert. Die Änderung der Standardwerte ist eine Aufgabe für Fortgeschrittene, die die Entitätsauflösung für Regeln einschließlich der Namensbewertung negativ beeinflussen kann. Wenden Sie sich an den IBM Kundendienst oder an den IBM Support, bevor Sie die Standardkonfigurationswerte ändern.

Vorgehensweise

1. Wählen Sie in der Konfigurationskonsole **Konfiguration** > **Auflösung** > **Name Manager-Abgleichkonfiguration** aus.
2. Wählen Sie eine Name Manager-Kultur aus.
3. Wählen Sie Ja in **Name Manager-Namensabgleich verwenden** aus.
4. Klicken Sie **Speichern** an.

Konfigurieren von DQM-Regeln

Sie können DQM-Regeln für das Reparieren und Bereinigen von Daten konfigurieren, die nicht den Mindeststandards für die Datenqualität entsprechen. DQM-Regeln werden auf einen bestimmten UMF-Tag in einem bestimmten UMF-Segment angewendet.

Informationen zu diesem Vorgang

DQM-Regeln können über die Registerkarte **DQM-Regeln** der Konsole angezeigt und modifiziert werden.

DQM-Regeln

DQM-Regeln sind konfigurierte, systemdefinierte Reparatur-, Bereinigungs- und Standardisierungsfunktionen, die in einer bestimmten Reihenfolge auf eingehende Identitätsdatenwerte angewendet werden.

DQM-Regeln definieren, wie das System die eingehenden Daten verarbeitet, formatieren Zahlen ordnungsgemäß, stellen Schreib- oder Transpositionsfehlern fest und korrigieren sie. Außerdem stellen sie absichtliche Ungenauigkeiten fest, die von Personen eingeführt wurden, die ihre Identitäten verheimlichen wollen, und korrigieren sie. DQM-Regeln können eine Reihe von Reparatur-, Bereinigungs- und Standardisierungsfunktionen für eingehende Identitätsdatenwerte ausführen.

Sie konfigurieren eine DQM-Regel, indem Sie ein bestimmtes UMF-Segment (wie NAME) und einen UMF-Tag (wie NAME_TYPE) auswählen, anschließend eine systemdefinierte DQM-Funktion auswählen, die auf die eingehenden Daten angewendet werden soll, und abschließend die zugeordneten Parameter für diese Funktion angeben, zu denen die Standardwerte gehören, die das System anwenden soll. Sie wählen auch die Reihenfolge aus, in der diese DQM-Regel auf das ausgewählte UMF-Segment angewendet werden soll, da das Produkt mehrere DQM-Regeln für jedes UMF-Segment unterstützt.

Anzeigen von DQM-Regeln

DQM-Regeln reparieren oder bereinigen Daten, die den Mindestanforderungen für den Datenqualitätsstandard nicht erfüllen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **DQM-Regeln** an.
4. Wählen Sie in der Dropdown-Liste **Segment** das UMF-Segment aus, das die anzuzeigenden DQM-Regeln enthält.

Erstellen von DQM-Regeln

Sie erstellen DQM-Regeln für das Reparieren und Bereinigen von Daten, die nicht den Mindeststandards für die Datenqualität entsprechen.

Informationen zu diesem Vorgang

DQM-Regeln werden auf einen bestimmten UMF-Tag in einem bestimmten UMF-Segment angewendet. DQM-Regeln können auch geklont werden, um neue Regeln auf der Basis vorhandener Regeln zu erstellen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **DQM-Regeln** an.
4. Wählen Sie in der Dropdown-Liste **Segment** das UMF-Segment aus, für das eine DQM-Regel erstellt werden soll.
5. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie die Schaltfläche **Neu** an, um eine vollständig neue DQM-Regel zu erstellen. an.
- Wählen Sie eine DQM-Regel in der Liste aus und klicken Sie anschließend die Schaltfläche **Klonen** an, um eine DQM-Regel auf der Basis einer vorhandenen DQM-Regel zu erstellen.

6. Geben Sie auf der Registerkarte **Allgemein** die Reihenfolge, den Namen des UMF-Tags, die Funktion, den Regelfilter, den UMF-Ausschluss, den Wert für **Korrigierbar**, den Status und sonstige Konfigurationsdaten für die DQM-Regel an.
7. Geben Sie auf der Registerkarte **Parameter** die Parameter für die DQM-Regel an.
8. Klicken Sie die Schaltfläche **Speichern** an.
9. Validieren Sie die DQM-Regel.

Löschen von DQM-Regeln

Wenn eine DQM-Regel nicht mehr erforderlich ist, sollten Sie sie löschen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **DQM-Regeln** an.
4. Wählen Sie in der Dropdown-Liste **Segment** das UMF-Segment aus, für das eine DQM-Regel gelöscht werden soll.
5. Wählen Sie das Kontrollkästchen neben der DQM-Regel bzw. neben den DQM-Regeln aus, die Sie löschen wollen.
6. Klicken Sie die Schaltfläche **Löschen** an.

Prüfen von DQM-Regeln

Wenn Sie eine DQM-Regel hinzufügen oder bearbeiten, sollten Sie sie vor der Anwendung auf Quellendaten prüfen.

Informationen zu diesem Vorgang

Die Prüffunktion wird verwendet, um alle Regeln in Beziehung zueinander für ein ganzes Segment zu prüfen. Eine Prüfung, die für eine einzelne Regel durchgeführt werden kann, wird beim Speichern der Regel automatisch durchgeführt.

Wenn Sie sich an der Konfigurationskonsole anmelden, werden die DQM-Regeln automatisch auf ihre Gültigkeit überprüft. Wird ein Fehler gefunden, wird eine Headernachricht oben in der Anzeige der Konfigurationskonsole angezeigt. Klicken Sie den Link **Prüfen Sie die Fehler** an, um ein neues Fenster zu öffnen, in dem die Fehler beschrieben werden.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **DQM-Regeln** an.
4. Wählen Sie in der Dropdown-Liste **Segment** das UMF-Segment aus, für das Sie eine DQM-Regel prüfen wollen. Wird kein Segment ausgewählt, wird die Prüfung für alle Segmente durchgeführt.
5. Klicken Sie die Schaltfläche **Prüfen** an.

Inaktivieren von DQM-Regeln

Sie können eine DQM-Regel inaktivieren, die nicht mehr benötigt wird.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **DQM-Regeln** an.
4. Wählen Sie in der Dropdown-Liste **Segment** das gewünschte UMF-Segment aus, das die DQM-Regel enthält, die inaktiviert werden soll.
5. Klicken Sie die DQM-Regel an, die inaktiviert werden soll.
6. Setzen Sie das Statusfeld auf der Registerkarte **Allgemein** auf **Inaktiv**.
7. Klicken Sie die Schaltfläche **Speichern** an.

Hilfethemen

DQM-Regeln - Registerkarte 'Allgemein':

Über die Registerkarte **Allgemein** können Sie die Details für die DQM-Regel angeben.

Segment
Geben Sie den Namen des UMF-Segments an, auf das die DQM-Regel angewendet werden soll. Dieses Feld ist normalerweise schreibgeschützt. Es kann nur bearbeitet werden, wenn die Dropdown-Liste **Segment** beim Erstellen einer neuen DQM-Regel leer gelassen wurde. Der Segmentname muss in Großbuchstaben eingegeben werden.

Reihenfolge
Geben Sie die Nummer für die Reihenfolge an, in der die DQM-Regel angewendet wird.

UMF-Tagname
Geben Sie den Namen des UMF-Tags an, auf den die DQM-Regel angewendet werden soll. Der UMF-Tagname muss in Großbuchstaben eingegeben werden.

Funktion
Wählen Sie in der Dropdown-Liste die DQM-Funktion aus, auf der die DQM-Regel basieren soll.

Funktionsbeschreibung
Das Feld für die Funktionsbeschreibung ist ein Anzeigefeld, das die Funktionsweise der DQM-Regel beschreibt.

Regelfilter
Wenn die DQM-Regel nur angewendet werden soll, wenn der UMF-Tag einen bestimmten Wert enthält, geben Sie eine Gleichung ein, die den UMF-Tagnamen und den zum Ausführen der DQM-Regel erforderlichen Wert enthält.

Beispiel: `NAME_TYPE=m`
Mit dieser Beispieleinstellung wird die DQM-Regel nur angewendet, wenn der UMF-Tag `NAME_TYPE` den Wert `m` enthält.

UMF-Ausschluss
Wenn die DQM-Regel auf bestimmte UMF-Eingabedokumente nicht ange-

wendet werden soll, geben Sie eine durch Kommas getrennte Liste von UMF-Eingabedokumenten ein, für die diese Regel nicht ausgeführt werden soll.

Beispiel: `UMF_QUERY, UMF_DISCLOSED RELATION`
Mit dieser Beispieleinstellung wird die DQM-Regel nicht auf die UMF-Eingabedokumente `UMF_QUERY` und `UMF_DISCLOSED_RELATION` angewendet.

Korrigierbar
Wählen Sie in der Dropdown-Liste **Ja** aus, um ungültige und unter dem Standard liegende Werte anzupassen. Wählen Sie andernfalls **Nein** aus.

Die Parameter der einzelnen DQM-Regeln legen fest, wie unter dem Standard liegende Datenwerte angepasst werden.

Status Wählen Sie in der Dropdown-Liste **Aktiv** aus, um anzugeben, dass diese DQM-Regel aktiv ist. Wählen Sie andernfalls **Inaktiv** aus.

Konfigurieren von Suchcodes

Suchcodes sind Standardwerte, die von verschiedenen Funktionen der Anwendung verwendet werden.

Suchcodes sind nach Codetypen klassifiziert. Mit der DQM-Regel 190 können Sie prüfen, ob eingehende Suchcodes Teil eines definierten Codetyps sind. Sie können sie diesem Codetyp optional hinzufügen, wenn sie fehlen.

Anzeigen von Suchcodes

Suchcodes sind Standardwerte, die von verschiedenen Funktionen der Anwendung verwendet werden.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Codes** an.
4. Wählen Sie in der Dropdown-Liste **Typ** den Typ der Suchcodewerte aus, den Sie anzeigen wollen.

Erstellen von Suchcodes

Suchcodes sind Standardwerte, die von verschiedenen Funktionen der Anwendung verwendet werden.

Informationen zu diesem Vorgang

Sie können einen vollständig neuen Suchcode erstellen oder einen Suchcode, der auf einem vorhandenen Suchcode basiert.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Codes** an.
4. Wählen Sie in der Dropdown-Liste **Typ** den Typ des Suchcodewerts aus, den Sie erstellen wollen. Zum Erstellen eines vollständig neuen Suchcodetyps lassen Sie den Wert unverändert.
5. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie die Schaltfläche **Neu** an, um einen vollständig neuen Suchcode zu erstellen.
- Wählen Sie einen Suchcode in der Liste aus und klicken Sie anschließend die Schaltfläche **Klonen** an, um einen Suchcode auf der Basis eines vorhandenen Suchcodes zu erstellen.

6. Geben Sie auf der Registerkarte **Allgemein** den Typ (dieses Feld ist ein Anzeigefeld, wenn der Typ bereits in der Dropdown-Liste **Typ** angegeben wurde), den Code, die Beschreibung, den Status und sonstige Konfigurationsdaten für diesen Suchcode an.

Löschen von Suchcodes

Sie können von Benutzern erstellte Suchcodes löschen, die nicht mehr verwendet werden.

Informationen zu diesem Vorgang

Sie sollten keine Systemstandardsuchcodes löschen, da diese für verschiedene Komponenten des Produkts erforderlich sind.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Codes** an.
4. Wählen Sie in der Dropdown-Liste **Typ** den Typ der Suchcodewerte aus, die Sie löschen wollen.
5. Wählen Sie in der Liste einen Suchcode aus und klicken Sie anschließend die Schaltfläche **Löschen** an.

Inaktivieren von Suchcodes

Sie können einen Suchcode inaktivieren, der nicht mehr benötigt wird.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Codes** an.
4. Wählen Sie in der Dropdown-Liste **Typ** den Typ der Suchcodewerte aus, den Sie inaktivieren wollen.
5. Wählen Sie einen Suchcode in der Liste aus.
6. Setzen Sie das Statusfeld auf der Registerkarte **Allgemein** auf **Inaktiv**.
7. Klicken Sie die Schaltfläche **Speichern** an.

Hilfethemen

Suchcodes - Registerkarte 'Allgemein':

Über die Registerkarte **Allgemein** können Sie die Details für den Suchcode angeben.

Typ Geben Sie den Suchcodetyp an, dem der Suchcode zugeordnet ist. Nachdem dieses Feld einmal angegeben wurde, ist es schreibgeschützt. Es kann nur bearbeitet werden, wenn in der Dropdown-Liste **Typ** beim Erstellen eines neuen Suchcodes keine Angabe vorgenommen wurde.

Code Geben Sie den Wert an, der als Standardwert für den Suchcode verfügbar

sein soll. In der Regel ist dies ein Wert, der tatsächlich in UMF-Tags verwendet wird und in Datenbanktabellen gespeichert ist. Beim Bearbeiten vorhandener Suchcodes ist dieses Feld schreibgeschützt.

Beschreibung
Geben Sie die Beschreibung des Suchcodes ein.

Status Wählen Sie in der Dropdown-Liste **Aktiv** aus, um anzugeben, dass dieser Suchcode aktiv ist. Wählen Sie andernfalls **Inaktiv** aus.

Suchcodes - Feld 'Typ':

Über das Feld **Typ** können Sie den Typ angeben, dem der Suchcode zugeordnet ist.

ADDR_STAT
Dieser Suchcodetyp wird für Adressstatuswerte verwendet. Mit diesen Werten können bestimmte Adressen mit Informationen markiert werden, die beispielsweise angeben, ob es sich um eine Lieferadresse handelt.

ADDR_TYPE
Benutzerdefinierbare Klassifikationen für Adressen. Dies sind die gültigen Werte für den UMF-Tag `ADDR_TYPE`.

ANALYZER_GROUP
Dieser Suchcodetyp wird für Rollenalertregeln und Visualizer verwendet. Ein neuer Suchcode mit dem Typ ANALYZER_GROUP ist als Option in der Dropdown-Liste **Alertgruppe** der Registerkarte **Allgemein** verfügbar, die über **Konfiguration** > **Beziehungen** > **Rollenalertregeln** aufgerufen wird. Außerdem ist ein solcher Suchcode in der Dropdown-Liste **Gruppe** der Registerkarte **Allgemein** verfügbar, die über **Konfiguration** > **Visualizer** > **Visualizer-Benutzer** aufgerufen wird.

ATTR_CLASS
Benutzerdefinierbare Klassifikationen für Merkmaltypen. Hier eingegebene Werte sind als Optionen in der Dropdown-Liste **Klasse** der Registerkarte **Allgemein** verfügbar, die über **Konfiguration** > **Quellen** > **Merkmale** aufgerufen wird. Merkmale, die den Suchcode LINK als Attributklasse verwenden, können in Visualizer als HTML-Link angezeigt werden, wenn der Merkmalwert das folgende Format aufweist:

Linkanzeigetext=URL

ATTR_MATCH_LEVEL
Dieser Suchcodetyp wird nicht weiter unterstützt.

CONF_LEVEL
Dieser Suchcodetyp wird nicht weiter unterstützt.

DENSITY_LOG_LEVEL
Dieser Suchcodetyp wird nicht weiter unterstützt.

DOC_TYPE
Dieser Suchcodetyp wird nicht weiter unterstützt.

DSRC_ACTION
Dieser Suchcode wird vom System verwendet und darf nicht modifiziert werden.

EX_CLASS
Dieser Suchcode wird vom System verwendet und darf nicht modifiziert werden.

EX_SEVERITY
Dieser Suchcode wird vom System verwendet und darf nicht modifiziert werden.

LOG_LEVEL
Dieser Suchcode wird vom System verwendet und darf nicht modifiziert werden.

ER_LEVEL
Dieser Suchcode wird vom System verwendet und darf nicht modifiziert werden.

ER_LOG_LEVEL
Dieser Suchcode wird vom System verwendet und darf nicht modifiziert werden.

LDR_MESSAGE_TYPE
Dieser Suchcodetyp wird nicht weiter unterstützt.

MM_STAT
Dieser Suchcodetyp wird nicht weiter unterstützt.

NAME_TYPE
Dieser Suchcodetyp wird zum Speichern von benutzerdefinierbaren Klassifikationen für Namen verwendet. Dies sind die gültigen Werte für den UMF-Tag `NAME_TYPE`.

NS-FGEN
Dieser Suchcode wird vom System verwendet und darf nicht modifiziert werden.

NS-LGEN
Dieser Suchcode wird vom System verwendet und darf nicht modifiziert werden.

NS-PREFIX
Dieser Suchcode wird vom System verwendet und darf nicht modifiziert werden.

NS-SUFFIX
Dieser Suchcode wird vom System verwendet und darf nicht modifiziert werden.

NUM_CLASS
Dieser Suchcodetyp wird zum Speichern von benutzerdefinierbaren Klassifikationen für Nummerntypen verwendet. Hier eingegebene Werte sind als Optionen in der Dropdown-Liste **Klasse** der Registerkarte **Allgemein** verfügbar, die über **Konfiguration** > **Quellen** > **Nummern** aufgerufen wird.

REC_STAT
Dieser Suchcode wird vom System verwendet und darf nicht modifiziert werden.

SEARCH_REASON
Dieser Suchcode wird von Visualizer für eine Liste von Dropdown-Optionen verwendet, die für das Ursachenfeld für die Attributalertsuche zur Verfügung stehen. Benutzer können hier eine eigene Liste gültiger Ursachen für Attributalerts hinzufügen.

SYS_DELETE_STAT
Dieser Suchcode wird vom System verwendet und darf nicht modifiziert werden.

UNIQUE_FLAG
Dieser Suchcodetyp wird nicht weiter unterstützt.

USABILITY_LOG_LEVEL
Dieser Suchcode wird vom System verwendet und darf nicht modifiziert werden.

Konfigurieren generischer Datenwerte

Sie können Datenwerte als generisch konfigurieren, wenn sie eine angegebene Anzahl von Vorkommen in der Entitätendatenbank überschreiten.

Generische Werte

Generische Werte beschreiben Datenwerte, die wiederholt in der Entitätendatenbank auftreten und daher vom System nicht mehr für die Entitätsauflösung verwendet werden.

Datenwerte werden als generisch betrachtet, wenn sie einen bestimmten Schwellenwert überschreiten. Der Schwellenwert ist eine konfigurierte maximale Anzahl Entitätsvorkommen in der Entitätendatenbank, die den Datenwert gemeinsam haben können.

Generische Werte sind nach Attribut und Attributtyp organisiert und konfiguriert. Der generische Datenwert eines bestimmten Attributtyps überschreibt den generischen Datenwert des übergeordneten Attributs. Die Werte folgender Standarddatenelemente können als generisch betrachtet werden:

- Adresse
- Merkmal
- E-Mail
- Name
- Nummer

Beispiel

Wenn der generische Schwellenwert für Telefonnummern auf 25 gesetzt ist und ein Telefonnummernwert (wie z. B. 0555-555-5555) für mehr als 25 Entitäten gilt, wird dieser bestimmte Wert ab dieser Zeit nicht mehr zum Auflösen von Entitäten verwendet.

Anmerkung: Berücksichtigen Sie beim Festlegen von generischen Schwellenwerten, dass ein zu hoher Schwellenwert eventuell die Systemleistung beeinträchtigt, weil er zu einer Flut von Daten führen kann, die generisch sein sollten. Ein zu niedriger generischer Schwellenwert hingegen führt eventuell dazu, dass wichtige Alerts nicht generiert werden, weil Schlüsselkriterien als generisch betrachtet werden.

Anzeigen von generischen Datenwerten

Generische Datenwerte sind Schwellenwerte für generische Daten für jedes Datenelement, das Sie als generisch ansehen wollen. Möglicherweise wollen Sie vorhandene generische Daten anzeigen, wenn Sie eine neue Datenquelle hinzufügen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **Schwellenwert für generische Daten** an.

Konfigurieren generischer Datenwerte

Damit generische Werte bei der Entitätsauflösung ignoriert werden, müssen Sie für das Datenelement einen Schwellenwert für generische Daten konfigurieren.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **Schwellenwert für generische Daten** an.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie die Schaltfläche **Neu** an, um einen vollständig neuen generischen Datenwert zu erstellen.
   - Wählen Sie einen generischen Datenwert in der Liste aus und klicken Sie anschließend die Schaltfläche **Klonen** an, um einen generischen Datenwert auf der Basis eines vorhandenen generischen Datenwerts zu erstellen.
5. Geben Sie auf der Registerkarte **Allgemein** das Attribut, den Attributtyp und den Schwellenwert des generischen Werts an.
6. Klicken Sie die Schaltfläche **Speichern** an.

Löschen von generischen Datenwerten

Generische Datenwerte sind Schwellenwerte für generische Daten für jedes Datenelement, das Sie als generisch ansehen wollen. Sie können vorhandene generische Datenwerte löschen, wenn sie für eingehende Daten nicht mehr relevant sind.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **Schwellenwert für generische Daten** an.
4. Wählen Sie das Kontrollkästchen neben dem Namen eines beliebigen, vorhandenen Elements aus, den Sie löschen wollen.
5. Klicken Sie die Schaltfläche **Löschen** an.

Hilfethemen

Schwellenwert für generische Daten - Registerkarte 'Allgemein':

Über die Registerkarte **Allgemein** können Sie die Details für den generischen Datenwert angeben.

Attributname
Wählen Sie in der Dropdown-Liste das Attribut aus, auf das der generische Datenwert angewendet werden soll.

Attributtyp
Wählen Sie in der Dropdown-Liste den Attributtyp aus, auf den der generische Datenwert angewendet werden soll.

Diese Dropdown-Liste enthält nur dann mehrere Optionen, wenn das Feld **Attributname** auf Name oder Merkmal gesetzt ist.

Schwellenwert
Geben Sie die Anzahl der Entitäten ein, die denselben UMF-Wert des konfigurierten Typs haben können, bevor er als generisch gilt.

Konfigurieren von Rollen

Sie können Rollen konfigurieren, um Entitäten in der Entitätendatenbank zu klassifizieren. Rollen können Datenquellen oder Entitäten zugeordnet werden. Bei zueinander in Konflikt stehenden Rollen werden Alerts generiert.

Informationen zu diesem Vorgang

Rollen können über die Registerkarte **Datenquellen** der Konsole angezeigt und modifiziert werden.

Rollen

Eine Rolle ist eine Klassifizierung einer Identität, die den Fokus oder den Zweck dieser Identität definiert. Sie können einer Identität mehr als eine Rolle zuordnen. Beim Auflösen von Identitäten in Entitäten übernehmen Entitäten alle zugeordneten Rollen.

Mit Rollen konfigurieren Sie Rollenalertregeln, die Beziehungen von Interesse definieren und Alerts generieren.

Es gibt zwei Methoden, eine Identität einer Rolle zuzuweisen:

Nach eingehender Datenquelle
: Wenn Sie eine neue Datenquelle konfigurieren, ordnen Sie dieser Datenquelle eine Rolle zu. Die Datenquelle weist diese Rolle allen Identitäten zu, die den entsprechenden Code für die Datenquelle enthalten.

Nach UMF
: Wenn Sie die Datenquelle in UMF (Universal Message Format) umsetzen, können Sie Rollen direkt als Teil des UMF-Datensatzes zuordnen. Verwenden Sie hierzu das UMF-Segment <SEP_ROLES> mit dem UMF-Tag <ROLE_CODE>. Wenn Sie nach UMF konfigurieren, müssen Sie DQM-Regeln und eine Suchtabelle hinzufügen.

Beispiele nützlicher Rollen sind Mitarbeiter, Lieferanten, Kunden oder Überwachungslisten.

Beispiel für das Zuordnen von Rollen mit UMF

Wenn Sie die Rolle 'Mitarbeiter' einem Identitätsdatensatz mithilfe von UMF zuordnen wollen, geben Sie das folgende UMF-Segment <SEP_ROLES> und den folgenden UMF-Tag <ROLE_CODE> für den Identitätsdatensatz ein:

```
<SEP_ROLES>

    <ROLE_CODE>Mitarbeiter</ROLE_CODE>

</SEP_ROLES>
```

Anzeigen von Rollen

Eine Rolle definiert, wie eine Entität im System klassifiziert wird oder bekannt ist. Möglicherweise wollen Sie vorhandene Rollen anzeigen, wenn Sie planen, eine neue Rolle hinzuzufügen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Beziehungen** an.
3. Klicken Sie die Registerkarte **Rollencodes** an.

4. Wählen Sie die Rolle aus, die Sie anzeigen wollen.

Erstellen von Rollen

Erstellen Sie Rollen im System, um zu definieren, wie Entitäten zu anderen Entitäten in Beziehung stehen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Beziehungen** an.
3. Klicken Sie die Registerkarte **Rollencodes** an.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie die Schaltfläche **Neu** an, um eine vollständig neue Rolle zu erstellen.
   - Wählen Sie eine Rolle in der Liste aus und klicken Sie anschließend die Schaltfläche **Klonen** an, um eine Rolle auf der Basis einer vorhandenen Rolle zu erstellen.
5. Geben Sie auf der Registerkarte **Allgemein** den Rollencode, die Beschreibung, die Klasse, den Status und sonstige Konfigurationsdaten für die neue Rolle an.
6. Klicken Sie die Schaltfläche **Speichern** an.

Nächste Schritte

Sie können diese Rolle beim Definieren von Rollenalertregeln verwenden.

Löschen von Rollen

Eine Rolle definiert, wie eine Entität im System klassifiziert wird oder bekannt ist. Es empfiehlt sich möglicherweise, eine vorhandene Rolle zu löschen, wenn sie nicht mehr gültig ist.

Informationen zu diesem Vorgang

Sie können eine Rolle nicht löschen, wenn sie von einer Rollenalertregel oder einer Datenquelle verwendet wird.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Beziehungen** an.
3. Klicken Sie die Registerkarte **Rollencodes** an.
4. Wählen Sie das Kontrollkästchen neben einer beliebigen, vorhandenen Rolle aus, die Sie löschen wollen.
5. Klicken Sie die Schaltfläche **Löschen** an.

Hilfethemen

Rollen - Registerkarte 'Allgemein':

Über die Registerkarte **Allgemein** können Sie die Details für die Rolle angeben.

ID Geben Sie die eindeutige ganze Zahl ein, die die Rollen-ID kennzeichnet.

Der ID-Wert wird automatisch mit der nächsten fortlaufenden Zahl gefüllt, die nicht verwendet wird.

Rollencode
Geben Sie einen eindeutigen Wert ein, der diese Rolle kennzeichnet.

Beschreibung
Geben Sie eine Beschreibung für diese Rolle ein.

Rollenklasse
Geben Sie eine Rollenklasse für diese Rolle ein.

Status Wählen Sie in der Dropdown-Liste **Aktiv** aus, um anzugeben, dass diese Rolle aktiv ist. Wählen Sie andernfalls **Inaktiv** aus.

Konfigurieren von Rollenalertregeln

Sie können Rollenalertregeln konfigurieren, um eine Kombination von Rollen zu definieren, bei deren Feststellung Alerts generiert werden.

Informationen zu diesem Vorgang

Rollenalertregeln können über die Registerkarte **Rollenalertregeln** der Konsole angezeigt und modifiziert werden.

Rollenalert

Ein Rollenalert wird im System durch eine Rollenalertregel definiert, die Beziehungen darstellt, mit denen Alerts generiert werden.

Rollenalertregeln definieren eine Kombination aus Rollen, die beim Erkennen in einer Beziehung oder Entität auf einen Konflikt in irgendeiner Form schließen lässt. So kann eine Rollenalertregel z. B. angeben, dass grundsätzlich ein Rollenalert vorhanden ist, wenn eine Entität in der Rolle 'Mitarbeiter' eine Entität in der Rolle 'Lieferant' kennt. Diese Rollenalertregel kann als 'Mitarbeiter kennt Lieferanten' beschrieben werden. Wenn das System Rollenalerts in Entitäten oder Beziehungen feststellt, werden Alerts erstellt, die im Unternehmen veröffentlicht und in den Analyst Toolkit-Anwendungen angezeigt werden können.

Obwohl in den meisten Rollenalertregeln eine Kombination aus zwei unterschiedlichen Rollen angegeben wird, die auf einen Konflikt hinweisen, kann eine Rollenalertregel auch vorhanden sein, wenn sich zwei Entitäten derselben Rolle kennen. Beispielsweise kann es für Sie von Interesse sein, Beziehungen zwischen Ihren Kunden zu kennen und eine Rollenalertregel zu erstellen, die jedes Mal einen Rollenalert generiert, wenn eine Kundenentität in Beziehung zu einer anderen Kundenentität tritt. Diese Rollenalertregel kann als 'Kunde kennt Kunde' beschrieben werden.

Rollenalertregeln basieren auf vorhandenen Rollencodes. Die Rollen müssen definiert werden, bevor Sie Konfliktregeln für die Rollen erstellen können.

Anzeigen von Rollenalertregeln

Eine Rollenalertregel wird zum Generieren von Alerts verwendet, wenn eine Beziehung zwischen zwei definierten Rollen erkannt wird. Möglicherweise wollen Sie vorhandene Rollenalertregeln anzeigen, wenn Sie planen, eine neue Rollenalertregel hinzuzufügen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Beziehungen** an.
3. Klicken Sie die Registerkarte **Rollenalertregeln** an.
4. Wählen Sie die Rollenalertregel aus, die Sie anzeigen wollen.

Konfigurieren von Rollenalertregeln

Sie können Rollenalertregeln konfigurieren, um Rollenalerts oder Beziehungen zwischen zwei Rollen oder Identitäten zu generieren.

Vorbereitende Schritte

Vor dem Definieren einer Rollenalertregel müssen Sie zunächst die Rollen konfigurieren, die Sie in der Rollenalertregel verwenden wollen. Wenn Sie z. B. eine Rollenalertregel konfigurieren wollen, bei der ein Mitarbeiter kein Lieferant sein kann, muss Ihr System die Rollen 'Mitarbeiter' und 'Lieferant' enthalten.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** an.
2. Klicken Sie die Schaltfläche **Beziehungen** an.
3. Klicken Sie die Registerkarte **Rollenalertregeln** an.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie die Schaltfläche **Neu** an, um eine vollständig neue Rollenalertregel zu erstellen.
   - Wählen Sie eine Rollenalertregel in der Liste aus und klicken Sie anschließend die Schaltfläche **Klonen** an, um eine Rollenalertregel auf der Basis einer vorhandenen Rollenalertregel zu erstellen.

   Das Feld **Rollenalertregel-ID** wird automatisch mit der nächsten eindeutigen ID gefüllt. Sie können diesen Wert in eine beliebige eindeutige ID-Nummer ändern.
5. Klicken Sie die Schaltfläche **Neu** an.
6. Geben Sie auf der Registerkarte **Allgemein** die ID, die Beschreibung, die Wertigkeit, die Rollencodes, die Alertgruppe und den Mindestgrenzwert für Alerts für diese Rollenalertregel an.
7. Geben Sie auf der Registerkarte **Filter** optional den Identitätsfilter, den Datenänderungsfilter und die Pfadrelevanzanpassung an. (Das Feld für die Pfadrelevanzanpassung wird nur angezeigt, wenn das Feld für den Datenänderungsfilter auf Pfadrelevanzanpassung gesetzt ist.) Wenn beide Filter gesetzt sind, müssen nur die Kriterien eines Filters erfüllt werden, damit ein Rollenalert generiert wird.
8. Klicken Sie die Schaltfläche **Speichern** an.

Löschen von Rollenalertregeln

Sie sollten eine Rollenalertregel löschen, wenn eine in der Rollenalertregel angegebene Rolle gelöscht wird oder wenn die Rollenkombination in der Rollenalertregel nicht mehr von Interesse ist.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Beziehungen** an.
3. Klicken Sie die Registerkarte **Rollenalertregeln** an.
4. Wählen Sie das Kontrollkästchen neben einer beliebigen, vorhandenen Rollenalertregel aus, die Sie löschen wollen.
5. Klicken Sie die Schaltfläche **Löschen** an.

Hilfethemen

Rollenalertregeln - Registerkarte 'Allgemein':

Über die Registerkarte **Allgemein** im Fenster **Rollenalertregeln** können Sie die Details der Rollenalertregeln konfigurieren. Rollen sind Datenquellen zugeordnet. Jeder Identität, die aus einer Datenquelle im System aufgenommen wird, wird eine Rolle zugeordnet, basierend auf der Konfiguration der Datenquelle. Rollenalertregeln definieren, wann ein Rollenalert aufgrund eines Konflikts zwischen den Rollen der aufgenommenen Identitäten und der Rollen der Identitäten, die Entitäten in der Entitätendatenbank zugeordnet sind, generiert wird.

Rollenalertregel-ID
Der ID-Wert wird automatisch mit der nächsten fortlaufenden Zahl gefüllt, die nicht verwendet wird.

Beschreibung
Geben Sie eine Beschreibung für diese Rollenalertregel ein. Dieser Text wird in Visualizer angezeigt, wenn ein Rollenalert basierend auf dieser Rollenalertregel generiert wird.

Wertigkeit
Ein benutzerdefinierter, aus einem Zeichen bestehender Code, der den Stellenwert der Alerts kategorisiert, die aufgrund diese Regel generiert werden.

Stimmen Sie die Wertigkeit des Rollenalerts auf den Stellenwert ab. Dieser Code wird zusammen mit den aufgrund dieser Rollenalertregel generierten Rollenalerts in Visualizer angezeigt. Analysten verwenden die Wertigkeit um anzugeben, welche Alerts vorrangig überprüft werden sollen. Der aus einem Zeichen bestehende Code sollte daher für Benutzer von Visualizer möglichst aussagekräftig sein. So wäre eine Rollenalertregel, die einen Alert generiert, sobald ein Passagier mit einer Person auf der No-Fly-Liste übereinstimmt, z. B. kritischer, als eine Rollenalertregel, die einen Alert generiert, wenn ein Mitarbeiter einen Kunden kennt.

Beispiele für Codes für die Wertigkeit sind: C für Kritisch (Critical), N für Neutral (Neutral), I für Interessant (Interesting), H für Hoch (High) oder L für Niedrig (Low).

Rolle 1
Wählen Sie in der Dropdown-Liste die erste Rolle zum Vergleich in dieser Rollenalertregel aus.

Es werden die vorhandenen, konfigurierten Rollen angezeigt. Wird die Rolle nicht angezeigt, die Sie auswählen wollen, konfigurieren Sie sie zunächst über die Registerkarte **Rollen**.

Rolle 2
Wählen Sie in der Dropdown-Liste die zweite Rolle zum Vergleich in dieser Rollenalertregel aus.

Es werden die vorhandenen, konfigurierten Rollen angezeigt. Wird die Rolle nicht angezeigt, die Sie auswählen wollen, konfigurieren Sie sie zunächst über die Registerkarte **Rollen**.

Alertgruppe
Wählen Sie in der Dropdown-Liste die Visualizer-Analysegruppe aus, die die Rollenalerts analysiert, die aufgrund dieser Rollenalertregel generiert werden. Sie könnten z. B. alle für Passagiere in der No-Fly-Liste generier-

ten Rollenalerts an einen Sicherheitsdienst und alle Rollenalerts zur Beziehung zwischen Mitarbeiter und Lieferant an die Personalabteilung weiterleiten.

Es werden die aktiven, konfigurierten Visualizer-Analysegruppen mit dem Codetyp ANALYZER_GROUP angezeigt. Wird die Gruppe nicht angezeigt, die Sie auswählen wollen, konfigurieren Sie zunächst über die Registerkarte **Konfiguration - Allgemein - Codes** einen neuen Code ANALYZER-_GROUP.

Da es sich hierbei um ein erforderliches Feld handelt, müssen Sie einen Altertgruppencode konfigurieren und auswählen, auch wenn Visualizer in Ihrem Unternehmen nicht verwendet wird.

Rollenalertregeln:

Wenn beide Filter gesetzt sind, müssen nur die Kriterien eines Filters erfüllt werden, damit ein Rollenalert generiert wird.

Identitätsfilter
Wählen Sie in der Dropdown-Liste einen Filter aus, um die Rollenalertgenerierung zu beschränken, wenn den am Rollenalert beteiligten Entitäten neue Identitäten hinzugefügt werden.

Dieser Filter beeinflusst nur das Verhalten für die erneute Benachrichtigung. Wenn die Rollenalertregel zum ersten Mal für eine angegebene Gruppe von Entitäten erfüllt ist, wird immer ein Rollenalert generiert. Dieser Filter kann verhindern, dass wiederholt derselbe Rollenalert generiert wird, wenn an den betroffenen Entitäten Änderungen vorgenommen werden.

Aus Wählen Sie diesen Feldtyp aus, um die Rollenalertbeschränkung zu inaktivieren, wenn den am Rollenalert beteiligten Entitäten neue Identitäten hinzugefügt werden.

Neue Identität
Wählen Sie diesen Feldtyp aus, um nur dann neue Alerts zu generieren, wenn bei den Identitäten neue Datenquellencodes in die am Rollenalert beteiligten Entitäten eingeführt werden.

Neuer Datenquellencode
Wählen Sie diesen Feldtyp aus, um Alerts zu generieren, wenn bei den Identitäten ein neuer Datenquellencode eingeführt wird.

Datenänderungsfilter
Wählen Sie in der Dropdown-Liste einen Filter aus, um die Rollenalertgenerierung zu beschränken, wenn den am Rollenalert beteiligten Entitäten neue attributive Daten hinzugefügt werden.

Dieser Filter beeinflusst nur das Verhalten für die erneute Benachrichtigung. Wenn die Rollenalertregel zum ersten Mal für eine angegebene Gruppe von Entitäten erfüllt ist, wird immer ein Rollenalert generiert. Dieser Filter kann verhindern, dass wiederholt derselbe Rollenalert generiert wird, wenn an den betroffenen Entitäten Änderungen vorgenommen werden.

Aus Wählen Sie diesen Feldtyp aus, um die Rollenalertbeschränkung zu inaktivieren, wenn den am Rollenalert beteiligten Entitäten neue attributive Daten hinzugefügt werden.

Neue attributive Daten
Wählen Sie diesen Feldtyp aus, um nur dann neue Alerts zu generieren, wenn den am Rollenalert beteiligten Entitäten neue attributive Daten hinzugefügt werden.

Pfadrelevanzanpassung
Wählen Sie diesen Feldtyp aus, um nur dann neue Alerts zu generieren, wenn neue attributive Daten hinzugefügt werden, die eine Änderung der Pfadrelevanz bewirken, die größer-gleich dem Wert **Pfadrelevanzanpassung** ist.

Pfadrelevanzanpassung
Dieses Feld wird nur angezeigt, wenn die Dropdown-Liste **Datenänderungsfilter** auf Pfadrelevanzanpassung gesetzt ist. Geben Sie einen Anpassungswert (-100 bis 100) ein, der verwendet werden soll, wenn **Datenänderungsfilter** auf Pfadrelevanzanpassung gesetzt ist. Damit werden Rollenalerts nur dann erneut generiert, wenn neue attributive Daten hinzugefügt werden, die eine Änderung der Pfadrelevanz bewirken, die größergleich dem Wert für die Pfadrelevanzanpassung ist. Die Angabe von Null ist gleichbedeutend mit einem Inaktivieren des Filters.

Konfigurieren von Entitätstypen

Sie können Entitätstypen konfigurieren, um den genauen Typ der Entität zu kennzeichnen.

Informationen zu diesem Vorgang

Wenn einer Datenquelle neue Identitätsdaten hinzugefügt werden und Sie diese Daten als einen Entitätstyp klassifizieren wollen, der noch nicht im System konfiguriert ist, müssen Sie einen neuen Entitätstyp für die neuen Daten erstellen.

Entitätstypen können über die Registerkarte **Entitätstypen** der Konsole angezeigt und modifiziert werden.

Entitätstypen

Entitätstypen sind benutzerdefinierte Eigenschaften, die einer Entität zugeordnet sind, um deren genaue Spezifik anzugeben.

Impersonal Awareness verwendet Entitätstypen zum Verknüpfen von Entitäten, die andernfalls keine einstufige Beziehung aufweisen würden.

Wenn Sie z. B. unpersönliche Beziehungen mithilfe von Telefonanrufen ermitteln wollen, könnten Sie einen neuen Entitätstyp namens *Telefonanruf* erstellen und Ihren Übernahmeknoten so anpassen, dass jeder Datensatz für Telefonanrufe ordnungsgemäß mit dem Entitätstyp *Telefonanruf* gekennzeichnet wird.

Wenn die Datensätze mit den Telefonanrufen in die Pipelines aufgenommen werden, findet der Prozess zur Auflösung von Entitäten und Beziehungen eine einstufige Beziehung zwischen der Entität mit dem Typ *Telefonanruf* und der Entität, die den Anruf getätigt hat (*Person*). Das Programm findet auch eine einstufige Beziehung zwischen der angerufenen Person und der Entität *Telefonanruf*. Das System ist nicht in der Lage, selbstständig eine einstufige Beziehung zwischen den beiden Personen zu finden.

```
<UMF_ENTITY>
<DSRC_CODE>100</DSRC_CODE>
<DSRC_ACCT>123abc</DSRC_ACCT>
<DSRC_REF>1</DSRC_REF>
```

```
<ENTITY_TYPE>PHONE</ENTITY_TYPE>
<NUMBER>
<NUM_TYPE>PH</NUM_TYPE>
<NUM_VALUE>702-555-1212</NUM_VALUE>
</NUMBER>
</UMF_ENTITY>
```

Impersonal Awareness

Impersonal Awareness ist eine Produktkomponente, die den traditionellen Beziehungsauflösungsprozess um das Suchen und Analysieren unpersönlicher Beziehungen erweitert. Der Beziehungserkennungsprozess findet Beziehungen zwischen Entitäten auf der Grundlage von Attributwerten, die den Entitäten zugeordnet sind. Manchmal ist es wichtig, Beziehungen zwischen Entitäten zu finden, die auf Aktivitäten oder anderen unpersönlichen Kennungen basieren. Diese auf Aktivitäten oder anderen unpersönlichen Kennungen basierenden Beziehungen zwischen Entitäten werden als *unpersönliche* Beziehungen bezeichnet. Aktivitäten oder unpersönliche Kennungen, die Beziehungen zwischen Personen darstellen, werden *Zuordnungsfakten* genannt.

Unpersönliche Beziehungen sind immer bei mehrstufigen Beziehungen mit mindestens zwei Abgrenzungsgraden vorhanden, weil das Zuordnungsfaktum selbst eine Entität darstellt. Wenn Sie Impersonal Awareness aktivieren und unpersönliche Beziehungen finden wollen, müssen Sie also Ihre Datenquellen für die Verwendung von Degrees of Separation konfigurieren. Diese Komponente erweitert die Entitäts- und Beziehungsauflösung, sodass auch Beziehungen mit mehreren Abgrenzungsgraden gefunden werden.

Beispielsweise enthält eine Telefontransaktion Daten zu Telefonnummern, und zwar die anrufende Nummer sowie die empfangende Nummer. Obwohl eine Person eine andere Person angerufen hat, können diesen Personen allein auf Grundlage der Telefontransaktion keine gemeinsamen Daten zugewiesen werden. Oft ist das Zuordnungsfaktum (der Telefonanruf) schon bekannt, bevor andere Informationen zu den zusammengehörigen Entitäten (die beiden Personen, die das Telefongespräch führten) bekannt sind. Da die Zuordnungsfakten keiner Person zugeordnet werden können, müssen sie als eigenständige Entitäten dargestellt werden, die keine Personen sind, sich aber auf Personen beziehen. Mithilfe von Impersonal Awareness kann jedoch anhand des Telefonanrufs erkannt werden, dass eine Beziehung zwischen zwei Personen vorhanden ist.

UMF beinhaltet eine Funktionalität für Entitätstypen, die es Ihnen ermöglicht, Zuordnungsfakten als Entitätstypen zu definieren. Bei Verwendung dieser Funktionalität werden Zuordnungsfakten in der Entitätendatenbank zu eigenständigen Entitäten. Sie können dann dazu verwendet werden, Beziehungen zwischen Entitäten des Typs 'Person' zu ermitteln. Durch das Konfigurieren neuer Entitätstypen, durch Angeben der entsprechenden Entitätstypen in UMF und durch das Erstellen neuer Auflösungskonfigurationen können diese Zuordnungsfakten dazu verwendet werden, unpersönliche Beziehungen und Konflikte zwischen Entitäten automatisch zu suchen.

Entitäten verschiedener Entitätstypen können nicht typenübergreifend aufgelöst werden, auch wenn die Auflösungsregeln es zulassen und sogar die Daten eine Auflösung unterstützen. Das bedeutet, dass ein Entitätstyp 'Telefonanruf' niemals in einen Entitätstyp 'Person' aufgelöst werden kann.

Analyst Toolkit stellt unpersönliche Beziehungen und zugeordnete Alerts grafisch dar und listet sie auf, wie dies bei persönlichen Beziehungen und zugeordneten Alerts der Fall ist.

Beispiel für Impersonal Awareness

Wenn Sie z. B. unpersönliche Beziehungen unter Verwendung von Telefonanrufen ermitteln wollten, dann würden Sie einen neuen Entitätstyp 'Telefonanruf' erstellen und Ihren Übernahmeknoten so anpassen, dass jeder Telefonanrufdatensatz mit dem Entitätstypentag *Telefonanruf* gekennzeichnet wird.

Wenn die Datensätze mit den Telefonanrufen in das System aufgenommen wird, findet die Standardauflösung für Entitäten und Beziehungen eine einstufige Beziehung zwischen der Entität mit dem Typ 'Telefonanruf' und der Entität, die den Anruf getätigt hat (Person). Das Programm findet auch eine einstufige Beziehung zwischen der angerufenen Person und der Entität 'Telefonanruf'. Das System findet keine Beziehung zwischen den beiden Personen.

Wenn jedoch Degrees of Separation konfiguriert ist, setzt diese Komponente die Analyse fort und erkennt die zweistufige unpersönliche Beziehung zwischen dem Anrufer und der angerufenen Person. Eine unpersönliche Beziehung ist vorhanden, und zwar auf der Basis der Telefonnummern, die Attribute des Entitätstyps 'Telefonanruf' sind. Degrees of Separation analysiert dann die unpersönliche Beziehung und generiert einen Alert, wenn ein Konflikt gefunden wird.

Anzeigen von Entitätstypen

Entitätstypen sind benutzerdefinierte Eigenschaften, die einer Entität zugeordnet sind, um deren genaue Spezifik anzugeben. Möglicherweise wollen Sie vorhandene Entitätstypen anzeigen, wenn Sie darüber nachdenken, einen neuen Entitätstyp hinzuzufügen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Registerkarte **Entitätstypen** an.
4. Wählen Sie den Entitätstyp aus, den Sie anzeigen wollen.

Erstellen von Entitätstypen

Entitätstypen sind benutzerdefinierte Eigenschaften, die einer Entität zugeordnet sind, um deren genaue Spezifik anzugeben. Möglicherweise empfiehlt es sich, dem System einen neuen Entitätstyp hinzuzufügen, wenn Sie dem System einen neuen Datentyp hinzufügen.

Vorbereitende Schritte

Bevor Sie einen neuen Entitätstyp erstellen, sollten Sie die eingehenden Identitätsdaten prüfen, um festzustellen, ob sie mit einem der vorhandenen Entitätstypen beschrieben werden können.

Informationen zu diesem Vorgang

Impersonal Awareness verwendet Entitätstypen zum Verknüpfen von Entitäten, die andernfalls keine einstufige Beziehung aufweisen würden.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Registerkarte **Entitätstypen** an.

4. Klicken Sie die Schaltfläche **Neu** an.
5. Geben Sie auf der Registerkarte **Allgemein** die ID, den Typ, die Beschreibung, die Entitätsauflösungskonfiguration und den Suchtyp für diesen Entitätstyp an. Geben Sie zudem an, ob der Entitätstyp für generische Zähler oder Rollenalerts verwendet wird und ob die Auflösung zulässig ist.
6. Klicken Sie die Schaltfläche **Speichern** an.

Ergebnisse

Das System kann nun Entitätstypen Daten zuordnen und Entitäten mithilfe von Impersonal Awareness verknüpfen, die andernfalls keine einstufige Beziehung aufweisen würden.

Löschen von Entitätstypen

Sie können einen vorhandenen Entitätstyp löschen, wenn er von der Entitätendatenbank nicht mehr verwendet wird.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Registerkarte **Entitätstypen** an.
4. Wählen Sie das Kontrollkästchen neben dem Merkmaltyp aus, den Sie löschen wollen.
5. Klicken Sie die Schaltfläche **Löschen** an.

Hilfethemen

Entitätstypen - Registerkarte 'Allgemein':

Über die Registerkarte **Entitätstypen** können Sie die Details für den Entitätstyp angeben.

ID Geben Sie die ID-Nummer des Entitätstyps ein, den Sie erstellen wollen.

Die ID ist ein numerischer Code, der sich automatisch erhöht. Das Programm stellt die nächste verfügbare Nummer in der Folge zur Verfügung, Sie können den Code allerdings auch als einen beliebigen eindeutigen numerischen Wert angeben, indem Sie den Wert in das Feld **ID** eingeben.

Typ Geben Sie den Namen des Entitätstyps ein, den Sie erstellen wollen.

Beispielsweise könnte der Entitätstyp Telefonanruf zur Beschreibung von Entitäten verwendet werden, bei denen es sich um Aufzeichnungen von Telefonanrufen zwischen zwei Identitäten handelt.

Beschreibung
Geben Sie die Beschreibung des Entitätstyps ein, den Sie erstellen wollen.

Entitätsauflösungskonfiguration
Wählen Sie in der Dropdown-Liste die Auflösungskonfiguration aus, die dieser Entitätstyp beim Laden verwendet.

Auflösungskonfigurationen werden in der Anzeige **Konfiguration** > **Auflösung** > **Auflösungskonfigurationen** definiert.

Verwendung für generischen Zähler
Wählen Sie in der Dropdown-Liste **Ja** aus, um anzugeben, dass die Daten dieses Entitätstyps in generische Daten konvertiert werden können. Wählen Sie andernfalls **Nein** aus.

Verwendung für Rollenalert
Wählen Sie in der Dropdown-Liste **Ja** aus, um anzugeben, dass die Daten dieses Entitätstyps Rollenalerts generieren können. Wählen Sie andernfalls **Nein** aus.

Suchtyp
Wählen Sie in der Dropdown-Liste **Ja** aus, um anzugeben, dass die Daten dieses Entitätstyps für Suchen verwendet werden können. Wählen Sie andernfalls **Nein** aus.

Auflösung zulassen
Wählen Sie in der Dropdown-Liste **Ja** aus, um anzugeben, dass die Daten dieses Entitätstyps zum Auflösen von Entitäten verwendet werden können. Wählen Sie andernfalls **Nein** aus.

Degrees of Separation - Übersicht

Die Komponente Degrees of Separation erweitert das Leistungsspektrum für den Beziehungsabgleich von IBM Relationship Resolution.

Standardmäßig identifiziert IBM InfoSphere Identity Insight potenziell interessante Beziehungen und führt einen Abgleich für Entitäten durch, die einen Abgrenzungsgrad von 1 zu einer eingehenden Identität haben, die in eine Entität aufgelöst wird. Die Aktivierung der Komponente Degrees of Separation erweitert diese Funktionalität auf beinahe uneingeschränkte benutzerdefinierte Angaben für den Abgrenzungsgrad von eingehenden Identitäten, die in Entitäten aufgelöst werden.

Die Komponente Degrees of Separation verwendet Abgrenzungskonfigurationen, Rollen, Rollenalertregeln und Beziehungsbewertungen, um Echtzeit-Link-Analysen für sehr umfangreiche Datenbestände durchzuführen.

Wenn eine eingehende Identität in eine Entität aufgelöst wird, wird ein Entitätsdiagramm erstellt, das die von IBM Relationship Resolution ermittelten einstufigen Beziehungen verwendet. Das Entitätsdiagramm verwendet die einstufigen Beziehungen, um mehrstufige Beziehungsketten zu erzeugen, die von der Entität ausgehen, in die die Identität aufgelöst wurde. Dann kann eine Rollenalertkette durch Verbinden zweier mehrstufiger Beziehungsketten erstellt werden, die jeweils von der Entität ausgehen, in die die eingehende Identität aufgelöst wurde. Die Rollenalertkette kann dann dazu verwendet werden, eine Beziehung zwischen den Entitäten am Ende und innerhalb der mehrstufigen Beziehungskette zu finden.

Degrees of Separation reduziert den Arbeitsaufwand, indem alle Pfade ausgewertet werden, die zwei Entitäten miteinander verbinden, wobei die höchste Pfadrelevanz zur Berichterstellung von Beziehungen verwendet wird. Degrees of Separation kann so konfiguriert werden, dass ein Rollenalert für jede konfigurierte Rollenalertregel pro Entität zurückgemeldet wird, in die die eingehende Identität aufgelöst wurde.

Die Konfiguration von Degrees of Separation kann auf der Registerkarte **Systemkonfiguration** der Konsole über den Wert für Abgrenzungsgrade festgelegt werden.

Beispiel für Abgrenzungsgrade

Dieses Beispiel führt Sie durch einen Beziehungspfad und verdeutlicht, welche Rolle die Konfigurationsfaktoren für Abgrenzungsgrade beim Ermitteln von Rollenalerts spielen.

Beispiel für Abgrenzungsgrade

Nach der Verarbeitung eingehender Daten meldet Identity Insight den folgenden Beziehungspfad zurück:

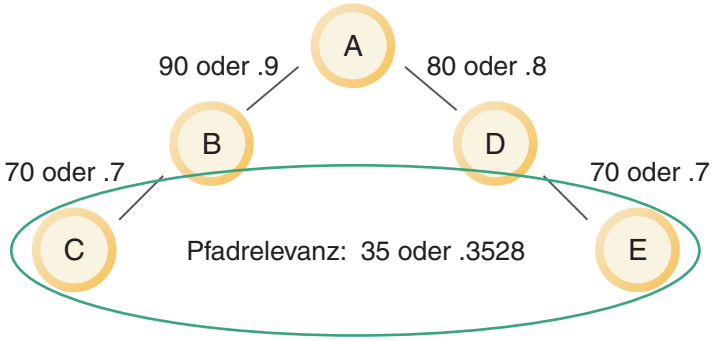
- Entität A kennt Entität B.
- Entität B kennt Entität C.
- Entität A kennt Entität D.
- Entität D kennt Entität E.

Ein *Beziehungspfad* ist die Kette der Entitäten und Attribute, die eine Entität mit einer anderen verknüpfen.

Identity Insight ermittelt die Relevanz des Beziehungspfads während der Verarbeitung der Beziehungs- und Rollenalerts. Die Pfadrelevanz ist das Produkt aus den Dezimalkonvertierungen der Beziehungsbewertung jeder Entität in der Kette, konvertiert in eine ganze Zahl.

In diesem Beispiel berechnet das Produkt die Beziehungsbewertungen und konvertiert diese in Dezimalzahlen:

- Der Beziehungsbewertung für Entität A ist bekannt, dass Entität B '90' ist. 90 wird in die Dezimalzahl 0.9 (0,9) konvertiert.
- Der Beziehungsbewertung für Entität B ist bekannt, dass Entität C '70' ist. 70 wird in die Dezimalzahl 0.7 (0,7) konvertiert.
- Der Beziehungsbewertung für Entität A ist bekannt, dass Entität D '80' ist. 80 wird in die Dezimalzahl 0.8 (0,8) konvertiert.
- Der Beziehungsbewertung für Entität D ist bekannt, dass Entität E '70' ist. 70 wird in die Dezimalzahl 0.7 (0,7) konvertiert.

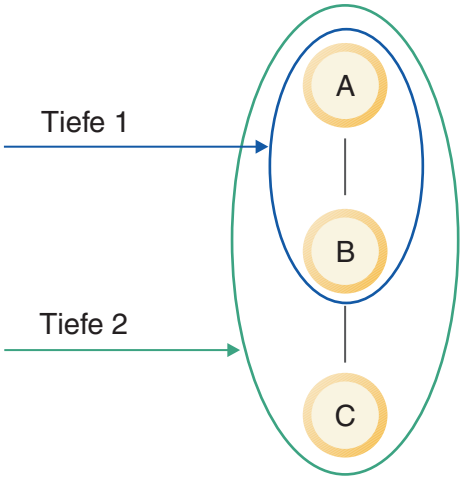


Die Beziehungsbewertungen im Beziehungspfad werden multipliziert. Das Ergebnis der Berechnung ist eine Relevanz des Beziehungspfad mit dem Wert 0.3528 (0,3528), der in die ganze Zahl 35 konvertiert wird.

Das Produkt vergleicht anschließend die berechnete Pfadrelevanz mit dem konfigurierten Abgrenzungspfadparameter für den Schwellenwert der Pfadrelevanz (**path strength threshold**). Entspricht die Relevanz des Beziehungspfads dem konfigurierten Pfadschwellenwert oder überschreitet sie ihn, generiert das Produkt Rollenalerts. Liegt die Relevanz des Beziehungspfads unter dem konfigurierten Pfadrelevanzschwellenwert, generiert das Produkt keine Rollenalerts.

Das Produkt verwendet anschließend den konfigurierten Abgrenzungsgradparameter für die maximale Tiefe (**max depth**), um die Abgrenzungsgrade zwischen den Entitäten in der Beziehungskette zu berechnen. Die Einstellung von **max depth** be-

stimmt die maximale Anzahl von Abgrenzungsgraden in einem mehrstufigen Beziehungspfad, der als Teil der Erkennung von Rollenalerts betrachtet werden kann.



Der Parameter **max depth** ist in der Regel auf den Wert 2 gesetzt.

In diesem Beispiel ist der Parameter **max depth** auf den Wert 6 gesetzt. Entität C und Entität E haben einen Rollenkonflikt und sind durch 6 Stufen getrennt. Daher wird ein Rollenalert generiert.

Anzeigen von Abgrenzungskonfigurationen

Da das Produkt mehrere Abgrenzungskonfigurationen zulässt, können Sie diese Anweisungen verwenden, um die Einstellungen für eine bestimmte Abgrenzungskonfiguration anzuzeigen.

Vorgehensweise

1. Klicken Sie in der Konfigurationskonsole **Konfiguration** > **Beziehungen** > **Abgrenzungskonfiguration** an.
2. Wählen Sie die Abgrenzungskonfiguration aus.

Erstellen neuer Abgrenzungskonfigurationen

Sie definieren Abgrenzungskonfigurationen, um festzulegen, ob die Beziehungsauflösung einen, zwei oder mehr Abgrenzungsgrade zwischen Entitäten feststellt.

Vorgehensweise

1. Klicken Sie in der Konfigurationskonsole **Konfiguration** > **Beziehungen** > **Abgrenzungskonfiguration** an.
2. Klicken Sie **Neu** an.
3. Geben Sie auf der Registerkarte **Allgemein** die Einstellungen für diese Abgrenzungskonfiguration an.
4. Klicken Sie **Speichern** an.

Bearbeiten von Abgrenzungskonfigurationen

Bearbeiten Sie eine Abgrenzungskonfiguration, um die Einstellungen zu ändern, die angeben, wie viele Grade zwei Entitäten trennen dürfen, um vom System weiterhin als Beziehung angesehen zu werden.

Vorgehensweise

1. Klicken Sie in der Konfigurationskonsole **Konfiguration** > **Beziehungen** > **Abgrenzungskonfiguration** an.
2. Wählen Sie die **Abgrenzungskonfiguration** aus, die Sie bearbeiten wollen, und nehmen Sie die gewünschten Änderungen vor.
3. Klicken Sie **Speichern** an.

Hilfethemen

Abgrenzungskonfiguration - Registerkarte 'Allgemein':

Über die Registerkarte **Allgemein** können Sie die Details der Abgrenzungskonfiguration angeben.

ID Geben Sie die eindeutige ganze Zahl ein, mit der die Abgrenzungskonfiguration angegeben wird.

Der ID-Wert wird automatisch mit der nächsten fortlaufenden Zahl gefüllt, die nicht verwendet wird.

Code Geben Sie einen eindeutigen Wert ein, der diese Rolle kennzeichnet.

Beschreibung
Geben Sie eine Beschreibung für diese Abgrenzungskonfiguration ein.

Maximale Tiefe
Die maximale Anzahl von Abgrenzungsgraden in einer mehrstufigen Beziehungskette eines Entitätsdiagramms, die bei der Erkennung von Rollenalerts berücksichtigt wird.

Schwellenwert der Pfadrelevanz
Der berechnete Wert für den Schwellenwert der Pfadrelevanz (**`path strength threshold`**) einer Rollenalertkette. Eine Rollenalertkette mit einer Pfadrelevanz unterhalb dieses Schwellenwerts wird keine Rollenalerts generieren.

Die Pfadrelevanz ist das in eine ganze Zahl konvertierte Produkt aus den Dezimalkonvertierungen der Beziehungsbewertung jeder Entität in der Rollenalertkette. Die Standardeinstellung für diesen Parameter ist 15.

Der Abgrenzungsgrad wertet alle Pfade aus, die zwei Entitäten miteinander verbinden, und verwendet die höchste Pfadrelevanz zur Berichterstellung für Beziehungen.

Konfigurieren von UMF-Dokumenten

Die erfolgreiche Verwendung von UMF-Dokumenten (Unified Messaging Format) setzt voraus, dass diese Dokument bekannt und konfiguriert sind.

Anzeigen von Standard-UMF-Eingabedokumenten

Bei UMF-Eingabedokumenten handelt es sich um die Sammlung von UMF-Segmenten, die die eingehenden Daten strukturieren, um Daten in der Entitätendatenbank zu laden, zu modifizieren oder abzufragen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **Eingabedokumente** an.

Konfigurieren von Ausgabedokumenten

Sie müssen den Status **Aktiviert** eines Formatcodes für das Ausgabedokument konfigurieren, falls verwendet.

Informationen zu diesem Vorgang

Mit UMF-Ausgabedokumenten werden UMF-Ergebnisdaten formatiert.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **Ausgabedokumente** an.
4. Klicken Sie einen beliebigen Link in der Zeile an, die den Formatcode für das UMF-Ausgabedokument enthält, den Sie bearbeiten wollen.
5. Wählen Sie in der Dropdown-Liste **Aktiviert** den entsprechenden Status des Formatcodes für das UMF-Ausgabedokument aus.
6. Klicken Sie die Schaltfläche **Speichern** an.

Konfigurieren der Datenquelle

Sie müssen eine Datenquelle konfigurieren, wenn Sie Daten aus einer neuen Datenquelle in die Entitätendatenbank laden wollen.

Vorbereitende Schritte

Zum Konfigurieren einer Datenquelle müssen Sie zunächst Rollen einrichten.

Informationen zu diesem Vorgang

Datenquellen können über die Registerkarte **Datenquellen** der Konsole angezeigt und modifiziert werden.

Datenquellen

Datenquellen enthalten die Identitäten, die Sie für Entitätsauflösung verarbeiten und in die Entitätendatenbank laden wollen. Datenquellen enthalten identifizierende Daten (eindeutige persönliche Kennungen für eine Identität) und nicht identifizierende Daten (andere Attribute und Dateneinträge für eine Identität). Die Identitätsdatensätze in der Datenquelle müssen in UMF (Universal Message Format) exportiert werden, bevor sie vom System verarbeitet oder in die Entitätendatenbank geladen werden können. Beispiele für Datenquellen sind Mitarbeiterlisten, Überwachungslisten, Kundenverzeichnisse und Anbieterlisten.

Datenquellen enthalten wichtige Informationen wie Angaben zur ursprünglichen Quelle (weil die ursprünglichen Daten in UMF umgesetzt wurden) oder die externe Referenz für die Datenquelle. Durch diese Details wird jede Datenquelle im System eindeutig.

Wenn während der Entitätsauflösung zwei Entitäten nicht aufgelöst werden, verwendet das System die Informationen zur Datenquelle, um zu ermitteln, welche Informationen zu welcher Entität gehören.

Datenquellenpositionen und Quellensysteme

Sie können eingehende Datenquellen organisieren, indem Sie Datenquellenpositionen sowie Quellensysteme erstellen und diese Ihren Datenquellen zuordnen. Sie

können mit Datenquellenpositionen und Quellensystemen zwischen ähnlichen Typen von Datenquellen unterscheiden.

Wenn Sie z. B. Reservierungsdaten und Personalabteilungsdaten von mehreren Standorten verarbeiten, können Sie mit einer Datenquellenposition ermitteln, welcher Standort die Daten beiträgt:

- Eigenschaft X Reservierungsdaten
- Eigenschaft X Personalabteilungsdaten
- Eigenschaft Y Reservierungsdaten
- Eigenschaft Y Personalabteilungsdaten

Konfigurationen nach Datenquelle

Sie können die Ergebnisse der Entitätsauflösung und Beziehungserkennung maximieren, indem Sie jede Datenquelle mithilfe der folgenden Einstellungen konfigurieren:

Rollen
Da Datenquellen Gruppierungen desselben Datentyps sind, können Sie jedem Identitätsdatensatz in derselben eingehenden Datenquelle automatisch dieselbe Rolle zuordnen. Wenn Sie z. B. einer Datenquelle der Personalabteilung die Rolle 'Mitarbeiter' zuordnen, wird allen eingehenden Datensätzen aus der Mitarbeiterliste automatisch die Rolle 'Mitarbeiter' zugeordnet.

Ladeebenen
Sie können festlegen, ob alle Daten in einer eingehenden Datenquelle geladen werden oder nur die Daten, die in mindestens eine Entität aufgelöst werden bzw. mindestens eine Entitätsbeziehung erkennen.

Einstellungen für Beziehungsauflösung
Sie können die Stufe der Beziehungserkennung nach Datenquelle konfigurieren. Sie können z. B. die Beziehungsauflösung für eine Datenquelle inaktivieren oder die Anzahl Abgrenzungsgrade für die Erkennung von Beziehungen in dieser bestimmten Datenquelle auswählen.

Anzeigen von Datenquellen

Eine Datenquelle enthält die Daten, die in die Entitätendatenbank geladen werden. Möglicherweise wollen Sie vorhandene Datenquellen anzeigen, wenn Sie planen, eine neue Datenquelle hinzuzufügen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Registerkarte **Datenquellen** an.
4. Wählen Sie die Datenquelle aus, die Sie anzeigen wollen.

Konfigurieren einer Datenquelle

Zum erfolgreichen Laden von Daten in die Entitätendatenbank müssen Sie das System so konfigurieren, dass es alle Datenquellen erkennt.

Vorbereitende Schritte

Sie können Daten nur in das System laden, wenn die Datenquelle den UMF-Standard verwendet.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Registerkarte **Datenquellen** an.
4. Klicken Sie die Schaltfläche **Neu** an.
5. Geben Sie auf der Registerkarte **Allgemein** die ID, die Beschreibung und sonstige Konfigurationsdaten für die Datenquelle an.
6. Klicken Sie die Registerkarte **Entitätsauflösung** an.
7. Geben Sie auf der Registerkarte **Entitätsauflösung** die Informationen zur Auflösungskonfiguration für die Datenquelle an.
8. Klicken Sie die Registerkarte **Beziehungen** an.
9. Geben Sie auf der Registerkarte **Beziehungen** die Informationen zur Beziehungskonfiguration für die Datenquelle an.
10. Klicken Sie die Schaltfläche **Speichern** an.

Konfigurieren der Name Manager-Namensvergleichsebene

Sie konfigurieren die Name Manager-Vergleichsebene nach Datenquelle, da Ihre Namensdaten je nach Quelle variieren können. Die Vergleichsebene, die Sie auswählen, ist ein Vergleichsparameter, der festlegt, wie genau der Abgleich für eingehende Namen aus dieser Datenquelle ist.

Vorgehensweise

1. Wählen Sie in der Konfigurationskonsole **Konfiguration** > **Quellen** > **Datenquellen** aus.
2. Wählen Sie die Datenquelle aus.
3. Klicken Sie **Auflösung** an.
4. Wählen Sie in **Name Manager-Vergleichsebene** die Vergleichsebene aus. In den meisten Fällen können Sie den Standardwert verwenden, da dessen Genauigkeit zum Erzielen guter Namensvergleiche ausreicht.

Konfigurieren von Datenquellen für erweitertes Namenshashing

Wenn Sie das erweiterte Namenshashing verwenden, müssen Sie jede Datenquelle so konfigurieren, dass sie die Erstellung von Namensattributen für Kandidatenlisten zulässt. Setzen Sie dazu die Konfiguration für Kandidatenerstellungsregeln auf die Kandidatenerstellungsregel **Default w/ Name Only**.

Löschen von Datenquellen

Eine Datenquelle enthält die Daten, die in die Entitätendatenbank geladen werden. Es empfiehlt sich möglicherweise, eine Datenquelle zu löschen, wenn sie nicht mehr vorhanden oder nicht mehr für die Entitätendatenbank relevant ist.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Registerkarte **Datenquellen** an.
4. Wählen Sie das Kontrollkästchen neben der Datenquelle aus, die Sie löschen wollen.
5. Klicken Sie die Schaltfläche **Löschen** an.

Erstellen eines Datenquellenstandorts

Wenn ein Standort bei der Klassifizierung einer Datenquelle zur Auswahl verfügbar sein soll, muss dieser Standort im System konfiguriert sein.

Informationen zu diesem Vorgang

Datenquellenstandorte werden über die Konfigurationskonsole erstellt. Dies ist eine optionale Funktion, die hauptsächlich verwendet wird, wenn die Datenquelle Daten aus mehreren physischen Positionen zusammenstellt. Beispiel: eine Hotelsystemdatenbank, die Daten von Hotels an verschiedenen Standorten zusammenstellt.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Standorte** an.
4. Klicken Sie die Schaltfläche **Neu** an.
5. Geben Sie auf der Registerkarte **Allgemein** den Standortcode, den Standortnamen, den Bezirk, das Unternehmen, den Breitengrad, den Längengrad, den Status und sonstige Konfigurationsdaten für den Datenquellenstandort an.
6. Klicken Sie die Schaltfläche **Speichern** an.

Nächste Schritte

Sie können den gerade konfigurierten Standort nun auf Datenquellen im System anwenden.

Hilfethemen

Datenquellen - Registerkarte 'Entitätsauflösung':

Über die Registerkarte **Entitätsauflösung** können Sie die Details für die Entitätsauflösung der Datenquelle angeben.

Entitätsauflösungskonfiguration
Wählen Sie in der Liste die Auflösungskonfiguration aus, die diese Datenquelle beim Laden von Daten verwendet.

Konfiguration für Kandidatenerstellungsregeln
Wählen Sie in der Liste die während der Verarbeitung der Entitätsauflösung verwendete Konfiguration für Kandidatenerstellungsregeln aus, wenn Sie Daten aus dieser Datenquelle laden.

Standard
Wählen Sie diese Einstellung aus, um die Standardkonfiguration für Kandidatenerstellungsregeln zu verwenden.

Default w/ Name Only
Wählen Sie diese Einstellung aus, um die Standardkonfiguration für Kandidatenerstellungsregeln plus zusätzlichen Namensabgleich zu verwenden.

Wählen Sie diese Konfiguration für Kandidatenerstellungsregeln aus, wenn Sie Name Hasher zum Verarbeiten von Namensdaten für diese Datenquelle verwenden wollen. (Stellen Sie sicher, dass die Systemparameter für Name Hasher festgelegt sind.)

Merkmalbestätigungen
Wählen Sie in der Liste **Ja** aus, um anzugeben, dass Merkmalbestätigungen beim Laden dieser Datenquelle verarbeitet werden. Wählen Sie andernfalls **Nein** aus.

Abhängen ausführen
Diese Einstellung wird in der Regel nur für Hotelsysteme verwendet.

Wählen Sie in der Liste **Ja** aus, um anzugeben, dass die Pipeline Datenabgleiche ohne das Datenquellenbenutzerkonto ausführt. Ist der Abgleich nicht erfolgreich, wird das Löschdatum für die früheren Daten gesetzt. Wählen Sie andernfalls **Nein** aus.

Name Manager-Vergleichsebene
Wählen Sie in der Liste den Wert für die Vergleichebene aus, der zum Bewerten eingehender Namensdaten aus dieser Datenquelle verwendet werden soll.

Standard
Wählen Sie diesen Wert aus, um die häufigste Vergleichsebene für den Namensabgleich zu verwenden.

Grob Wählen Sie diesen Wert aus, wenn Sie weitere Namensabgleiche für diese Datenquelle durchführen wollen. Dieser Wert lockert die Vergleichsebene für den Namensabgleich, wodurch der Vergleich weniger genau ist als bei Verwendung des Standardwerts.

Stark Wählen Sie diesen Wert aus, wenn Sie weniger Namensabgleiche für diese Datenquelle durchführen wollen. Dieser Wert verschärft die Vergleichsebene für den Namensabgleich, wodurch der Vergleich genauer ist als bei Verwendung des Standardwerts.

Aufheben der Auflösung zulassen
Die Funktion zum Aufheben der Auflösung besteht aus dem Prozess, bei dem aufgelöste Identitäten auf der Basis neuer Informationen aus eingehenden Daten in zwei separate Entitäten getrennt werden. Treffen Sie in der Liste die entsprechende Auswahl für diese Datenquelle:

- Wählen Sie **Ja** aus, um die Entitätsauflösung (sofern im Lieferumfang enthalten) zuzulassen, mit der Identitäten beim Laden von Benutzerkonten für diese Datenquelle in separate Entitäten getrennt werden.
- Wählen Sie **Nein** aus, um die Entitätsauflösung zu verhindern, bei der Identitäten beim Laden von Benutzerkonten für diese Datenquelle in separate Entitäten getrennt werden.

Datenquellen - Registerkarte 'Allgemein':

Über die Registerkarte **Allgemein** können Sie die Details für die Datenquelle angeben.

ID Geben Sie die ID-Nummer der Datenquelle ein, die Sie erstellen wollen.

Die ID ist ein numerischer Code, der sich automatisch erhöht. Das Programm stellt die nächste verfügbare Nummer in der Folge zur Verfügung, Sie können den Code allerdings auch als einen beliebigen eindeutigen numerischen Wert angeben, indem Sie den Wert in das Feld **ID** eingeben.

Code Geben Sie den Code der Datenquelle ein, die Sie erstellen wollen.

Dies ist der Wert des UMF-Tags `DSRC_CODE`. Der Wert für den Datenquellencode kann alphanumerisch sein und wird zur weiteren Identifikation einer Datenquelle verwendet. Der Wert muss eindeutig sein und kann nach dem Speichern des Datensatzes nicht mehr geändert werden.

Beschreibung
Geben Sie die Beschreibung der Datenquelle ein, die Sie erstellen wollen.

Standort
Wählen Sie in der Dropdown-Liste den Standortcode für die Datenquelle aus, die Sie erstellen wollen.

Dieses Feld dient nur zu Referenzzwecken.

Quellensystem
Wählen Sie in der Dropdown-Liste den Quellensystemcode für die Datenquelle aus, die Sie erstellen wollen.

Dieses Feld dient nur zu Referenzzwecken.

Status Wählen Sie in der Dropdown-Liste **Aktiv** aus, um anzugeben, dass diese Datenquelle aktiv ist. Wählen Sie andernfalls **Inaktiv** aus.

Aktion akzeptieren
Wählen Sie in der Dropdown-Liste **Ja** aus, um anzugeben, dass Sie der Korrektheit des UMF-Tags `ACTION` von Ihrer Datenquelle vertrauen. Andernfalls wählen Sie **Nein** aus, um die Aktion durch Untersuchen der Entitätendatenbank festzulegen. Bei Auswahl von **Nein** wird die Leistung verschlechtert.

Zum Suchen
Wählen Sie in der Dropdown-Liste **Ja** aus, um anzugeben, dass diese Datenquelle zum Laden von Suchen verwendet wird. Wählen Sie andernfalls **Nein** aus.

Transliterieren
Wählen Sie in der Dropdown-Liste **Ja** aus, um anzugeben, dass die Transliteration für diese Datenquelle erfolgen soll. Dadurch wird die Unterstützung für den Zeichensatz des lateinischen Alphabets 1 hinzugefügt. Wählen Sie andernfalls **Nein** aus.

Anmerkung: Wenn Sie die Einstellung für das Transliterieren für eine Datenquelle aktivieren, müssen Sie auch die Konfigurationseinstellung für das Transliterieren für die Datenquellen-ID 1589 (Suche) aktivieren. Die Datenquelle 1589 wird vom Produkt verwendet, um Suchen in die Pipeline einzufügen, und setzt standardmäßig die Eingabe von ASCII-Zeichen voraus. Durch das Aktivieren dieser Konfiguration stellen Sie sicher, dass Namen, die Teil einer Suche sind, auch ordnungsgemäß transliteriert werden, um besonders akkurate Suchergebnisse bereitzustellen.

Datenquellen - Registerkarte 'Beziehungen':

Über die Registerkarte **Beziehungen** können Sie die Beziehungsdetails für die Datenquelle angeben.

Rolle Wählen Sie den Rollencode aus, um diese Datenquelle zuzuordnen.

Datenquellenklasse
Wählen Sie die entsprechende Datenquellenklasse für diese Datenquelle aus.

Full Load
Wählen Sie diesen Feldtyp aus, um die Daten in die Datenbank zu laden.

Diese Einstellung löst außerdem alle auflösbaren Identitäten auf, aktualisiert die Entität, erkennt alle möglichen Beziehungen und generiert die benutzerdefinierten Rollenalerts.

Fully Passive
Wählen Sie diesen Feldtyp aus, um die Daten nicht in die Datenbank zu laden.

Bei diesem vollständigen passiven Ladevorgang werden keine Daten gespeichert. Visualizer kann den Alert nicht anzeigen.

Load if Resolve/Relate
Wählen Sie diesen Feldtyp aus, um die Daten in die Datenbank zu laden, wenn sie in vorhandene Datensätze in der Entitätendatenbank aufgelöst werden können oder wenn sie in Beziehungen zu vorhandenen Entitäten stehen.

Diese Einstellung löst außerdem alle auflösbaren Identitäten auf, aktualisiert die Entität, erkennt alle möglichen Beziehungen und generiert die benutzerdefinierten Rollenalerts.

Load if Selective Resolve/Relate
Wählen Sie diesen Feldtyp aus, um die Daten in die Datenbank zu laden, wenn sie in vorhandene Datensätze in der Entitätendatenbank aufgelöst werden können oder wenn sie in Beziehung zu vorhandenen Entitäten stehen; jedoch nur, wenn diese Datenquelle in der Tabelle SELECTIVE_PASSIVE_CONFIG konfiguriert ist.

Diese Einstellung löst außerdem alle auflösbaren Identitäten auf, aktualisiert die Entität, erkennt alle möglichen Beziehungen und generiert die benutzerdefinierten Rollenalerts.

Load if Selective Resolve
Wählen Sie diesen Feldtyp aus, um die Daten in die Datenbank zu laden, wenn sie in Beziehung zu vorhandenen Datensätzen in der Entitätendatenbank stehen; jedoch nur, wenn diese Datenquelle in der Tabelle SELECTIVE_PASSIVE_CONFIG konfiguriert ist.

Diese Einstellung löst außerdem alle auflösbaren Identitäten auf, aktualisiert die Entität, erkennt alle möglichen Beziehungen und generiert die benutzerdefinierten Rollenalerts.

Abgrenzungsebene
Wählen Sie in der Dropdown-Liste die entsprechende Abgrenzungsebene für diese Datenquelle aus.

Daten laden
Wählen Sie diesen Feldtyp immer aus. Er ist zurzeit die einzige Option.

DoS-Konfiguration
Wählen Sie in der Dropdown-Liste die entsprechende Abgrenzungsgradkonfiguration für diese Datenquelle aus.

Die Abgrenzungskonfigurationen werden in der Anzeige **Konfiguration** > **Beziehungen** > **Abgrenzungskonfiguration** definiert.

Standorte - Registerkarte 'Allgemein':

Über die Registerkarte **Standorte** können Sie die Details für den Datenquellenstandort angeben.

Standortcode
Geben Sie den Standortcode ein, der diesem Datenquellenstandort zugeordnet werden soll.

Ein alphanumerischer Wert, der nicht mehr geändert werden kann, nachdem der Datensatz gespeichert wurde.

Dieser Wert ist erforderlich.

Standortname
Geben Sie den Standortnamen ein, der diesem Datenquellenstandort zugeordnet werden soll.

Bezirk Geben Sie den Bezirk ein, der diesem Datenquellenstandort zugeordnet werden soll.

Dieser Wert ist erforderlich.

Unternehmen
Geben Sie den Firmennamen ein, der diesem Datenquellenstandort zugeordnet werden soll.

Breitengrad
Geben Sie den Breitengrad für diesen Datenquellenstandort im folgenden Format an:

GG:MM:SS

Längengrad
Geben Sie den Längengrad für diesen Datenquellenstandort im folgenden Format an:

GG:MM:SS

Status Wählen Sie in der Dropdown-Liste **Aktiv** aus, um anzugeben, dass dieser Datenquellenstandort aktiv ist. Wählen Sie andernfalls **Inaktiv** aus.

Inaktivieren der Beziehungserkennung

Wenn Sie für Ihre Geschäftsvorgänge nur wissen müssen, wer jemand ist, aber nicht welche Beziehungen untereinander bestehen, können Sie den Verarbeitungsumfang reduzieren, der für jeden neuen Datensatz erforderlich ist, und die Gesamtsystemleistung erhöhen, indem Sie die Geschäftsanforderung so konfigurieren, dass nur eine Entitätsauflösung ausgeführt wird und Beziehungen zwischen Entitäten nicht erkannt werden.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie **Konfiguration bearbeiten** ausgewählt haben, als Sie sich an der aktuellen Sitzung der Konfigurationskonsole angemeldet haben.

Vorgehensweise

1. Inaktivieren Sie die Rollenzuordnungen für jede Datenquelle.
   a. Klicken Sie **Konfiguration** an.
   b. Klicken Sie **Quellen** an.
   c. Klicken Sie auf der Registerkarte **Datenquellen** die Datenquelle an, die Sie bearbeiten wollen.
   d. Klicken Sie die Registerkarte **Beziehungen** an.
   e. Wählen Sie **— Bitte auswählen —** in der Dropdown-Liste **Rolle** aus.
   f. Wählen Sie **Nur Alerts** in der Dropdown-Liste **Abgrenzungsebene** aus.
   g. Klicken Sie **Speichern** an.
2. Inaktivieren Sie die Datenqualitätsmanagementregel für Standardrollenzuordnungen.
   a. Klicken Sie **Konfiguration** an.

b. Klicken Sie **UMF** an.
c. Wählen Sie auf der Registerkarte **DQM-Regeln** den Eintrag **ROOT** in der Dropdown-Liste **Segment** aus.
d. Klicken Sie einen beliebigen Link in der Zeile an, die die DQM-Funktion 551 (Standardrollenzuordnung) enthält.
e. Wählen Sie auf der Registerkarte **Allgemein** den Eintrag **Inaktiv** in der Dropdown-Liste **Status** aus.
f. Klicken Sie **Speichern** an.

3. Löschen Sie alle Auflösungsregeln, die nicht für das Auflösen von Entitäten definiert wurden.
   a. Klicken Sie **Konfiguration** an.
   b. Klicken Sie **Auflösung** an.
   c. Klicken Sie die Registerkarte **Auflösungsregeln** an.
   d. Wählen Sie **STANDARD** in der Dropdown-Liste **Auflösungskonfiguration** aus.
   e. Klicken Sie das Kontrollkästchen neben jeder Auflösungsregel an, für die ein Wert **Nein** in der Spalte **Löst Auflösung aus** angezeigt wird.
   f. Klicken Sie **Löschen** an.
   g. Bestätigen Sie das Löschen der ausgewählten Auflösungsregeln durch Anklicken von **OK**.
4. Löschen Sie schließlich alle Konfliktregeln.
   a. Klicken Sie **Konfiguration** an.
   b. Klicken Sie **Beziehungen** an.
   c. Klicken Sie die Registerkarte **Konfliktregel** an.
   d. Klicken Sie das Kontrollkästchen neben jeder Konfliktregel an.
   e. Klicken Sie **Löschen** an.
   f. Bestätigen Sie das Löschen der ausgewählten Konfliktregeln durch Anklicken von **OK**.

Nächste Schritte

Das System ist jetzt so konfiguriert, dass Entitäten ohne das Erkennen von Beziehungen aufgelöst werden.

Konfigurieren von Ereignistypen

Sie können Ereignistypen konfigurieren, um vom Ereignismanager verarbeitete Ereignistypen zu definieren und zu kategorisieren. Bevor das System aber eingehende Daten mit Ereignistypen verarbeitet, müssen Sie die Ereignisverarbeitung in den Systemparametern des Ereignismanagers aktivieren, die Geschäftsregeln im Eclipse-basierten Prozessortool für komplexe Ereignisse konfigurieren und die eingehenden Ereignisdaten unter Verwendung der Definitionen des UMF-Datensegments EVENT formatieren.

Ereignistypen können über die Registerkarte **Ereignistypen** der Konsole angezeigt und modifiziert werden.

Ereignistypen

Ereignistypen kategorisieren Ereignisse und definieren die Maßeinheit für den Wert, der Ereignissen im Ereignismanager zugeordnet ist. Beispiele von Ereignistypen sind Geldüberweisungen, Kontoeröffnungen oder Kreditkartentransaktionen.

Ereignistypen sind für die Ereignisverarbeitung erforderlich, da die benutzerdefinierten Geschäftsregeln, die der Ereignisprozessor verwendet, einen bestimmten Ereignistyp aufrufen. Wenn der Ereignistyp nicht vorhanden ist, kann der Ereignisprozessor das Ereignis nicht verarbeiten.

Erstellen von Ereignistypen

Wenn Sie ein neues Ereignisszenario zur Verarbeitung von Ereignissen hinzufügen wollen, müssen Sie möglicherweise einen neuen Ereignistyp erstellen, um die Typen der Transaktionen oder Aktivitäten zu definieren, die in diesem Ereignisszenario enthalten sind. Außerdem müssen Sie die Maßeinheit angeben, die dieser Ereigniskategorie zugeordnet ist.

Vorbereitende Schritte

Der Ereignismanager muss für Ihr IBM InfoSphere Identity Insight-System aktiviert sein.

Informationen zu diesem Vorgang

Ereignistypen werden vom Prozessor für komplexe Ereignisse aufgerufen, während er Ereignisse entsprechend der vom Benutzer definierten Geschäftsregeln verarbeitet. Vor der Verwendung eines Ereignistyps müssen Sie außerdem mindestens eine Geschäftsregel erstellen, die diesen Ereignistyp verwendet.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Schaltfläche **Ereignistyp** an.
4. Klicken Sie die Schaltfläche **Neu** an.
5. Erforderlich: Geben Sie auf der Registerkarte **Allgemein** den Namen und die Beschreibung des Ereignistyps, die diesem Ereignistyp zugeordnete Maßeinheit und den Status für diesen Ereignistyp ('Aktiv' oder 'Inaktiv') an.
6. Optional: Sie können auch zusätzliche Informationen angeben, wie z. B. die Kategorie, die Unterkategorie und Hinweise zu diesem Ereignistyp.
7. Klicken Sie die Schaltfläche **Speichern** an.

Bearbeiten von Ereignistypen

Sie bearbeiten einen Ereignistyp, wenn Sie die Beschreibung, die Maßeinheit oder die dem Ereignistyp zugeordneten Zusatzinformationen ändern wollen. Sie können einen Ereignistyp auch bearbeiten, um ihn zu inaktivieren, sodass er nicht mehr verwendet werden kann. Der Name des Ereignistyps kann nicht bearbeitet werden.

Informationen zu diesem Vorgang

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Schaltfläche **Ereignistyp** an.
4. Wählen Sie den Ereignistyp aus, den Sie bearbeiten wollen.
5. Nehmen Sie Ihre Änderungen auf der Registerkarte **Allgemein** vor.
6. Klicken Sie die Schaltfläche **Speichern** an.

Nächste Schritte

Löschen von Ereignistypen

Möglicherweise wollen Sie einen Ereignistyp löschen, wenn er nicht mehr für die Ereignisverarbeitung verwendet wird. Wenn Sie den Ereignistyp nicht löschen sondern nur inaktivieren wollen, können Sie den Status des Ereignistyps bearbeiten anstatt ihn zu löschen.

Vorbereitende Schritte

Informationen zu diesem Vorgang

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Quellen** an.
3. Klicken Sie die Schaltfläche **Ereignistyp** an.
4. Wählen Sie das Kontrollkästchen neben dem Ereignistyp aus, den Sie löschen wollen.
5. Klicken Sie die Schaltfläche **Löschen** an.

Nächste Schritte

Hilfethemen

Ereignistypen - Registerkarte 'Allgemein':

Über diese Registerkarte können Sie einen Ereignistyp definieren oder bearbeiten. Ereignistypen definieren und kategorisieren Ereignisse und werden während der Ereignisverarbeitung verwendet, wenn der Ereignismanager für Ihr System aktiviert ist.

Typ Geben Sie einen eindeutigen Namen für diesen Ereignistyp ein. Sie könnten z. B. einen Ereignistyp mit dem Namen `Geldüberweisung` erstellen.

Beschreibung
Geben Sie eine Beschreibung dieses Ereignistyps ein.

Maßeinheit
Geben Sie eine Abkürzung der Maßeinheit für den Wert ein, der dem Ereignistyp zugeordnet ist. Sie könnten z. B. `EUR` für Euro eingeben.

Status Wählen Sie in der Dropdown-Liste den Status für den Ereignistyp aus, entweder **Aktiv** oder **Inaktiv**. (Mit dem Status **Inaktiv** können Sie den Ereignistyp aus der Ereignisverarbeitung ausschließen, die Konfiguration für den Ereignistyp aber beibehalten.)

Kategorie
Geben Sie einen optionalen Kategorienamen für den Ereignistyp ein.

Unterkategorie
Geben Sie einen optionalen Unterkategorienamen für den Ereignistyp ein.

Kurzinfo – Überschrift 1
Geben Sie eine optionale Überschrift 1 der Kurzinfo für den Ereignistyp ein.

Kurzinfo – Überschrift 2
Geben Sie eine optionale Überschrift 2 der Kurzinfo für den Ereignistyp ein.

Konfigurieren der Entitätsauflösung

Die Entitätsauflösung ist der Prozess, der Beziehungen in den Daten erkennt. Einstellungen für die Entitätsauflösungskonfiguration sind in Gruppen zusammengefasst, die als Auflösungskonfigurationen bezeichnet werden. Eine Auflösungskonfiguration besteht aus fünf Komponenten: Auflösungsregeln, Bestätigungen und Zurückweisungen, Attributen, Name Manager-Abgleichkonfigurationen und der Kandidatenerstellungsregel.

Entitätsauflösung

Entitätsauflösung ist der Prozess, der Entitäten auflöst und Beziehungen erkennt. Die Pipelines führen Entitätsauflösung beim Verarbeiten von eingehenden Identitätsdatensätzen in drei Phasen aus: 'Erkennen', 'Auflösen' und 'Beziehungen erkennen'.

Konfigurieren von Auflösungskonfigurationen

Alle Einstellungen für die Entitätsauflösung werden in Auflösungskonfigurationen verwaltet. Zwei dieser Auflösungskonfigurationen werden standardmäßig bereitgestellt.

Auflösungskonfigurationen

Entitätsauflösungseinstellungen sind in einer Gruppe von Auflösungskonfigurationen zusammengefasst, die auf der Registerkarte **Systemkonfiguration** der Konfigurationskonsole über den Wert der Auflösungsregel für die Systembelastung definiert werden.

Die Standardinstallation von Relationship Resolution enthält zwei Auflösungskonfigurationen:

- **DEFAULT**: Standardauflösungseinstellungen, die verwendet werden, wenn neue Daten aus einer definierten Datenquelle in das System aufgenommen werden.
- **SEARCH**: Auflösungseinstellungen, die vom Prozess für aufgelöste Suche verwendet werden, wenn ein Benutzer eine vollständig aufgelöste Suchanforderung übergibt.

Sie können Ihre eigene Gruppe von Auflösungseinstellungen erstellen und sie über eine neu erstellte Auflösungskonfiguration identifizieren. Sie starten diesen Prozess, indem Sie die Auflösungskonfiguration **DEFAULT** klonen und als Ausgangspunkt für Ihre neue Auflösungskonfiguration verwenden.

Verschiedene Auflösungskonfigurationen können bestimmten Datenquellen zugeordnet werden. Wenn Sie mehrere Auflösungskonfigurationen für mehrere Datenquellen anwenden wollen, müssen Sie beachten, dass die Entitätsauflösung immer die Auflösungskonfiguration verwendet, die der eingehenden Identität zugeordnet ist, wenn Alerts generiert werden. Je nachdem, welche der verglichenen Identitäten die eingehende Identität ist und welche der Identitäten bereits in der Entitätendatenbank vorhanden ist, kann dies zu verschiedenen Alertergebnissen führen. Beispielsweise wird die Identität #123 aus der Datenquelle 'Customer' der Auflösungskonfiguration DEFAULT zugeordnet, die eine Auflösungsregel für Name und Adresse mit einem Namensschwellenwert von 80 und einem Adressenschwellenwert von 5 enthält. Die Identität #456 aus der Datenquelle 'Vendor' verwendet die Auflösungskonfiguration NEW, die dieselbe Auflösungsregel hat. Allerdings sind der Namensschwellenwert auf 95 und der Adressenschwellenwert auf 7 gesetzt. Wenn 'Customer 123' die eingehende Identität ist und mit der vorhandenen Entität 'Vendor 456' verglichen wird, wird die Namensbewertung zwischen ihnen als 85

berechnet und die Adressenbewertung ist 5. Diese Berechnungen führen zu einem Alert. Wenn die Verarbeitungsreihenfolge umgekehrt wird, d. h., 'Customer 123' ist bereits im System vorhanden und 'Vendor 456' wird in das System aufgenommen, generieren sie auch in diesem Fall dieselben Auflösungsbewertungen von 85 für den Namen und 5 für die Adresse. Allerdings wird kein Alert generiert, weil die Auflösungsbewertungen die in der Auflösungskonfiguration NEW festgelegten Auflösungsschwellenwerte von 95 für den Namen und 7 für die Adresse nicht erreichen.

Anmerkung:

Wenn Sie eine andere Konfiguration als die Standardkonfiguration für Entitätsauflösung verwenden wollen, wird dringend empfohlen, äußerst sorgfältig und mit entsprechender Planung vorzugehen. Die Standardeinstellungen der Entitätsauflösung wie Auflösungsregeln und Bewertungseinstellungen sind das Ergebnis aus Hunderten von Mannjahren der Analyse und des Studierens von realistischen Daten. Änderungen dieser Standardwerten sind in der Regel nur dann erforderlich, wenn Daten oder Geschäftsregeln bestimmte vom Standard abweichende Verhaltensweisen vom System verlangen.

Anzeigen von Auflösungskonfigurationen

Eine Auflösungskonfiguration wird verwendet, um eine Sammlung von Entitätsauflösungseinstellungen anzugeben. Möglicherweise wollen Sie vorhandene Auflösungskonfigurationen anzeigen, wenn Sie planen, Änderungen an Ihren Entitätsauflösungseinstellungen vorzunehmen, oder wenn Sie eine neue Gruppe von Entitätsauflösungseinstellungen erstellen wollen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Auflösung** an.

Klonen und Anpassen der Standardauflösungskonfiguration

Das beste Verfahren zum Erstellen einer neuen Entitätsauflösungskonfiguration besteht darin, die Standardauflösungskonfiguration zu klonen (d. h. zu kopieren) und als Ausgangspunkt für die neue Auflösungskonfiguration zu verwenden. Wenn die Standardkonfiguration nicht geändert wird, können Sie bei Bedarf immer zu der Standardkonfiguration zurückkehren, ohne dass das Produkt erneut installiert werden muss.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Auflösung** an.
3. Wählen Sie auf der Registerkarte **Auflösungskonfigurationen** das Kontrollkästchen neben der Auflösungskonfiguration DEFAULT aus.
4. Klicken Sie die Schaltfläche **Klonen** an.
5. Geben Sie den neuen Namen für die Auflösungskonfiguration der Registerkarte **Allgemein** in das Feld **Code** ein.
6. Geben Sie eine neue Beschreibung für die geklonte Auflösungskonfiguration in das Feld **Beschreibung** ein.
7. Klicken Sie die Schaltfläche **Speichern** an.

Nächste Schritte

Wenn Sie Änderungen an den Einstellungen für die Entitätsauflösung vornehmen, beispielsweise beim Konfigurieren von Auflösungsregeln, Bestätigungen und Zurückweisungen oder Kandidatenerstellungsregeln, können Sie die neue Auflösungskonfiguration auswählen.

Löschen angepasster Auflösungskonfigurationen

Wenn Sie eine angepasste Auflösungskonfiguration nicht mehr verwenden, können Sie sie löschen. Löschen Sie die Standardauflösungskonfiguration jedoch nicht. Wenn die Standardkonfiguration nicht geändert wird, können Sie bei Bedarf immer zu der Standardkonfiguration zurückkehren, ohne dass das Produkt erneut installiert werden muss.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Auflösung** an.
3. Wählen Sie auf der Registerkarte **Auflösungskonfigurationen** das Kontrollkästchen neben der Auflösungskonfiguration aus, die Sie löschen wollen.
4. Klicken Sie die Schaltfläche **Löschen** an.
5. Klicken Sie **OK** im Bestätigungsfenster an, um die Auflösungskonfiguration zu löschen.

Nächste Schritte

Sie können diese Auflösungskonfiguration nicht mehr auswählen, wenn Sie Änderungen an den Entitätsauflösungseinstellungen vornehmen. Darüber hinaus können die zu dieser Auflösungskonfiguration gehörigen Entitätsauflösungseinstellungen nicht mehr auf den Entitätsauflösungsprozess angewendet werden.

Hilfethemen

Fenster 'Auflösungskonfigurationen':

Über dieses Fenster können Sie eine Liste der verfügbaren Entitätsauflösungskonfigurationen anzeigen. Einstellungen für die Entitätsauflösung werden in Gruppen eingeteilt, die als Auflösungskonfigurationen bezeichnet werden. Den einzelnen Datenquellen können verschiedene Auflösungskonfigurationen zugeordnet werden. Auf jede Datenquelle kann nur jeweils eine Auflösungskonfiguration angewendet werden.

Code Name der Auflösungskonfiguration

Beschreibung
Beschreibung der Auflösungskonfiguration

Konfigurieren von Auflösungsregeln

Wenn Sie definieren wollen, wie verglichene Entitäten aufgelöst und Beziehungen zwischen Entitäten erkannt werden, müssen Sie Auflösungsregeln einschließlich Kandidatenschwellenwerten und Schwellenwerten für Bestätigung/Zurückweisung konfigurieren.

Informationen zu diesem Vorgang

Auflösungsregeln können über die Registerkarte **Auflösungsregeln** der Konsole angezeigt und modifiziert werden.

Auflösungsregeln

Auflösungsregeln sind die Gruppe von Kriterien, mit denen das System definiert, wie verglichene Entitäten aufgelöst werden (wenn sie dieselbe Entität sind oder nicht) und wie sie Beziehungen erkennen (wenn Entitäten nicht in dieselbe Entität aufgelöst werden, wie viele Attribute sie gemeinsam haben).

Beim Definieren von Auflösungsregeln müssen Sie Schwellenwerte angeben, die zur Gesamtauflösungsbewertung beitragen, die bestimmt, ob eine eingehende Identität in eine vorhandene Entität aufgelöst wird:

- Kandidatenschwellenwerte geben an, welche Attributdatenwerte verglichen werden, um zu ermitteln, ob eine Identität und eine Entität in eine zusammengesetzte Entität aufgelöst werden. Der Schwellenwert ist die Mindestbewertung, die ein bestimmter Attributwert bei einem Vergleich der eingehenden Identität mit einer vorhandenen Entität erreichen muss, um die Auflösungsregel zu erfüllen.
- Bestätigungs-/Zurückweisungsschwellenwerte geben an, welche Bewertungsgewichtung (positiv oder negativ) übereinstimmenden oder sich widersprechenden Attributdatenwerten zugewiesen wird, wenn Sie die Verwendung von Zurückweisungen aktivieren.

Sie können auch angeben, wie sich widersprechende Werte für dieselben Attribute sich auf die Auflösungsbewertung auswirken. Diese sich widersprechenden Werte heißen Zurückweisungen. Sie können Auflösungsregeln konfigurieren, die angeben, dass die Regel nicht erfüllt ist, wenn in den Attributwerten Konflikte (Zurückweisungen) vorhanden sind. Sie können auch die Schwellenwerte für eine Auflösungsregel anpassen, um basierend auf den Vergleichsbewertungen, die mindestens eine angegebene Schwellenwertbewertung nicht erfüllen, automatische Zurückweisungen zu erstellen. Je höher eine Schwellenwertbewertung festgelegt wird, desto präziser muss die Übereinstimmung sein, um die Auflösungsregel zu erfüllen.

Kandidatenschwellenwerte

Kandidatenschwellenwerte sind die ersten Komponenten einer Auflösungsregel, mit denen ermittelt wird, ob eine eingehende Identität eine vorhandene Entität oder eine vollständig neue Entität darstellt.

Kandidatenschwellenwerte werden über die Konsole konfiguriert und sind ein integraler Bestandteil einer Auflösungsregel. Wenn z. B. für eine Auflösungsregel eine eindeutige Nummer als Kandidatenschwellenwert definiert ist, kann für diese Auflösungsregel angegeben werden, dass sie eine übereinstimmende eindeutige Nummer erfordert.

Kandidatenschwellenwerte werden nur auf vorhandene Entitäten angewendet, um diese Entitäten als Teil des Entitätsauflösungsprozesses in die Kandidatenliste aufzunehmen. Der tatsächliche Schwellenwert ist die Mindeststufe, auf der ein bestimmter Datentyp einer eingehenden Identität und einer vorhandenen Entität übereinstimmen muss, damit der Entitätsauflösungsprozess die vorhandene Entität der Kandidatenliste hinzufügen kann.

Adressgenauigkeit:

Adressgenauigkeit ist der Bewertungsprozess, mit dem die Entitätsauflösung ermittelt, ob zwei miteinander verglichene Adressen dieselbe Adresse darstellen.

Adressgenauigkeit ist in neun eindeutige Stufen (1-9) unterteilt. Die meisten Adressen enthalten grundlegende Komponenten, die verglichen werden können, z. B.

Straße (einschließlich Hausnummer), Ort, Bundesland/Staat, Postleitzahl oder US-Postleitzahl +4. Beim Vergleich dieser Komponenten startet die Adressgenauigkeit mit einer übereinstimmenden Straßenkomponente und ordnet die Genauigkeitsstufe 5 zu. Diese Genauigkeitsstufe wird dann je nachdem, ob zusätzliche Komponenten übereinstimmen oder abweichen, nach oben oder unten angepasst. Jede übereinstimmende Komponente erhöht die Genauigkeitsstufe um 1 und jede abweichende Komponente reduziert die Genauigkeitsstufe um 1. Wenn ein Komponentenwert in einer Adresse vorhanden ist, jedoch für dieselbe Komponente in der anderen Adresse ein Wert fehlt, wird die Genauigkeit nicht angepasst.

Die Entitätsauflösung betrachtet standardmäßig alle verglichenen Adressen mit einer Adressgenauigkeitsstufe von fünf oder höher als Kandidaten für übereinstimmende Adressen.

Tabelle 29. Stufen der Adressgenauigkeit

Stufe	Beschreibung
1	Straßenübereinstimmung mit allen Teilen, US-Postleitzahl +4 abweichend. Das heißt, es muss eine Adresse vorliegen, die in allen Teilen übereinstimmt, aber eine unterschiedliche US-Postleitzahl +4 aufweist. Beispiel: 123 N Water St. Las Vegas, NV 89123-1234 und 123 S Water St. Las Vegas, NV 89123-5433.
2	Straßenübereinstimmung, alle Teile abweichend. Das bedeutet, dass nur die Straße übereinstimmt, die Angaben für Stadt, Bundesstaat, Postleitzahl und Land jedoch unterschiedlich sind oder fehlen. Beispiel: 123 Main St. Orlando, FL 32555 und 123 Main St. Las Vegas, NV
3	Straßenübereinstimmung mit Abweichungswert -2. Das bedeutet, dass die Straße übereinstimmt, die Berechnung aber zu einem Abweichungswert von -2 geführt hat. Beispiel: 123 Main St. Las Vegas, NV 89111 und 123 Main St. Las Cruces, NM.
4	Straßenübereinstimmung mit Abweichungswert -1. Das bedeutet, dass die Straße übereinstimmt, die Berechnung aber zu einem Abweichungswert von -1 geführt hat. Beispiel: 123 Main St. Las Vegas, NV 89111 und 123 Main St. Las Vegas, NM 54633.
5	Straßenübereinstimmung mit Wert 0 (Basis). Das bedeutet, dass die Straße übereinstimmt, die Berechnung aber 0 ergeben hat. Beispiel: 123 Main St. Las Vegas, NV 89111 und 123 Main St.
6	Straßenübereinstimmung mit Übereinstimmungswert +1. Das bedeutet, dass die Straße übereinstimmt, die Berechnung aber +1 ergeben hat. Beispiel: 123 Main St. Las Vegas, NV 89111 und 123 Main St. Las Vegas
7	Straßenübereinstimmung mit Übereinstimmungswert +2. Das bedeutet, dass die Straße übereinstimmt, die Berechnung aber +2 ergeben hat. Beispiel: 123 Main St. Las Vegas, NV 89111 und 123 Main St. Las Vegas, NV.
8	Straßenübereinstimmung mit allen Teilen, US-Postleitzahl +4 fehlt. Das bedeutet, dass alle Teile der Adresse, übereinstimmen, die US-Postleitzahl +4 jedoch nicht vorhanden ist. Beispiel: 123 Main St. Las Vegas, NV 89111 und 123 Main St. Las Vegas, NV 89111
9	Exakte Übereinstimmung (Straße mit allen Teilen). Diese Auswahl bedeutet, dass alle Teile der Adresse, einschließlich der US-Postleitzahl +4, übereinstimmen. Beispiel: 123 Main St. Las Vegas, NV 89111-1234 und 123 Main St. Las Vegas, NV 89111-1234 **Anmerkung:** Dies funktioniert nur, wenn die in den USA übliche vierstellige Erweiterung des Postleitzahlencodes verwendet wird.

Genauigkeitsstufe 1

Jede der Genauigkeitsstufen von eins bis neun stellt eine steigende Genauigkeitsstufe dar, ausgenommen Stufe eins. Stufe eins stellt einen besonderen Fall dar, in dem Adressinformationen übereinstimmen, jedoch bei der Angabe der Himmelsrichtung der Straße, d. h. North/South (Nord/Süd) oder East/West (Ost/West), eine Abweichung aufweisen. Beispiel: 456 North Main Street Sometown, Nevada und 456 South Main Street Sometown, Nevada. In diesem Fall stimmen die Adressen möglicherweise überein, bei der Angabe für US-Postleitzahl + 4 liegt jedoch definitiv eine Abweichung vor. Oberflächlich betrachtet könnten diese Adressen für eine Auflösung geeignet sein. Diese Adressen sollten jedoch nicht gegeneinander aufgelöst werden, da es sich tatsächlich um verschiedene Adressen handelt. Da dieser zunächst für eine Adressauflösung scheinbar gut geeignete Fall im Gegenteil keinesfalls für eine Auflösung in Betracht gezogen werden darf, befindet sich der Wert, der der Genauigkeitsstufe dieses Szenarios zugeordnet ist, am Ende der Skala (Stufe eins), um zu verhindern, dass solche Adressen aufgelöst werden.

Stufe 1 kann auch auf einen absichtlichen Adressfehler hinweisen. Einige Kunden sind besonders an Mustern von absichtlichen Adressabweichungen interessiert, d. h. an Fällen, in denen Personen zu Betrugszwecken eine Adresse absichtlich ändern. Aus diesem Grund kann die Reihenfolge der Auflösungsregeln so konfiguriert werden, dass niedrige Adressgenauigkeitsstufen wie Stufe 1 berücksichtigt werden.

Anmerkung: Wenn Stufe 1 für die Auflösung von Entitäten von Bedeutung ist (wenn Sie beispielsweise ermitteln wollen, ob jemand widersprüchliche Angaben zum Adressteil US-Postleitzahl + 4 macht), müssen Sie eine separate Auflösungsregel erstellen. Diese Regel muss der Standardauflösungsregel vorangestellt werden, die alle Genauigkeitsstufen von fünf und höher berücksichtigt. Auf Grund der Komplexität einer ordnungsgemäßen Erstellung neuer Auflösungsregeln sollten Sie dies nur mit ausreichendem eigenen Fachwissen oder mithilfe von IBM ausführen.

Detaillierte Beispiele für die Adressgenauigkeit:

Die folgenden Beispiele stellen die für den Vergleich verwendeten Daten zusammen mit der resultierenden Bewertung der Adressgenauigkeit dar.

Die erste Adresse stellt die in der Entitätendatenbank vorhandene Adresse dar und die zweite Adresse stellt die eingehende Adresse dar.

Genauigkeitsstufe 1 - Straßenübereinstimmung mit allen Teilen, US-Postleitzahl +4 abweichend.

Dieser Fall zeigt zwei Adressen in derselben Straße, bei denen es sich jedoch um unterschiedliche Adressen handelt. Die eine Adresse liegt am nördlichen Ende der Straße, die andere hingegen am südlichen Ende. Der einzige Unterschied zwischen diesen beiden Adressen liegt in den Werten für PLZ+4.

STRASSE	STADT	BUNDESSTAAT	POSTLEITZAHL
123 N Main St	Fairmount	IN	46928-1655
123 S Main St	Fairmount	IN	46928-1924

Anmerkung: Genauigkeitsstufe eins stellt einen besonderen Fall dar, in dem Adressinformationen übereinstimmen, jedoch bei der Angabe der Himmelsrichtung der Straße, d. h. North/South (Nord/Süd) oder East/West (Ost/West), eine Ab-

weichung aufweisen. Oberflächlich betrachtet könnten diese Adressen für eine Auflösung geeignet sein. Diese Adressen dürfen jedoch nicht gegeneinander aufgelöst werden, da es sich tatsächlich um verschiedene Adressen handelt. Da dieser zunächst für eine Auflösung scheinbar gut geeignete Fall im Gegenteil keinesfalls für eine Auflösung in Betracht gezogen werden darf, wird der Wert für dieses Szenario ganz an das untere Ende der Skala (1) gestellt, um zu verhindern, dass solche Adressen aufgelöst werden.

Genauigkeitsstufe 2 - Straßenübereinstimmung, alle Teile abweichend.

Dieses Beispiel zeigt zwei Adressen mit identischer Straße, aber unterschiedlichen Angaben zu Stadt, Bundesstaat und Postleitzahl. Die zweite Adresse ist offensichtlich falsch (möglicherweise absichtlich), da Postleitzahlen in Nevada normalerweise immer die Anfangsziffern 89 haben.

STRASSE	STADT	BUNDESSTAAT	POSTLEITZAHL
123 E Main St	Fairmount	IN	46928
123 S Main St	Las Vegas	NV	46999

Genauigkeitsstufe 3 - Straßenübereinstimmung mit Abweichungswert -2.

In diesem Beispiel stimmen nur die Straßenangaben überein. In der eingehenden Adresse ist kein Bundesstaat angegeben und die Stadt- und Postleitzahlangaben sind widersprüchlich.

STRASSE	STADT	BUNDESSTAAT	POSTLEITZAHL
123 E Main St	Delphi	IN	46923-1522
123 E Main St	Fairmount		46928

Genauigkeitsstufe 4 - Straßenübereinstimmung mit Abweichungswert -1.

Dieses Beispiel zeigt zwei Adressen mit übereinstimmenden Angaben für Straße und Bundesstaat, aber widersprüchlichen Angaben zu Stadt und Postleitzahl.

STRASSE	STADT	BUNDESSTAAT	POSTLEITZAHL
123 E Main St	Delphi	IN	46923-1522
123 E Main St	Fairmount	IN	46928-1924

Genauigkeitsstufe 5 - Straßenübereinstimmung mit Wert 0 (Basis).

In diesem Beispiel ist in der eingehenden Adresse nur die Straße angegeben. Obwohl die Adresse keine Angaben zu Stadt, Bundesstaat oder Postleitzahl enthält, erhält die Übereinstimmung die Ausgangsbewertung für Adressgenauigkeit, Stufe 5. Die Genauigkeitsbewertung berücksichtigt die fehlenden Adressteile (nicht zu verwechseln mit widersprüchlichen Adressteilen, da fehlende Adressteile nicht bewertet werden).

STRASSE	STADT	BUNDESSTAAT	POSTLEITZAHL
220 JEFFERSON	BUFFALO	IA	
220 Jefferson St.			

Genauigkeitsstufe 6 - Straßenübereinstimmung mit Übereinstimmungswert +1.

Dieses Beispiel zeigt eine eingehende Straßenadresse ohne Angaben zu Bundesstaat oder Postleitzahl, jedoch mit identischen Angaben zu Straße und Stadt. Bei der eingehenden Adresse handelt es sich höchstwahrscheinlich um die richtige Adresse, bei der jedoch Daten fehlen.

STRASSE	STADT	BUNDESSTAAT	POSTLEITZAHL
220 Washington	Syracuse	NY	
220 Washington Sq.	Syracuse		

Genauigkeitsstufe 7 - Straßenübereinstimmung mit Übereinstimmungswert +2.

Dieses Beispiel zeigt übereinstimmende Angaben zu Straße, Stadt und einfacher Postleitzahl, in der eingehenden Adresse ist jedoch kein Bundesstaat angegeben.

STRASSE	STADT	BUNDESSTAAT	POSTLEITZAHL
220 JEFFERSON	BUFFALO	IA	52728
220 Jefferson St.	Buffalo		52728

Genauigkeitsstufe 8 - Straßenübereinstimmung mit allen Teilen, US-Postleitzahl +4 fehlt.

In diesem Beispiel stimmen die beiden Adressen überein, die Adressbereinigung konnte die Adressen jedoch nicht auswerten, sodass sie keinen Wert für PLZ+4 erhielten.

STRASSE	STADT	BUNDESSTAAT	POSTLEITZAHL
220 JEFFERSON	BUFFALO	IA	52728
220 Jefferson St.	Buffalo	IA	52728

Genauigkeitsstufe 9 - Exakte Übereinstimmung (Straße mit allen Teilen). Diese Auswahl bedeutet, dass alle Teile der Adresse, einschließlich der US-Postleitzahl +4, übereinstimmen.

In diesem Beispiel haben die beiden Adressen übereinstimmende Angaben zu Straße, Stadt, Bundesstaat und PLZ+4. Die beiden verglichenen Adressen erhalten daher die höchste Bewertung für die Adressgenauigkeit.

Anmerkung: Dies funktioniert nur, wenn die in den USA übliche vierstellige Erweiterung des Postleitzahlencodes verwendet wird.

STRASSE	STADT	BUNDESSTAAT	POSTLEITZAHL
123 W Main St	Camden	IN	46917-9997
123 W Main	Camden	IN	46917-9997

Namensgenauigkeit:

Namensgenauigkeit ist der Bewertungsprozess, mit dem die Entitätsauflösung ermittelt, ob zwei verglichene Namen denselben Namen darstellen.

Die Namensgenauigkeitsbewertung basiert auf der Verwendung von zwei möglichen Algorithmen.

- Namensvergleichsoperator 1.0
- Namensvergleichsoperator 2.0

Jeder Algorithmus hat seinen eigenen Satz von Namensübereinstimmungskriterien, die bei der Konfiguration von Auflösungsregeln konfiguriert werden können.

Jeder dieser beiden Algorithmen kann mit der Komponente Name Manager eingesetzt werden. Name Manager ist eine separat konfigurierbare Komponente, die den Namensabgleich auf zusätzliche Abgleichfunktionen basierend auf eindeutigen kulturellen Aspekten erweitert.

Vergleichsaspekte

Der Namensvergleichsoperator 1.0 ist die Standardeinstellung für Upgradeinstallationen von Version 3.9.0 und früher. Der Namensvergleichsoperator 2.0 ist die Standardeinstellung für Upgradeinstallationen von Version 3.9.1 und höher und bei Neuinstallationen.

Berücksichtigen Sie bei der Auswahl des für Ihre Erfordernisse am besten geeigneten Algorithmus die Vorteile der einzelnen Algorithmen.

Namensvergleichsoperator 1.0:

- Erfordert weniger CPU-Belastung, was zu besserer Leistung führt.
- Vermittelt einen genaueren Überblick darüber, warum Namen übereinstimmen.

Namensvergleichsoperator 2.0:

- Handhabt Namen besser, die aus mehr als drei Wörtern bestehen.
- Gleicht in falscher Reihenfolge vorliegende Wörter besser ab.
- Führt die Suche nach groben Übereinstimmungen besser aus.
- Gleicht Namen von Unternehmen besser ab.
- Handhabt Initialen besser.

Namensvergleichsoperator 1.0:

Dieser Namensabgleichsalgorithmus wurde primär für Namen konzipiert, die aus zwei oder drei Wörtern bestehen. Er ist die Standardeinstellung für Namensabgleich bei Upgrades von Version 3.9.0 und früher.

Der Namensvergleichsoperator 1.0 vergleicht zwei Namen und stuft anschließend ihre Ähnlichkeit nach 15 eindeutigen Ähnlichkeitsstufen ein.

Tabelle 30. Namensvergleichsoperator 1.0 - Genauigkeitsstufen

Stufe	Beschreibung
1	Nur teilweise Übereinstimmung bei Vor- oder Nachnamen BEISPIEL: John Jacob Smith = Joe Smithson
2	Nur exakte Übereinstimmung bei Vor- oder Nachnamen BEISPIEL: John Jacob Smith = Jonathan Henry Smith

Tabelle 30. Namensvergleichsoperator 1.0 - Genauigkeitsstufen (Forts.)

3	Starke Hash-Übereinstimmung BEISPIEL: Joe Smith = Joe Snith
4	Nur die Nachnamen sind unterschiedlich, aber geänderte Reihenfolge BEISPIEL: Bob Jacob Smith = Jacob Bob Jones
5	Nur die Nachnamen sind unterschiedlich BEISPIEL: Bob Jacob Smith = Bob Jacob Jones
6	Übereinstimmung standardisierter Namen mit einigen Abweichungen BEISPIEL: John Jacob Smith = Jonathan Henry Smith
7	Übereinstimmung standardisierter Namen BEISPIEL: Joe W Anderson = Joseph Andersen
8	Standardisierte Übereinstimmung mit exakten Nachnamen, Übereinstimmung der Mittelinitiale, aber geänderte Reihenfolge BEISPIEL: J Bob Smith = Robert J Smith
9	Standardisierte Übereinstimmung mit exakten Nachnamen, Übereinstimmung der Mittelinitiale BEISPIEL: Joe W Anderson = Joseph W Anderson
10	Standardisierte Übereinstimmung mit exakten Nachnamen, aber geänderte Reihenfolge BEISPIEL: Bob Smith = Robert Smith
11	Standardisierte Übereinstimmung mit exakten Nachnamen BEISPIEL: John Jacob Smith = Johnny Jake Smith
12	Übereinstimmung unaufbereiteter Namen mit Übereinstimmung der Mittelinitiale, aber geänderte Reihenfolge BEISPIEL: Joe W. Brown = Will Joe Brown
13	Übereinstimmung unaufbereiteter Namen mit Übereinstimmung der Mittelinitiale BEISPIEL: Joe W Anderson = Joe W Anderson
14	Übereinstimmung unaufbereiteter Namen, aber geänderte Reihenfolge BEISPIEL: John Bob Smith = Bob John Smith
15	Übereinstimmung unaufbereiteter Namen BEISPIEL: Joe William Anderson = Joe William Anderson

Namensvergleichsoperator 2.0:

Dieser Namensabgleichsalgorithmus versieht verglichene Namen mit Token. Er teilt die Wörter, aus denen die Namenszeichenfolge zusammengesetzt ist, in einzelne Namen oder Token auf. Anschließend vergleicht der Algorithmus die Token

miteinander und erstellt für jedes Token eine Bewertung. Er ist die Standardeinstellung für Namensabgleich bei Upgradeinstallationen von Version 3.9.1 und höher und bei Neuinstallationen.

Der Namensvergleichsoperator 2.0 gruppiert Namen in drei Kategorien, die anschließend verglichen und bewertet werden:

- Vorname (erster und zweiter Vorname bzw. alle Namen mit Ausnahme des Nachnamens)
- Familienname (Nachname)
- Vollständiger Name (alle Namen)

Mit diesen drei Bewertungskategorien können Sie den Namensabgleich für bestimmte Auflösungsregeln optimieren, damit Ihre Namensabgleichsanforderungen erfüllt werden. Bewertungen basieren auf ganzen Zahlen und reichen von 0-100, wobei 0 die niedrigste und 100 die höchste Bewertung darstellt. Je höher die Bewertung in einer Kategorie, desto genauer stimmen die Namen in der betreffenden Kategorie überein.

Konfigurationsaspekte - Bewertungsrichtlinien

Verwenden Sie die folgenden Bewertungsrichtlinien beim Konfigurieren der Namensschwellenwerte von Auflösungsregeln, wenn Sie Namensabgleichseinstellungen für den Namensvergleichsoperator bearbeiten oder ändern. Diese Richtlinien sind auch hilfreich, wenn Sie die Bewertungsergebnisse der Bewertungskategorien dieses Algorithmus interpretieren.

Bewertung des vollständigen Namens

Auf der Basis der Bewertung von 0 - 100 und mithilfe der folgenden Richtlinien können Sie ermitteln, welche Abgleichstufe sich aus der Bewertung des vollständigen Namens ergibt:

- 100 = Exakte Übereinstimmung
- 90 = Sehr gute Übereinstimmung (für die Auflösung von Name und Geburtsdatum geeignet)
- 80 = Gute Übereinstimmung (für die meisten Auflösungsregeln geeignet)
- 70 = Mittlere Übereinstimmung (geeignet, wenn auch eindeutige Nummern vorhanden sind)
- Unter 70 = Nicht für einen Abgleich geeignet

Bewertung des Vornamens

Auf der Basis der Bewertung von 0 - 100 und mithilfe der folgenden Richtlinien können Sie ermitteln, welche Abgleichstufe sich aus der Bewertung des Vornamens ergibt:

- 100 = Exakte Übereinstimmung
- 90 = Sehr gute Übereinstimmung (weist auf einen möglichen Austausch von Vor- und Familiennamen hin)
- 85 = Geringste akzeptable Übereinstimmung
- Unter 85 = Nicht für einen Abgleich geeignet; möglicherweise in Kombination mit dem Vornamen oder dem vollständigen Namen nützlich, um eine gewisse Ähnlichkeit sicherzustellen.

Bewertung des Familiennamens

Auf der Basis der Bewertung von 0 - 100 und mithilfe der folgenden Richtlinien können Sie ermitteln, welche Abgleichstufe sich aus der Bewertung des Familiennamens ergibt:

- 100 = Exakte Übereinstimmung
- 90 = Sehr gute Übereinstimmung (weist auf einen möglichen Austausch von Vor- und Familiennamen hin)
- 85 = Geringste akzeptable Übereinstimmung
- Unter 85 = Nicht für einen Abgleich geeignet; möglicherweise in Kombination mit dem Vornamen oder dem vollständigen Namen nützlich, um eine gewisse Ähnlichkeit sicherzustellen.

Name Manager-Namensbewertung:

Der Name Manager-Algorithmus bewertet eingehende Namensdaten, indem er den Namen in Namensteile aufspaltet und anschließend die Kultur für jeden Namensteil bestimmt. Der Algorithmus bewertet anschließend jeden Namensteil und die resultierenden Bewertungen werden während der Entitätsauflösung verwendet.

Obwohl der Name Manager-Algorithmus von den Name Comparator-Algorithmen (NC1 und NC2) getrennt ist, müssen Sie weiterhin NC1 oder NC2 auswählen. Während des Entitätsauflösungsprozesses werden Namen zunächst auf Basis der ausgewählten Name Comparator-Algorithmen bewertet. Wenn der Name als exakte Übereinstimmung bewertet wird, überspringt die Entitätsauflösung die Name Manager-Bewertung, da die exakte Übereinstimmung den Namensbewertungsteil der Auflösungsregel erfüllt. Wenn der eingehende Name eine Bewertung erhält, die unter einer exakten Übereinstimmung liegt, wird der Name vom Entitätsauflösungsprozess mithilfe des Name Manager-Algorithmus bewertet.

Zunächst parst der Algorithmus den Namen in Namensteile (Vorname, Familienname und vollständiger Name) und ermittelt anschließend die Kultur für jeden Namensteil. Zuletzt weist der Algorithmus jedem Namensteil eine Bewertung zu und vergleicht die Bewertungen mit den Name Manager-Bewertungsschwellenwerten, um zu ermitteln, wie hoch die Übereinstimmung der Namen ist. Je höher der Bewertungsschwellenwert ist, desto höher muss die Übereinstimmung zwischen den eingehenden Namensdaten und den Namensteilen aus der vorhandenen Entität in der Entitätendatenbank sein.

Genauigkeit des Geburtsdatums:

Die Genauigkeit des Geburtsdatums ist der Bewertungsprozess, mit dem die Entitätsauflösung ermittelt, ob zwei verglichene Geburtsdaten dasselbe Datum darstellen.

Dieser Vergleich berücksichtigt verschiedene Methoden zur Bewertung der Ähnlichkeit von Geburtsdatenzeichenfolgen, einschließlich Position der ganzen Zahlen, Umsetzungen und Deltas von Tages-, Monats- und Jahreswerten. Die Angaben werden analysiert, um eine Ähnlichkeit von 2 bis 100 zu ermitteln. Sie können die Einstellungen der Genauigkeit des Geburtsdatums basierend auf vier Ähnlichkeitskategorien konfigurieren:

- Exakt: Übereinstimmung mit 100 Punkten
- Stark: Übereinstimmung mit >=90 Punkten
- Mittel: Übereinstimmung mit >=85 Punkten
- Grob: Übereinstimmung mit >=80 Punkten

Aspekte der Konfiguration

Das System stellt die vorkonfigurierte Einstellung **Stark** als Ähnlichkeitsmindeststufe bereit. Sie muss erreicht werden, damit eine Auflösungsregel zwei verglichene Geburtsdaten als identisch erachtet. Eine Änderung dieser Einstellung wirkt sich auf die Anzahl Übereinstimmungen aus und kann sich auch auf die Anzahl der vom System ausgeführten Entitätsauflösungen auswirken. Ändern Sie diese Einstellung nur, wenn dies unabdingbar ist, und stellen Sie sicher, dass Sie Änderungen testen, bevor Sie sie in einer Produktionsumgebung implementieren.

Detaillierte Beispiele für die Genauigkeit von Geburtsdaten:
Die folgenden Beispiele stellen die für den Vergleich verwendeten Daten zusammen mit der resultierenden Bewertung der Genauigkeit des Geburtsdatums dar. Das erste Geburtsdatum stellt das vorhandene Geburtsdatum einer Entität in der Entitätendatenbank dar und das zweite Geburtsdatum ist das Geburtsdatum einer eingehenden Identität.

Genauigkeitsstufe: Exakt (100 Punkte)

Dieses Beispiel zeigt zwei exakt übereinstimmende Geburtsdaten. Der Algorithmus wird eine Übereinstimmung mit 100 Punkten generieren.

GEBURTSDATUM	STATUS
1963/12/01	Vorhanden
1963/12/01	Eingehend

Genauigkeitsstufe: Stark (90 Punkte)

Dieses Beispiel zeigt zwei Daten mit einer Genauigkeitsbewertung von größergleich 90 Punkten. Das Beispiel zeigt zwei Geburtsdaten mit übereinstimmenden Werten für Jahr und Tag, aber mit einem um eins abweichenden Wert für Monat.

GEBURTSDATUM	STATUS
1963/12/01	Vorhanden
1963/11/01	Eingehend

Genauigkeitsstufe: Mittel (85 Punkte)

Dieses Beispiel zeigt zwei Daten mit einer Genauigkeitsbewertung von größergleich 85 Punkten. Das Beispiel zeigt zwei Geburtsdaten mit übereinstimmenden Werten für Monat und Tag, aber mit einem Zahlendreher der letzten beiden Ziffern des Werts für Jahr.

GEBURTSDATUM	STATUS
1963/12/01	Vorhanden
1936/12/01	Eingehend

Genauigkeitsstufe: Grob (80 Punkte)

Dieses Beispiel zeigt zwei Daten mit einer Genauigkeitsbewertung von größergleich 80 Punkten. Das Beispiel zeigt zwei Geburtsdaten mit übereinstimmenden

Werten für Monat und Tag, aber einer Abweichung bei der dritten Ziffer des Werts für Jahr (dies ergibt trotzdem ein gültiges Geburtsdatum).

GEBURTSDATUM	STATUS
1963/12/01	Vorhanden
1933/12/01	Eingehend

Anzeigen von Auflösungsregeln

Sie können die aktuelle Gruppe von Auflösungsregeln anzeigen, bevor Sie Auflösungsregeln hinzufügen oder löschen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Auflösung** an.
3. Klicken Sie die Registerkarte **Auflösungsregeln** an.
4. Wählen Sie in der Dropdown-Liste **Auflösungskonfiguration** eine Auflösungskonfiguration aus.
5. Klicken Sie zum Anzeigen der Details für eine bestimmte Auflösungsregel den Link in der Zeile an, die diese Auflösungsregel enthält.

Erstellen von Auflösungsregeln

Nach der sorgfältigen Untersuchung Ihrer geschäftlichen Anforderungen und der Prüfung der vorhandenen Auflösungsregeln empfiehlt es sich möglicherweise, neue Auflösungsregeln für Ihre Daten zu erstellen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Auflösung** an.
3. Klicken Sie die Registerkarte **Auflösungsregeln** an.
4. Wählen Sie in der Dropdown-Liste **Auflösungskonfiguration** eine Auflösungskonfiguration aus.
5. Klicken Sie die Schaltfläche **Neu** an.
6. Geben Sie auf der Registerkarte **Allgemein** die Werte an, die beim Vergleichen der Daten von zwei Entitäten verwendet werden sollen.
7. Klicken Sie die Registerkarte **Kandidatenschwellenwerte** an.
8. Geben Sie auf der Registerkarte **Kandidatenschwellenwerte** die Schwellenwerte für die Daten an.
9. Klicken Sie die Registerkarte **Schwellenwerte für Bestätigung/Zurückweisung** an.
10. Geben Sie auf der Registerkarte **Schwellenwerte für Bestätigung/ Zurückweisung** die Schwellenwerte für die Daten an.
11. Klicken Sie die Schaltfläche **Speichern** an.

Löschen von Auflösungsregeln

Wenn eine Auflösungsregel beim Entitätsauflösungsprozess nicht mehr berücksichtigt werden soll, löschen Sie die Regel.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Auflösung** an.

3. Klicken Sie die Registerkarte **Auflösungsregeln** an.
4. Wählen Sie in der Dropdown-Liste **Auflösungskonfiguration** eine Auflösungskonfiguration aus.
5. Wählen Sie das Kontrollkästchen neben den Auflösungsregeln aus, die Sie löschen wollen.
6. Klicken Sie die Schaltfläche **Löschen** an.
7. Klicken Sie **OK** im Bestätigungsfenster an, um die Auflösungskonfiguration zu löschen.

Hilfethemen

Fenster 'Auflösungsregeln':

Über diese Anzeige können Sie die Auflösungsregeln anzeigen, die in einer Auflösungskonfiguration enthalten sind. Auflösungsregeln werden in der aufgelisteten Reihenfolge verarbeitet. Wenn eine Auflösungsregel erfüllt ist, werden die zugeordneten Auflösungsbewertungen angewendet. Ist die Regel so konfiguriert, dass sie eine Auflösung auslöst, wird die eingehende Identität in die vorhandene Entität aufgelöst und für diesen Vergleich werden keine weiteren Entitätsauflösungsregeln mehr verarbeitet.

Reihenfolge
Reihenfolge, in der die Auflösungsregeln auf die eingehende Identität und die vorhandene Entität angewendet werden, die verglichen werden.

Beschreibung
Beschreibung der Auflösungsregel.

Übereinstimmungswahrscheinlichkeit für Auflösung
Auflösungsbewertung, die auf den Vergleich angewendet wird, wenn die Regel erfüllt ist.

Übereinstimmungswahrscheinlichkeit für Beziehung
Beziehungsbewertung, die auf den Vergleich angewendet wird, wenn die Regel erfüllt ist.

Löst Auflösung aus.
Gibt an, ob die Regel die eingehende Identität automatisch in die vorhandene Entität auflöst, wenn die Regel erfüllt ist.

Auflösungsregeln - Registerkarte 'Allgemein':

Über diese Registerkarte können Sie eine neue Auflösungsregel konfigurieren oder die Details für eine vorhandene Auflösungsregel anzeigen.

Reihenfolge
Geben Sie eine eindeutige Zahl ein, die die Reihenfolge für die Verarbeitung der Regel angibt.

Beschreibung
Geben Sie die Beschreibung für die Regel ein.

Übereinstimmungswahrscheinlichkeit für Auflösung
Geben Sie eine Übereinstimmungswahrscheinlichkeit für die Ähnlichkeit in Prozent ein, wenn diese Regel erfolgreich ist. Nur bei 100 % wird eine Auflösung erwogen.

Übereinstimmungswahrscheinlichkeit für Beziehung
Geben Sie eine Übereinstimmungswahrscheinlichkeit für die Beziehung in Prozent ein, wenn diese Regel erfolgreich ist. Nur bei 100 % wird eine Auflösung erwogen.

Löst Auflösung aus.
Wählen Sie **Ja** aus, um die eingehende Identität und die vorhandene Entität aufzulösen, wenn die Übereinstimmungswahrscheinlichkeit für Auflösung und die Übereinstimmungswahrscheinlichkeit für Beziehung 100 % sind.

Zurückweisungen aktiviert
Wählen Sie **Ja** aus, um die Verarbeitung von Bestätigungen/Zurückweisungen zu aktivieren. Andernfalls wird keine Verarbeitung von Zurückweisungen ausgeführt.

Merkmalzurückweisungen aktiviert
Wählen Sie **Ja** aus, um die Verarbeitung von Merkmalbestätigungen/-zurückweisungen zu aktivieren. Andernfalls wird keine Verarbeitung von Merkmalzurückweisungen ausgeführt.

Auflösungsregeln - Registerkarte 'Kandidatenschwellenwerte':

Über diese Registerkarte können Sie die Einstellungen für den Kandidatenschwellenwert einer neuen Auflösungsregel angeben oder die Details für den Kandidatenschwellenwert einer vorhandenen Auflösungsregel anzeigen. Diese Einstellungen definieren die Beschreibung der Auflösungsregel, die auf der Registerkarte **Allgemein** für die Auflösung eingegeben wird.

Schwellenwert für Adressgenauigkeit
Wählen Sie den mindestens erforderlichen Rang in der Adressreihenfolge aus, damit die Regel als erfüllt betrachtet wird.

Schwellenwert für ungefähre Adressen
Wählen Sie die mindestens erforderlichen ungefähren Adresswertübereinstimmungen aus, damit die Regel als erfüllt betrachtet wird.

Schwellenwert für räumliche Nähe
Wählen Sie die mindestens erforderlichen Adressen in dem durch die Qualitätsregel definierten Bereich aus, damit die Regel als erfüllt betrachtet wird.

Schwellenwert für eindeutige Zahl
Wählen Sie die mindestens erforderlichen Übereinstimmungen für eindeutige Zahlen aus, damit die Regel als erfüllt betrachtet wird.

Schwellenwert für nicht eindeutige Zahl
Wählen Sie die mindestens erforderlichen Übereinstimmungen für nicht eindeutige Zahlen aus, damit die Regel als erfüllt betrachtet wird.

Schwellenwert für Merkmale
Wählen Sie die mindestens erforderlichen Merkmalübereinstimmungen aus, damit die Regel als erfüllt betrachtet wird.

Schwellenwert für E-Mail-Adresse
Wählen Sie die mindestens erforderlichen Übereinstimmungen für E-Mail-Adressen aus, damit die Regel als erfüllt betrachtet wird.

Schwellenwert für Datensummen
Wählen Sie die mindestens erforderliche Summe der Übereinstimmungen für eindeutige Zahlen, andere Zahlen, Adressen, Merkmale und E-Mail-Adressen aus, damit die Regel als erfüllt betrachtet wird.

Schwellenwert für Summe
Wählen Sie die mindestens erforderliche Summe der Übereinstimmungen für die räumliche Nähe von Adressen, für ungefähre Adressen, ähnliche Nummern und Geburtsdaten aus, damit die Regel als erfüllt betrachtet wird.

Auflösungsregeln - Registerkarte 'Schwellenwerte für Bestätigung/Zurückweisung':

Über diese Registerkarte können Sie die Einstellungen für den Bestätigungs- und Zurückweisungsschwellenwert für eine neue Auflösungsregel angeben oder die Details für den Bestätigungs- und Zurückweisungsschwellenwert einer vorhandenen Auflösungsregel anzeigen.

Schwellenwert für ähnliche Zahl
Wählen Sie die mindestens erforderlichen Übereinstimmungen für ähnliche Zahlen aus, damit die Regel als erfüllt betrachtet wird.

Schwellenwert für Geburtsdatum
Wählen Sie die Mindestübereinstimmungsquote für das Geburtsdatum aus, damit die Regel als erfüllt betrachtet wird.

Einstellungen für 'Namensvergleichsoperator'
Diese Einstellungen legen die Anforderungen für die Namensgenauigkeit bei der Entitätsauflösung fest. Diese Einstellungen werden eigenständig oder mit den Name Manager-Einstellungen angewendet.

Schwellenwert für Bewertung von Vornamen
Geben Sie einen Schwellenwert zwischen 0 und 100 für die Bewertung des Vornamens ein.

Schwellenwert für Bewertung von Familiennamen
Geben Sie einen Wert zwischen 0 und 100 als Schwellenwert für die Bewertung des Familiennamens ein.

Schwellenwert für Bewertung von vollständigen Namen
Geben Sie einen Wert zwischen 0 und 100 als Schwellenwert für die Bewertung des vollständigen Namens ein.

Name Manager-Einstellungen
Name Manager erweitert die Standardnamensgenauigkeit um wichtige kulturelle Aspekte. Diese Einstellungen werden nur angewendet, wenn Name Manager konfiguriert ist.

Schwellenwert für Bewertung von Vornamen
Geben Sie die mindestens erforderliche Bewertung des Vornamens ein, damit die Regel als erfüllt betrachtet wird.

Der Schwellenwert muss ein ganzzahliger Wert zwischen 0 und 100 sein. Je höher die Bewertung ist, umso größer ist die Übereinstimmung. Eine Bewertung unter 70 ist in der Regel nicht für einen Abgleich geeignet, möglicherweise in Kombination mit dem Familiennamen oder dem vollständigen Namen jedoch nützlich, um eine gewisse Ähnlichkeit sicherzustellen.

Schwellenwert für Bewertung von Familiennamen
Geben Sie die mindestens erforderliche Bewertung des Familiennamens ein, damit die Regel als erfüllt betrachtet wird.

Der Schwellenwert muss ein ganzzahliger Wert zwischen 0 und 100 sein. Je höher die Bewertung ist, umso größer ist die Übereinstimmung. Eine Bewertung unter 70 ist in der Regel nicht für einen

Abgleich geeignet, möglicherweise in Kombination mit dem Vornamen oder dem vollständigen Namen jedoch nützlich, um eine gewisse Ähnlichkeit sicherzustellen.

Schwellenwert für Bewertung von vollständigen Namen
Geben Sie die mindestens erforderliche Bewertung des vollständigen Namens ein, damit die Regel als erfüllt betrachtet wird.

Der Schwellenwert muss ein ganzzahliger Wert zwischen 0 und 100 sein. Je höher die Bewertung ist, umso größer ist die Übereinstimmung. Eine Bewertung unter 70 ist in der Regel nicht für einen Abgleich geeignet.

Anpassen der Kandidatenerstellungsregel

Sie können die Einstellungen für die Kandidatenerstellungsregel ändern, indem Sie Konfigurationen für Kandidatenerstellungsregeln verwenden. Änderungen an der Funktion für die Kandidatenerstellungsregel werden über die Konfigurationskonsole vorgenommen.

Kandidatenerstellungsregel

Die Komponente für Kandidatenerstellungsregeln definiert Kriterien, mit denen das System der Kandidatenliste im Rahmen des Entitätsauflösungsprozesses eine vorhandene Entität hinzufügt.

Zu typischen Einstellungen der Kandidatenerstellungsregel zählen Adresse, eindeutige Nummern und andere Nummern. Das System vergleicht diese Datentypen, um zu ermitteln, welche vorhandenen Entitäten in eine eingehende Identität aufgelöst werden könnten. Wenn ein neuer Identitätsdatensatz in das System aufgenommen wird und eine vorhandene Entität über einen übereinstimmenden Wert für einen der von der Kandidatenerstellungsregel festgestellten Datentypen verfügt, wird diese Entität der Kandidatenerstellungsregel hinzugefügt.

Konfigurationen für Kandidatenerstellungsregeln

Die Einstellungen der Kandidatenerstellungsregel sind nach Konfigurationen für Kandidatenerstellungsregeln organisiert. In einer Auflösungskonfiguration kann nur jeweils eine Konfiguration für Kandidatenerstellungsregeln verwendet werden.

Im Produktumfang sind folgende Konfigurationen für Kandidatenerstellungsregeln enthalten:

- **Default**: Diese Einstellung schließt Adresse, eindeutige Nummern und andere Nummern als Kriterien für die Aufnahme einer Entität in die Kandidatenliste ein.
- **Default with name only**: Diese Einstellung schließt Namen als Kriterium für die Aufnahme einer Entität in die Kandidatenliste ein. Diese Einstellung sollte verwendet werden, wenn Ihre Entitätsdaten ausschließlich Namen oder Namen und sehr wenige andere Datentypen enthalten.

Aspekte der Konfiguration

Generische Daten wirken sich direkt darauf aus, ob ein Wert im Prozess für Kandidatenerstellungsregeln berücksichtigt wird. Ein als generischer Wert interpretierter Wert wird nicht mehr zum Generieren von Kandidatenlisten verwendet.

Die Einstellungen der Kandidatenerstellungsregel wirken sich unmittelbar auf die Systemleistung aus. Wenn das System zum Vergleichen einer eingehenden Identität

mit jeder Entität in der Entitätendatenbank Indexsuchen verwendet, werden nur Datentypen verglichen, die in der Komponente für Kandidatenerstellungsregeln konfiguriert sind. Hierdurch können Kandidatenlisten sehr schnell generiert werden. Bei wachsender Entitätendatenbank und zunehmender Anzahl enthaltener Entitäten muss die Kandidatenerstellungsregel mehr Daten vergleichen. Wenn Ihre Entitätendatenbank z. B. 100.000 Entitäten enthält und die Kandidatenerstellungsregel so eingestellt ist, dass sie beim Erstellen der Kandidatenliste drei Datentypen vergleicht, kann das System bei der Aufnahme einer neuen Identität bis zu 300.000 Vergleiche durchführen, nur um die Kandidatenliste zu generieren. Wenn Ihre Entitätendatenbank 1.000.000 Entitäten enthält und die Kandidatenerstellungsregel so eingestellt ist, dass sie beim Erstellen der Kandidatenliste drei Datentypen vergleicht, kann das System bei der Aufnahme einer neuen Identität bis zu 3.000.000 Vergleiche durchführen, nur um die Kandidatenliste zu generieren. Wenn Sie ein einzelnes Kriterium für die Kandidatenerstellungsregel hinzufügen, kann das System bis zu 1.000.000 zusätzliche Vergleiche durchführen, um die Kandidatenliste zu generieren. Das heißt, dass bis zu 1.000.000 zusätzliche Vergleiche pro Identitätsdatensatz ausgeführt werden können, der in das System geladen wird. Wenn die Kandidatenlisten zu umfangreich sind, weil sie zu viele Datentypen berücksichtigen, wird der Entitätsauflösungsprozess im Vergleich zu Einstellungen der Kandidatenerstellungsregel, die nur die zum Erstellen effektiver Kandidatenlisten erforderlichen Datentypen enthalten, viel langsamer ausgeführt.

Beachten Sie bei der Frage, ob Sie die Konfigurationseinstellung **Default** oder **Default with name only** verwenden sollten, dass Sie bei der Auswahl von **Default with name only** Vergleiche in einer Größenordnung hinzufügen, die die von der Konfigurationseinstellung **Default** erforderte Größenordnung übersteigt.

Kandidatenlisten

Kandidatenlisten sind die Listen der Entitäten, die potenziell mit dem eingehenden Identitätsdatensatz übereinstimmen können. Die Kandidatenliste wird erstellt, indem die Entitäten abgerufen werden, die basierend auf den in der Konfiguration für Kandidatenerstellungsregeln angegebenen Attributen mit der eingehenden Identität Attribute gemeinsam haben.

Der Entitätsauflösungsprozess verwendet zum Auflösen von Entitäten und Beziehungen nur die in der Kandidatenliste aufgeführten Entitäten.

Da Entitätsauflösung und Beziehungserkennung auf der Grundlage von Attributen ermittelt werden, müssen Sie sorgfältig erwägen, welche Attribute in Ihren Datenquellen die stärksten Kandidaten erstellen.

Nach der Generierung der Kandidatenliste vergleicht der Entitätsauflösungsprozess die eingehende Identität unter Verwendung der konfigurierten Auflösungsregeln mit dem ersten Kandidaten in der Liste. Das System berechnet mit den Auflösungsregeln eine Auflösungsbewertung, die darstellt, wie stark die Attribute der eingehenden Identität mit den Attributen der Kandidatenentität übereinstimmen. Wenn die Attribute der eingehenden Identität die Auflösungsbewertung für diese Regel erfüllen oder übersteigen, wird der eingehende Identitätsdatensatz in die Kandidatenentität aufgelöst.

Wenn die Auflösungsbewertung die für diese Auflösungsregel festgelegte Auflösungsbewertung nicht erfüllt oder nicht übersteigt, springt das System zur nächsten Auflösungsregel, bis der eingehende Identitätsdatensatz in eine Kandidatenentität aufgelöst wurde oder alle Auflösungsregeln ausgeschöpft wurden.

Wenn der eingehende Identitätsdatensatz nicht in eine vorhandene Entität aufgelöst wird, löst das System den Datensatz in eine neue Entität auf und speichert die neue Entität in der Entitätendatenbank.

Erstellen von Konfigurationen für Kandidatenerstellungsregeln

Über die Konfigurationskonsole können Sie neue Gruppen von Einstellungen für Kandidatenerstellungsregeln erstellen. Diese Konfigurationen für Kandidatenerstellungsregeln sind sehr nützlich, da sie die Anwendung einer Reihe konfigurierter Einstellungen für Kandidatenerstellungsregeln durch Änderung einer einzigen Einstellung ermöglichen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Auflösung** an.
3. Klicken Sie die Registerkarte **Kandidatenerstellungsregel (Candidate Builder)** an.
4. Stellen Sie sicher, dass in der Dropdown-Liste **Konfiguration für die Kandidatenerstellungsregeln** der Eintrag **- - - Bitte auswählen - - -** angezeigt wird, und klicken Sie die Schaltfläche **Neu** an.
5. Geben Sie in das Feld **Konfiguration für die Kandidatenerstellungsregeln** den Namen der neuen Konfiguration für die Kandidatenerstellungsregeln ein.
6. Wählen Sie im Feld **Abgleichtyp** den ersten Datentyp aus, den Sie als Kandidatenkriterium für Auflösung verwenden wollen.
7. Geben Sie in das Feld **Segmentname** den Namen des UMF-Segments ein, in dem sich die Abgleichtypdaten befinden.
8. Klicken Sie die Schaltfläche **Speichern** an.

Nächste Schritte

Die gerade erstellte Konfiguration für die Kandidatenerstellungsregeln wird nun in der Dropdown-Liste **Konfiguration für die Kandidatenerstellungsregeln** angezeigt. Sie können dieser neuen Konfiguration Kriterien hinzufügen.

Hinzufügen von Kriterien zu Konfigurationen für Kandidatenerstellungsregeln

Über die Konfigurationskonsole können Sie vorhandenen Konfigurationen für Kandidatenerstellungsregeln, die während des Entitätsauflösungsprozesses als Kriterien für das Hinzufügen einer vorhandenen Entität zu der Kandidatenliste verwendet werden, Datentypen hinzufügen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Auflösung** an.
3. Klicken Sie die Registerkarte **Kandidatenerstellungsregel (Candidate Builder)** an.
4. Wählen Sie eine Konfiguration in der Dropdown-Liste **Konfiguration für die Kandidatenerstellungsregeln** aus.
5. Klicken Sie die Schaltfläche **Neu** an.
6. Wählen Sie einen Datentyp in der Dropdown-Liste **Abgleichtyp** aus.
7. Geben Sie in das Feld **Segmentname** den Namen des UMF-Segments ein, in dem sich die Abgleichtypdaten befinden.
8. Klicken Sie die Schaltfläche **Speichern** an.

Nächste Schritte

Nun berücksichtigt das System den gerade angegebenen Datentyp, wenn während des Entitätsauflösungsprozesses Kandidatenlisten erzeugt werden.

Löschen von Konfigurationen für Kandidatenerstellungsregeln

Über die Konfigurationskonsole können Sie eine Konfiguration für Kandidatenerstellungsregeln löschen. Sie können eine Konfiguration für Kandidatenerstellungsregeln löschen, wenn Sie feststellen, dass Sie sie nicht mehr benötigen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Auflösung** an.
3. Klicken Sie die Registerkarte **Kandidatenerstellungsregel (Candidate Builder)** an.
4. Wählen Sie eine Konfiguration in der Dropdown-Liste **Konfiguration für die Kandidatenerstellungsregeln** aus.
5. Wählen Sie das Kontrollkästchen neben einem beliebigen Abgleichtyp aus, den Sie löschen wollen.
6. Klicken Sie die Schaltfläche **Löschen** an. Ein Bestätigungsfenster mit der Nachricht, dass die ausgewählten Datensätze gelöscht werden, wird angezeigt.
7. Klicken Sie **OK** an, um das Löschen der Konfiguration für Kandidatenerstellungsregeln zu bestätigen.

Nächste Schritte

Die Gruppe der Einstellungen für Kandidatenerstellungsregeln, die Sie gerade gelöscht haben, kann nicht mehr während des Entitätsauflösungsprozesses zur Generierung von Kandidatenlisten verwendet werden.

Hilfethemen

Fenster 'Kandidatenerstellungsregel':

Über dieses Fenster können Sie eine Liste der Einstellungen für die Kandidatenerstellungsregel anzeigen. Einstellungen für die Kandidatenerstellungsregel sind nach Konfigurationen für Kandidatenerstellungsregeln gruppiert.

Feld 'Konfiguration für die Kandidatenerstellungsregeln'
: Wählen Sie die Konfiguration für die Kandidatenerstellungsregeln aus, deren Einstellungen Sie anzeigen wollen.

Abgleichtyp
: Der Typ der Daten, die zwischen einer eingehenden Identität und einer vorhandenen Entität übereinstimmen müssen, damit diese vorhandene Entität der Kandidatenliste für die Entitätsauflösung hinzugefügt wird.

Segmentname
: Der Name des UMF-Segments, in dem sich die Abgleichtypdaten befinden.

Abgleichreihenfolge
: Gruppennummer für die Reihenfolge, in der die Kandidatenlistenkriterien verglichen werden.

Kandidatenerstellungsregel - Registerkarte 'Allgemein':

Über diese Registerkarte können Sie ein neues Kriterium für die Kandidatenerstellungsregel konfigurieren oder die Details eines vorhandenen Kriteriums für die Kandidatenerstellungsregel anzeigen.

Konfiguration für die Kandidatenerstellungsregeln
Die Konfiguration für die Kandidatenerstellungsregeln, zu der dieses Kriterium gehört.

Abgleichtyp
Wählen Sie den Datentyp aus, der übereinstimmen muss, damit die vorhandene Entität als Kandidat für die Auflösung betrachtet wird.

Segmentname
Geben Sie den Namen des UMF-Segments ein, in dem sich die Abgleichtypdaten befinden: Eindeutige Nummer & Andere Nummer = NUMBER; Adresse = ADDRESS; Merkmal = ATTRIBUTE; Name = NAME; E-Mail = EMAIL_ADDR.

Konfigurieren von Bestätigungen und Zurückweisungen

Sie können Einstellungen für Bestätigungen und Zurückweisungen anpassen, um die Auflösungsbewertung für verglichene Entitäten zu ändern.

Informationen zu diesem Vorgang

Bestätigungen und Zurückweisungen können über die Registerkarte **Auflösungsregeln** der Konsole angezeigt und modifiziert werden.

Bestätigungen und Zurückweisungen

Nach der Erstellung einer Kandidatenliste und dem Vergleich der grundlegenden Auflösungskriterien vergleicht die Entitätsauflösung zusätzliche Kriterien, um eine Auflösungsbewertung zu stärken bzw. zu schwächen. Diese zusätzlichen Kriterien sind Bestätigungen und Zurückweisungen.

Bestätigungen und Zurückweisungen vergleichen die folgenden Datentypen:

- Geburtsdatum
- Eindeutige Nummer
- Generation
- Merkmale
  - Sie können ein beliebiges Merkmal zur Verwendung in Bestätigungen und Zurückweisungen angeben.

Die Bestätigungsgewichtung ist der Wert, mit dem die Basisauflösungsbewertung von zwei verglichenen Entitäten eine größere Gewichtung erhält. Die Zurückweisungsgewichtung ist der Wert (in der Regel ein negativer Wert), mit dem die Basisauflösungsbewertung von zwei verglichenen Entitäten eine kleinere Gewichtung erhält.

Beispiel

Eine Auflösungskonfiguration kann für das Geburtsdatum einen Bestätigungswert von +10 und einen Zurückweisungswert von -20 haben. Wenn der eingehende Datensatz ein Geburtsdatum enthält, das mit dem einer Kandidatenentität übereinstimmt, wird der Auflösungsbewertung ein Wert von 10 hinzugefügt. Wenn die

Geburtsdaten der beiden Entitäten unterschiedlich sind, wird von der Auflösungsbewertung ein Wert von 20 abgezogen.

Anmerkung: Die Bestätigungs- und Zurückweisungsgewichtungen für das Geburtsdatum gelten für die Auflösungsbewertung, die von einer bestimmten Auflösungsregel zugeordnet wird. Sie entsprechen nicht dem Parameter **DOBConfThreshold**, der in der Konfigurationsdatei der Pipeline konfiguriert ist.

Anzeigen von Merkmalbestätigungen und -zurückweisungen

Sie können die aktuelle Liste der Merkmaltypen überprüfen, die bei der Entitätsauflösung verwendet werden, bevor Sie neue Bestätigungen und Zurückweisungen erstellen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Auflösung** an.
3. Klicken Sie die Registerkarte **Merkmale** an.
4. Wählen Sie in der Dropdown-Liste **Auflösungskonfiguration** eine Auflösungskonfiguration aus.

Erstellen von Merkmalbestätigungen und -zurückweisungen

Sie können einen beliebigen Merkmaltyp als Kriterium für die Entitätsauflösung angeben, indem Sie ihn der Liste der Merkmalbestätigungen und -zurückweisungen hinzufügen.

Vorbereitende Schritte

Bei der Konfiguration der Auflösungseinstellungen des Merkmaltyps müssen Sie **Bestätigen/Zurückweisen** als Auflösungsverwendung des Merkmaltyps konfiguriert haben.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Auflösung** an.
3. Klicken Sie die Registerkarte **Merkmale** an.
4. Wählen Sie in der Dropdown-Liste **Auflösungskonfiguration** eine Auflösungskonfiguration aus.
5. Klicken Sie die Schaltfläche **Neu** an.
6. Geben Sie auf der Registerkarte **Allgemein** im Gruppennummernfeld die Gruppennummer ein, die auf dieses Merkmal angewendet werden soll.
7. Geben Sie in das Feld **Beschreibung** eine Beschreibung des Merkmaltyps ein, der konfiguriert wird.
8. Wählen Sie in der Dropdown-Liste **Merkmaltyp** den zu konfigurierenden Merkmaltyp aus.
9. Geben Sie in das Feld **Bestätigungsgewichtung** den Wert (im Bereich 1 - 100) ein, der der Ähnlichkeitsbewertung hinzugefügt werden soll (wenn die verglichenen Entitäten den Bestätigungsanforderungen entsprechen).
10. Geben Sie in das Feld **Zurückweisungsgewichtung** mit einem Minuszeichen (-) den negativen Wert (im Bereich 1 - 100) ein, der von der Ähnlichkeitsbewertung abgezogen werden soll (wenn die verglichenen Entitäten den Zurückweisungsanforderungen entsprechen).
11. Klicken Sie die Schaltfläche **Speichern** an.

Löschen von Merkmalbestätigungen und -zurückweisungen

Wenn ein Merkmaltyp bei der Entitätsauflösung nicht mehr als Kriterium berücksichtigt werden soll, löschen Sie ihn aus der Liste der Merkmalbestätigungen und -zurückweisungen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Auflösung** an.
3. Klicken Sie die Registerkarte **Merkmale** an.
4. Wählen Sie in der Dropdown-Liste **Auflösungskonfiguration** eine Auflösungskonfiguration aus.
5. Wählen Sie das Kontrollkästchen neben den Merkmaltypen aus, die Sie löschen wollen.
6. Klicken Sie die Schaltfläche **Löschen** an.
7. Klicken Sie **OK** im Bestätigungsfenster an, um die Auflösungskonfiguration zu löschen.

Hilfethemen

Fenster 'Bestätigungen und Zurückweisungen':

Über dieses Fenster können Sie den Bestätigungs- und Zurückweisungsprozess für die Entitätsauflösung konfigurieren. Sie können Bewertungen für Bestätigungen und Zurückweisungen angeben, die der Auflösungsbewertung hinzugefügt werden, und Sie können die Reihenfolge angeben, in der die Bestätigungen und Zurückweisungen verarbeitet werden. Wenn eine Bestätigung oder Zurückweisung erfüllt ist, wird die entsprechende Bewertung angewendet und die übrigen Bestätigungen und Zurückweisungen werden nicht verarbeitet. Für Bestätigungen wird eine positive, für Zurückweisungen eine negative Bewertung angewendet.

Reihenfolge
Die aktuelle Verarbeitungsreihenfolge.

Beschreibung
Eine Beschreibung der Bestätigung oder Zurückweisung.

Bewertung
Geben Sie einen positiven oder negativen Bewertungsmodifikator für die angegebene Bestätigung/Zurückweisung ein.

Erneut sortieren
Klicken Sie die Pfeile (Aufwärts- oder Abwärtspfeil) an, um die Bestätigung oder Zurückweisung um eine Position in die entsprechende Richtung zu verschieben. Da die Verarbeitung gestoppt wird, nachdem die erste Bestätigung oder Zurückweisung erfüllt ist, kommt der richtigen Reihenfolge eine besondere Bedeutung zu. Sie hat erheblichen Einfluss auf die Ergebnisse des Entitätsauflösungsprozesses.

Fenster 'Merkmale':

Über dieses Fenster können Sie eine Liste der Entitätsmerkmale anzeigen, die so konfiguriert sind, dass ihr Vergleich sich auf die Bewertung bei der Entitätsauflösung auswirkt. Die Auswirkung auf die Bewertung bei der Entitätsauflösung tritt nur auf, wenn der Wert für **Merkmalzurückweisungen aktiviert** auf der Registerkarte **Auflösungsregeln - Allgemein** auf **Ja** gesetzt ist.

Beschreibung
Der Name des Merkmals, das verglichen wird.

Merkmaltyp
Der Systemname des Merkmaltyps, der verglichen wird.

Bestätigungsgewichtung
Der Wert, der dem Bewertungsprozess für die Entitätsauflösung hinzugefügt wird, wenn die verglichenen Merkmalwerte identisch sind.

Zurückweisungsgewichtung
Der Wert, der dem Bewertungsprozess für die Entitätsauflösung hinzugefügt wird, wenn die verglichenen Merkmalwerte verschieden sind.

Auflösung - Merkmale - Registerkarte 'Allgemein':

Über diese Registerkarte können Sie eine neue Merkmalbestätigung/-zurückweisung konfigurieren oder die Details einer vorhandenen Merkmalbestätigung/-zurückweisung anzeigen.

Gruppe
Geben Sie eine Nummer ein, die die Reihenfolge angibt, in der die Merkmalbestätigung/-zurückweisung verarbeitet wird.

Beschreibung
Geben Sie die Beschreibung für die Bestätigung/Zurückweisung ein.

Merkmaltyp
Wählen Sie den Merkmaltyp für die Bestätigung/Zurückweisung aus.

Bestätigungsgewichtung
Geben Sie die Bewertung ein, die der Entitätsauflösungsbewertung hinzugefügt wird, wenn die verglichenen Merkmalwerte gleich sind.

Zurückweisungsgewichtung
Geben Sie die negative Bewertung ein, die der Entitätsauflösungsbewertung hinzugefügt wird, wenn die verglichenen Merkmalwerte verschieden sind.

Konfigurieren von Systemparametern

Sie können bestimmte Funktionen des Identity Insight-Systems konfigurieren.

Konfigurieren von Systemparametern für die Namensbewertung

Sie können den Namensbewertungsalgorithmus konfigurieren, der beim Generieren einer Kandidatenliste während des Entitätsauflösungsprozesses verwendet wird.

Vorgehensweise

1. Wählen Sie in der Konfigurationskonsole **Konfiguration** > **Allgemein** > **Systemparameter** aus.
2. Wählen Sie in der Liste **Parametergruppe** die Parametergruppe **NAME_MATCHING** aus.
3. Wählen Sie den Systemparameter **ALGORITHM** aus.
4. Geben Sie im Feld **Aktueller Wert** den ganzzahligen Wert des zu verwendenden Name Comparator-Algorithmus an. Wenn Sie den Wert dieses Systempara-

meters auf seinen Standardwert zurücksetzen wollen, geben Sie in das Feld **Aktueller Wert** den Wert ein, der im Feld **Standardwert** angezeigt wird.

Anmerkung: Name Comparator 2 ist der Standardnamenbewertungsalgorithmus für die Produktversion 3.9.1 und höher.

5. Klicken Sie **Speichern** an.

Konfigurieren von Systemparametern für Name Manager

Die Systemparameter für die Name Manager-Namensbewertung werden standardmäßig beim Installieren des Produkts konfiguriert. Sie können die Standardsystemparameter jedoch bei Bedarf aktualisieren. Es kann beispielsweise sein, dass Sie die Position der Name Manager-Unterstützungsbibliotheken ändern müssen.

Informationen zu diesem Vorgang

Sie legen den Pfad der Name Manager-Unterstützungsbibliotheken fest und aktivieren über die Name Manager-Systemparameter die Kategorisierung von Namen nach Typ. Sie legen außerdem den Systemparameter **CROSSCHECKCULTURE** fest, um die Namensverarbeitung zwischen verschiedenen Namenskulturen zu konfigurieren.

Vorgehensweise

1. Wählen Sie in der Konfigurationskonsole **Konfiguration** > **Allgemein** > **Systemparameter** aus.
2. Wählen Sie die Parametergruppe **NAMEMANAGER** in der Liste **Parametergruppe** aus.
3. Wählen Sie im linken Teilfenster den zu konfigurierenden Systemparameter von Name Manager aus:

Name Manager-Systemparameter	Beschreibung
SUPPORTPATH	Gibt die Position der Name Manager-Unterstützungsdateien an. Der Standardwert lautet ./data und gibt den relativen Pfad zum übergeordneten Produktverzeichnis an. Ändern Sie diesen Wert in den absoluten Pfad der neuen Position, wenn die Unterstützungsdateien während der Installation an eine andere Position verschoben werden.
NAMESIFTER	Gibt an, ob die Funktion für die Namenskategorisierung nach Namenstyp (persönliche Namen oder Unternehmensnamen) aktiviert ist. Geben Sie den Wert 1 (neuer Standardwert für die Installation) in **Aktueller Wert** ein, um die Kategorisierung von Namen nach Typ (Name Sifter-Funktion) zu aktivieren. Geben Sie den Wert 0 (Standardwert für das Upgrade) in **Aktueller Wert** ein, um die Kategorisierung von Namen nach Typ (Name Sifter-Funktion) zu inaktivieren.

Name Manager-Systemparameter	Beschreibung
CROSSCHECKCULTURE	Gibt an, ob eine Name Manager-Namensbewertung zwischen Namenskulturen ausgeführt werden soll, wenn sich die Namenskulturen voneinander unterscheiden. Wenn Sie nur den eingehenden Namenskulturwert vor dem Bewerten beider Namen prüfen wollen, geben Sie `0` in **Aktueller Wert** ein. Wenn Sie die Namenskulturwerte vor dem Bewerten prüfen wollen (neuer Standardwert für die Installation), geben Sie den Wert 1 in **Aktueller Wert** ein.

Achtung: Der Systemparameter **CROSSCHECKCULTURE** hat Einfluss darauf, wie die Entitätsauflösung die Namensbewertung nach Kultur in den Pipelines ausführt. Wenden Sie sich an den IBM Kundendienst oder den IBM Support, bevor Sie den aktuellen Wert dieses Systemparameters ändern.

4. Klicken Sie **Speichern** an.

Konfigurieren von Systemparametern für die Datenbank

Sie können die maximale Größe der Klausel IN für alle Kandidatenlisten konfigurieren, die während der Entitätsauflösung von der Pipeline erstellt werden.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Systemparameter** an.
4. Wählen Sie in der Dropdown-Liste **Parametergruppe** die Parametergruppe **DB_CONFIG** aus.
5. Klicken Sie den Systemparameter **MAX_IN_CLAUSE** an.
6. Geben Sie in das Feld **Aktueller Wert** die maximale Anzahl Zeichen ein, die eine Klausel IN umfassen soll, wenn während des Entitätsauflösungsprozesses eine Kandidatenliste generiert wird. Gültige Werte sind ganze Zahlen von 0 bis 1000. Wenn Sie den Wert dieses Systemparameters auf seinen Standardwert zurücksetzen wollen, geben Sie in dieses Feld den Wert ein, der im Feld **Standardwert** angezeigt wird.

   Anmerkung: Dieser Wert beeinflusst die Leistung Ihrer Datenbank. Berücksichtigen Sie die Größe Ihrer Datenbank und die Leistungsmerkmale Ihrer Systemhardware, wenn Sie den Wert für diesen Parameter angeben.
7. Klicken Sie **Speichern** an.

Konfigurieren von Systemparametern für die Protokolle

Sie können die Protokollstufe konfigurieren, die Sie für bestimmte Entitätsauflösungstabellen in der Datenbank verwenden wollen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.

3. Klicken Sie die Registerkarte **Systemparameter** an.
4. Wählen Sie im Dropdown-Menü **Parametergruppe** den Systemparameter **LOG_LEVEL** aus.
5. Klicken Sie den Namen des Parameters an, den Sie konfigurieren wollen.
6. Geben Sie in das Feld **Aktueller Wert** die Protokollebene ein, die Sie auf diesen Parametercode anwenden wollen. Gültige Werte sind mit Beschreibung im Feld **Parameterbeschreibung** aufgelistet. Wenn Sie den Wert dieses Systemparameters auf seinen Standardwert zurücksetzen wollen, geben Sie in dieses Feld den Wert ein, der im Feld **Standardwert** angezeigt wird.

   Anmerkung: Dieser Wert beeinflusst die Leistung Ihrer Datenbank und Komponenten wie beispielsweise Visualizer. Berücksichtigen Sie die Größe Ihrer Datenbank und die Leistungsmerkmale Ihrer Systemhardware, wenn Sie den Wert für diesen Parameter angeben. Wenn LOG_LEVEL beispielsweise für bestimmte Tabellen in einen Wert unter 4 geändert wird, stoppt Visualizer den Betrieb. Beispiele für diese Tabellen sind:
   - ER_DETAIL
   - ER_ENTITY_SCORE
   - ER_ENTITY_STATE
   - ER_RELOCATION
7. Klicken Sie **Speichern** an.

Konfigurieren von Systemparametern für Bestätigung und Zurückweisung

Sie können angeben, dass jeder konfigurierte Bestätigungs- und Zurückweisungsvergleich ausgeführt werden soll. Sie können aber auch angeben, dass diese Vergleiche in der konfigurierten Reihenfolge ausgeführt werden sollen, bis eine Bestätigung oder Zurückweisung erfüllt ist. Durch die Verwendung der zweiten Option kann die Verarbeitungszeit verkürzt werden.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Systemparameter** an.
4. Wählen Sie die Parametergruppe **MM** im Dropdown-Menü **Parametergruppe** aus.
5. Klicken Sie den Systemparameter **MULTICONFIRMATION** an.
6. Geben Sie in das Feld **Aktueller Wert** den Wert 1 ein, damit alle Bestätigungen und Zurückweisungen verarbeitet werden. Für alle Bestätigungen und Zurückweisungen, deren Bedingung erfüllt ist, wird die Summe der Bewertungsänderungen auf die Auflösungsregel angewendet, die gerade verarbeitet wird. Sie können auch den Wert 0 eingeben, damit die Bestätigungen und Zurückweisungen in der angegebenen Reihenfolge verarbeitet werden, bis die Bedingung einer Bestätigung oder Zurückweisung erfüllt ist. Die Verarbeitung wird gestoppt und die Bewertungsänderung wird auf die Auflösungsregel angewendet, die gerade verarbeitet wird. Wenn Sie den Wert dieses Systemparameters auf seinen Standardwert zurücksetzen wollen, geben Sie in dieses Feld den Wert ein, der im Feld **Standardwert** angezeigt wird.
7. Klicken Sie **Speichern** an.

Konfigurieren von Systemparametern für Rollenalerts

Sie können konfigurieren, ob jeder Rollenalert oder nur der stärkste Rollenalert berichtet werden soll, der von einer Entitätsauflösungsregel für eine eingehende Entität generiert wird.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Systemparameter** an.
4. Wählen Sie die Parametergruppe **MM** im Dropdown-Menü **Parametergruppe** aus.
5. Klicken Sie den Systemparameter **REPORT_SAME_CONFLICTS** an.
6. Geben Sie in das Feld **Aktueller Wert** den Wert `1` ein, damit alle Rollenalerts berichtet werden, die von einer Auflösungsregel für eine eingehende Entität generiert werden. Sie können auch den Wert `0` eingeben, damit nur der stärkste Rollenalert berichtet wird, der von jeder Auflösungsregel für eine eingehende Entität generiert wird. Wenn Sie den Wert dieses Systemparameters auf seinen Standardwert zurücksetzen wollen, geben Sie in dieses Feld den Wert ein, der im Feld **Standardwert** angezeigt wird.
7. Klicken Sie **Speichern** an.

Konfigurieren von Systemparametern für Attributalertgeneratoren

Sie können die Standardanzahl der Tage konfigurieren, während der ein neuer Attributalertgenerator aktiv ist, bevor er abläuft.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Systemparameter** an.
4. Wählen Sie **PERSISTENT_SEARCH** in der Dropdown-Liste **Parametergruppe** aus.
5. Klicken Sie den Systemparameter **SEARCH_EXPIRATION_TIME** an.
6. Geben Sie in das Feld **Aktueller Wert** die Standardanzahl der Tage ein, während der ein neuer Attributalertgenerator aktiv sein soll, bevor er abläuf. Visualizer-Benutzer können zwar ein anderes Ablaufdatum angeben; dieser Wert gibt jedoch die Standardanzahl der Tage an, während der ein neuer Attributalertgenerator aktiv ist.
7. Klicken Sie **Speichern** an.

Konfigurieren der Systemparameter für den gemeinsamen Zugriff

Wenn Ihre Pipelines für die parallele Pipelineverarbeitung konfiguriert sind, können Sie die Standardanzahl der parallelen Pipeline-Threads festlegen, die beim Starten der Pipeline gestartet werden.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie das Kontrollkästchen **Konfiguration bearbeiten** ausgewählt haben, wenn Sie sich an der Konfigurationskonsole angemeldet haben. Diese

Auswahl ermöglicht es Ihnen, eine Systemkonfiguration hinzuzufügen, zu ändern und zu löschen, einschließlich der Systemparameter.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Systemparameter** an.
4. Wählen Sie die Parametergruppe **CONCURRENCY** im Dropdown-Menü **Parametergruppe** aus.
5. Wählen Sie den Systemparameter **DEFAULT_CONCURRENCY** aus.
6. Geben Sie in das Feld **Aktueller Wert** die Zahl ein, die die Standardanzahl der Pipeline-Verarbeitungs-Threads darstellt, die bei jedem Starten einer Pipeline gestartet werden sollen.

Konfigurieren von Systemparametern für das Datenqualitätsmanagement

Sie können den Standarddatumsbegrenzer konfigurieren, den die Konfigurationskonsole bei der Formatierung von Datumsangaben verwendet.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Systemparameter** an.
4. Wählen Sie im Dropdown-Menü **Parametergruppe** die Parametergruppe **DQM** aus.
5. Klicken Sie den Systemparameter **SYSTEM_DATE_DELIMITER** an.
6. Geben Sie in das Feld **Aktueller Wert** das Zeichen **/** oder **-** ein, um anzugeben, welchen Begrenzer das System zum Formatieren von Datumsangaben verwenden soll. Wenn Sie den Wert dieses Systemparameters auf seinen Standardwert zurücksetzen wollen, geben Sie in dieses Feld den Wert ein, der im Feld **Standardwert** angezeigt wird.
7. Klicken Sie **Speichern** an.

Konfigurieren von Systemparametern für Produktoptionen

Sie können konfigurieren, welche weiteren Produktoptionen Sie aktivieren wollen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Systemparameter** an.
4. Wählen Sie im Dropdown-Menü **Parametergruppe** die Parametergruppe **CONSOLE_CONFIG** aus.
5. Klicken Sie den Systemparameter **PRODUCT_OPTIONS** an.
6. Geben Sie in das Feld **Aktueller Wert** den von IBM bereitgestellten Code für die Produktfunktion ein, die Sie aktivieren wollen. Sie dürfen nur Großbuchstaben verwenden. Sie können eine durch Leerzeichen getrennte Liste aller Funktionen eingeben, die das System aktivieren soll. Wenn Sie den Wert dieses Systemparameters auf seinen Standardwert zurücksetzen wollen, geben Sie in dieses Feld den Wert ein, der im Feld **Standardwert** angezeigt wird.
7. Klicken Sie **Speichern** an.

Konfigurieren von Systemparametern für den Ereignismanager

Sie können die Ereignisverarbeitung des Ereignismanagers aktivieren und Systemparameter für die Ereignisverarbeitung konfigurieren, einschließlich des URI (Universal Resource Indicator) des Ereignisprozessors.

Vorgehensweise

1. Klicken Sie in der Konfigurationskonsole die Registerkarte **Systemkonfiguration** an.
2. Wählen Sie im linken Teilfenster den zu konfigurierenden Systemparameter des Ereignismanagers aus:
   a. **Ereignisverarbeitung aktivieren** gibt an, ob die Ereignisverarbeitung durch den Ereignismanager aktiviert oder inaktiviert ist.
   b. **Zeitlimit für Ereignisprozessor** gibt die Anzahl der Sekunden an, die die Pipeline auf eine Antwort vom externen Ereignisprozessor wartet, bevor ein Zeitlimit überschritten und ein Fehler übergeben wird. Der Standardwert ist 60 Sekunden.
   c. **Ereignisprozessor-URI** gibt den URI (Universal Resource Indicator) für die Verbindung zum externen Ereignisprozessor an. Geben Sie in **Aktueller Wert** den URI ein, einschließlich der Portnummer, auch wenn es sich um die Standardportnummer handelt. Beispiel: `http://localhost:13510/gem`
   d. **Ereignisprotokollfenster** gibt die Anzahl der Tage im Ereignisverlauf an, die die Pipeline bei der Auswertung eines neuen eingehenden Ereignisses an den externen Ereignisprozessor sendet. (Der Standardwert für die Anzahl der Tage ist 180.)
3. Klicken Sie die Schaltfläche **Speichern** an.

Konfigurieren von Systemparametern für Visualizer

Über den Systemparameter für Visualizer können Sie festlegen, dass einzelnen Visualizer-Benutzern alle Alerts angezeigt werden, einschließlich derjenigen, die unter dem **Mindestgrenzwert für Alerts** liegen, der in jeder Rollenalertregel definiert ist. Sie können diese Einstellung ändern, um Visualizer-Benutzern mehr Flexibilität bei der Anzeige von Alerts zu geben.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Systemparameter** an.
4. Wählen Sie in der Dropdown-Liste **Parametergruppe** die Parametergruppe **VISUALIZER** aus.
5. Klicken Sie den Systemparameter **ALLOW_ALERT_THRESHOLD_OVERRIDE** an.
6. Wählen Sie eine der folgenden Optionen:
   - Geben Sie `1` im Feld **Aktueller Wert** ein, um den definierten Grenzwert für Alerts auf der Registerkarte **Rollenalertregel - Filter** in der Konfigurationskonsole zu überschreiben.
   - Geben Sie `0` ein, wenn Visualizer-Benutzer nicht die Möglichkeit haben sollen, den vom System definierten Grenzwert für Alerts auf der Registerkarte **Rollenalertregel - Filter** in der Konfigurationskonsole außer Kraft zu setzen.

- Wenn Sie den Wert dieses Systemparameters auf seinen Standardwert zurücksetzen wollen, geben Sie in das Feld **Aktueller Wert** den Wert ein, der im Feld **Standardwert** angezeigt wird.

7. Klicken Sie die Schaltfläche **Speichern** an.

Festlegen des Standardpfads für Centrifuge

Wenn Sie den optionalen Centrifuge Desktop aus Centrifuge Systems zum Darstellen und Anzeigen von Entitätsdiagrammen verwenden, müssen Sie den Dateipfad für Centrifuge Desktop in den Visualizer-Vorgaben angeben.

Informationen zu diesem Vorgang

Für jeden Visualizer-Client werden Standardpfadeinstellungen konfiguriert. Der über diese Task angegebene Standardpfad gilt nur für die Visualizer-Instanz, an der Sie zurzeit angemeldet sind.

Vorgehensweise

1. Klicken Sie in Visualizer **Datei** > **Benutzervorgaben** > **Benutzervorgaben für das System** an.
2. Führen Sie unter dem Abschnitt **Dateipfade** in **Centrifuge-Pfad** einen der folgenden Schritte aus:
   - Geben Sie den Dateipfad oder die URL (Uniform Resource Locator) für die Centrifuge Desktop-Anwendung in das Feld ein.
   - Navigieren Sie zur Centrifuge Desktop-Anwendung und öffnen Sie sie.
3. Klicken Sie **Übergeben** an. Sie werden mit einer Bestätigungsnachricht informiert, dass Sie Visualizer erneut starten müssen, damit Ihre Änderungen wirksam werden.
4. Klicken Sie in der Bestätigungsnachricht **OK** an.
5. Schließen Sie Visualizer, öffnen Sie ihn wieder und melden Sie sich erneut an.

Ergebnisse

Nachdem der Pfad konfiguriert ist, wird die Schaltfläche **Centrifuge** in den Anzeigen **Rollenalert-Detail** und **Entitätszusammenfassung** im Prüffenster angezeigt. Klicken Sie die Schaltfläche an, um Ihre Centrifuge Desktop-Anwendung direkt in Visualizer zu starten.

Festlegen des Standardpfads für UMF-Dateien

Wenn Sie regelmäßig Identitätsdatensätze in UMF-Datendateien zur Verarbeitung durch den Visualizer laden, sparen Sie sich durch das Festlegen des Standardpfads einen Arbeitsschritt.

Informationen zu diesem Vorgang

Für jeden Visualizer-Client werden Standardpfadeinstellungen konfiguriert. Der über diese Task angegebene Standardpfad gilt nur für die Visualizer-Instanz, an der Sie zurzeit angemeldet sind.

Vorgehensweise

1. Wählen Sie in Visualizer **Datei** > **Benutzervorgaben** > **Benutzervorgaben für das System** aus.

2. Führen Sie im Bereich **Standardpfad für Laden von Datei** einen der folgenden Schritte aus:
   - Geben Sie den vollständigen Pfad des zu verwendenden Verzeichnisses ein.
   - Navigieren Sie zum Verzeichnis, um es auszuwählen.
3. Klicken Sie **Übergeben** an. Sie werden mit einer Bestätigungsnachricht informiert, dass Sie Visualizer erneut starten müssen, damit Ihre Änderungen wirksam werden.
4. Klicken Sie in der Bestätigungsnachricht **OK** an.
5. Schließen Sie Visualizer, starten Sie ihn wieder und melden Sie sich erneut an.

Ergebnisse

Bei jedem Laden einer UMF-Datei ist der Standardpfad das Verzeichnis, das Sie angegeben haben.

Attribut- und Scoring-Anpassung

IBM InfoSphere Identity Insight bietet funktionelle Erweiterungen zum Konfigurieren von Attributdaten und Integrieren von Scoring-Algorithmen. Durch diese Änderungen werden Größe und Typen der Identitätsdaten erweitert, die verglichen und bewertet werden können. Außerdem werden hierdurch zusätzliche neue Scoring-Algorithmen für den Entitätsauflösungsprozess ermöglicht. Diese Funktionalität wird allgemein als Attribut- und Scoring-Anpassung bezeichnet.

Die Technologie der Entitätsauflösung ermöglicht Ihnen die Verwendung von Abgleichs- und Scoring-Algorithmen zum Vergleichen und Auflösen gängiger Identitätsdaten wie Namen, Adressen, Telefonnummern, Kreditkartennummern, Steueridentifikationsnummern und Lizenznummern, sowie die die nach der BeschreibungBuchungen. Die Datenelemente, die ein Benutzerkonto oder eine Entität beschreiben, werden hier als 'Attribute' bezeichnet. Attribute können Merkmale oder Eigenschaften einschließen, die eine Person, ein Unternehmen, einen Bereich oder ein Element beschreiben. Mit der Erweiterung der Attribut- und Scoring-Anpassung können Sie neue Typen von Identifikationsdaten und zugehörige Scoring-Algorithmen hinzufügen, die als Scoring-Plug-ins für das Produkt entwickelt wurden. So können Sie z. B. von Fingerabdrücken, Netzhautscans oder DNA-Tests abgeleitete Identitätsdaten hinzufügen und diese mit einem Scoring-Plug-in bewerten, das einen geeigneten Vergleichsalgorithmus enthält.

Diese Attribut- und Scoring-Erweiterungen verbessern den Prozess der Entitätsauflösung durch folgende Möglichkeiten:

- Große Attributdaten mit ATTR_VALUE (erweitert auf 8 KB) und ATTR_LARGE_DATA (für noch größere Daten) speichern und vergleichen.
- Bereitgestellte Scoring-Algorithmen auf ein breiteres Spektrum von Attributtypen anwenden und diese Attribute einfacher und mit mehr Steuerungsmöglichkeiten konfigurieren.
- Die Ergebnisse aus dem angepassten Attributvergleich und Scoring mithilfe der Berichts- und Alertfunktionen von Visualizer integrieren.
- Ein Plug-in-Modell zum Hinzufügen von Scoring-Algorithmen anwenden, die von Benutzern erstellt wurden.
- Angepasste Scoring-Plug-ins mithilfe der Konfigurationskonsole integrieren.

Speichern großer Attributdaten

Damit das System größere Attributdaten mit Scoring-Plug-ins speichern und verarbeiten kann, müssen Metadaten in UMF (Universal Message Format) konvertiert und in den entsprechenden Spalten gespeichert werden.

Informationen zu diesem Vorgang

Vorgehensweise

1. Analysieren Sie Ihre eingehenden Daten mit dem Entitätsmodell, das Sie für das System erstellt haben, um zu überprüfen, inwieweit sie dem UMF-Standard entsprechen. Sie sollten eine konkrete Vorstellung der vorhandenen UMF-Segmente und -Tags haben, bevor Sie mit dem nächsten Schritt fortfahren.
2. Konfigurieren Sie Ihr ETL-Tool so, dass es UMF-Datensätze erstellt, die mit Ihrem Entitätsmodell übereinstimmen.
3. Führen Sie das ETL-Tool aus.

Nächste Schritte

Nach der Konvertierung Ihrer Daten in UMF können Sie die UMF-Datensätze zur Verarbeitung an die Pipeline senden.

Speicherparameter für große Attributdaten

Damit das System große Attributdaten für das Scoring speichern und verarbeiten kann, müssen Metadaten in UMF (Universal Message Format) konvertiert und in den entsprechenden Spalten gespeichert werden.

Verwenden Sie die Spalten ATTR_VALUE und ATTR_LARGE_DATA zum Speichern großer oder unstrukturierter Attributdaten für angepasste Attribut- und Scoring-Anwendungen.

Spalte und UMF-Tagname	Datentyp und Größe	Erforderlich	Erläuterung
ATTR_VALUE	varchar(255) (Standardwert) auf maximal 8 KB erweiterbar	**Ja**	Daten, die als eines der Attribute in einem ETL-Prozess mit den Basis-Plug-ins für das Scoring verwendet werden. Wenn die Daten größer als 8 KB sind und im Binärformat vorliegen, speichern Sie sie in der Spalte ATTR_LARGE_DATA und erstellen Sie eine eindeutige Kennung für diese Daten in der Spalte ATTR_VALUE. Diese ATTR_VALUE-Kennung wird dann für Vergleich und Scoring verwendet. Erstellen Sie z. B. einen einseitig gerichteten MD5-Hash-Code (MD5 - Message-Digest Algorithmus 5), der im Visualizer und in den Berichten verglichen und angezeigt werden kann. Die maximale Spaltengröße ist von der Datenbank abhängig. Damit Binärdaten, die größer als 255/3 sind, in ATTR_VALUE gespeichert werden können, muss die Spaltengröße geändert werden. Aus Leistungsgründen sollten Sie eine erneute Optimierung des Datenbankcache erwägen, da wahrscheinlich weitaus weniger Zeilen in den Cache passen.

ATTR_LARGE_DATA	Großes Zeichenobjekt (CLOB) zur Verwendung von Daten über 8 KB.	**Nein**	Als Zeichendaten speichern. Verwenden Sie z. B. Base64-Codierung von Binärdaten. Verwenden Sie diese Spalte zum Speichern von Attributdaten, die für die Spalte ATTR_VALUE zu groß sind. ATTR_LARGE_DATA ist eine Spalte des Typs CLOB (großes Zeichenobjekt), die Daten ohne Größenbeschränkung aufnehmen kann. Diese Daten stehen für die Entitätsauflösung zur Verfügung. Die Struktur der Daten muss dem Verfasser des angepassten Vergleichs-Plug-ins bekannt sein. Visualizer zeigt diese Daten nicht an, da das Format kein Standardformat ist und bei unterschiedlichen Systemtypen variiert. Die Leistung eines CLOB fällt gegenüber der einer varchar-Spalte ab, da ein CLOB nicht in den Cache gestellt werden kann und von Platte gelesen werden muss. Daher ist ATTR_VALUE vorzuziehen. Wird die Spalte ATTR_VALUE vergrößert, bedeutet dies, dass weniger Attributdaten im Cache abgelegt werden. Daher kann es unter Umständen besser sein, für Daten unter 8 KB einfach die Spalte ATTR_LARGE_DATA zu verwenden, um sicherzustellen, dass andere nicht so große Attribute wie Geschlecht und Geburtsdatum in den Cache gestellt werden. Diese Entscheidung liegt beim Architekten. Wenden Sie sich im Zweifelsfall an Ihren Systemadministrator. Wird die Spalte ATTR_LARGE_DATA verwendet, muss ATTR_VALUE mit einem Wert gefüllt werden. Wenn aus den Daten ein aussagekräftiges Suchkriterium erstellt werden kann, das in die Spalte ATTR_VALUE gestellt werden kann, sollte dies getan werden. Wenn kein aussagekräftiges Suchkriterium erstellt werden kann, muss ein anderer eindeutiger Wert in die Spalte ATTR_VALUE gestellt werden, andernfalls kann die Pipeline nicht ordnungsgemäß ausgeführt werden und schlägt wahrscheinlich aufgrund von DQM-Fehlern fehl. Durch Konfigurieren einer DQM-Regel kann ein eindeutiger Schlüssel automatisch generiert werden, um einen MD5-Hash der Daten (Regel 600) oder einen angepassten Hash basierend auf konfigurierten Regeln (Regel 615) zu erstellen. Es ist wichtig, dass dieser Wert eindeutig ist, insbesondere, wenn der Attributtyp für die persistente Suche konfiguriert wird, da die Spalte ATTR_VALUE zur Festsetzung generischer Werte verwendet wird. **Anmerkung:** Das zum Lieferumfang gehörende Plug-in 'binaryAttributeScoring' nimmt keinerlei Vergleich von ATTR_VALUE vor. Es prüft lediglich das Segment ATTR_LARGE_DATA und bewertet es.

Beispiel

Hier ein Beispiel einer MD5-Hashwertausgabe großer Binärdaten:

```
<ATTRIBUTE><ATTR_TYPE>BIOMETRIC-1</ATTR_TYPE>
<ATTR_VALUE>214b21fc3e040f844a07710b1bb451a0
</ATTR_VALUE><ATTR_LARGE_DATA>
<![H4sICBRTqkgAA2Zvby50eHQAK0ktLuHlAgDkTqoPBgAAAA==]>
</ATTR_LARGE_DATA></ATTRIBUTE>
```

Tatsächliche ATTR_LARGE_DATA-Werte sind in der Regel weitaus größer als in diesem Beispiel gezeigt.

Konfigurieren von Quellenmerkmalen für große Attributdaten

Verwenden Sie die Konfigurationskonsole zum Konfigurieren von Quellenmerkmalen für große Attributdaten.

Informationen zu diesem Vorgang

In der Konfigurationskonsole können Sie neue Typen von Attributdaten für angepasste Scoring-Plug-ins auf dieselbe Weise konfigurieren, wie Sie auch Daten für Basis-Plug-ins konfigurieren.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Plug-ins** in der Konfigurationskonsole das Auswahlfeld für das angepasste Plug-in an.
2. Klicken Sie die Registerkarte **Merkmale** an.
3. Klicken Sie die Registerkarte **Allgemein** an und füllen Sie die Felder entsprechend aus.
4. Wählen Sie den zutreffenden Datentyp aus. Folgende Datentypen stehen zur Auswahl: CHAR, DATE oder CLOB. Beachten Sie dabei die Voraussetzungen für den Datentyp in „Speicherparameter für große Attributdaten" auf Seite 195.
5. Wählen Sie eine zutreffende Klasse aus.
6. Wählen Sie einen Wert für die Auflösungsverwendung aus.
7. Wählen Sie den Namen des Scoring-Plug-ins aus, das Sie konfigurieren.
8. Wählen Sie einen geeigneten Wert im Feld für die Anzeigeebene aus. Wählen Sie **Nur ohne Wert eingeben** aus, um zu verhindern, dass Visualizer den Inhalt der Spalte ATTRIBUTE.ATTR_VALUE oder ATTRIBUTE.ATTR_LARGE_DATA anzeigt. Die Spalte ATTR_VALUE wird normalerweise nicht verwendet, wenn die Spalte für große Objekte (CLOB) verwendet wird. Darüber hinaus würde die Spalte ATTR_LARGE_DATA (CLOB) in der Regel mit Base-64 verschlüsselte Daten enthalten, deren Anzeige in Visualizer nicht relevant oder hilfreich wäre.
9. Klicken Sie **Speichern** an.

Ergebnisse

Die Registerkarte **Merkmale** unter **Quellen** zeigt den neuen Typ und zugehörige Informationen.

Konfigurieren von Auflösungsmerkmalen für große Daten

Verwenden Sie die Konfigurationskonsole zum Konfigurieren von Auflösungsmerkmalen für große Attributdaten und angepasste Scoring-Plug-ins.

Informationen zu diesem Vorgang

Bestätigungs- und Zurückweisungsinformationen für einen neuen Merkmaltyp werden zuletzt konfiguriert.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** in der Konfigurationskonsole an.
2. Klicken Sie die Schaltfläche **Auflösung** an.
3. Klicken Sie die Registerkarte **Merkmale** an.
4. Wählen Sie eine geeignete Auflösungskonfiguration im Dropdown-Menü aus, z. B. DEFAULT, und klicken Sie dann die Schaltfläche **Neu** an.
5. Wählen Sie die Registerkarte **Allgemein** aus und geben Sie Werte in die angezeigten Felder ein. Beschreibungen der Feldoptionen und Empfehlungen finden Sie in „Auflösungsmerkmale und -optionen".
6. Klicken Sie **Speichern** an.

Ergebnisse

Die Übersichtsanzeige zeigt eine Übersichtstabelle mit den von Ihnen für die Auflösungskonfiguration erstellten Werten an.

Auflösungsmerkmale und -optionen

Verwenden Sie die Registerkarte **Allgemein** für die Auflösungsmerkmale zum Konfigurieren von Aktionen und Optionen für große Datentypen und angepasste Scoring-Plug-ins.

Wenn Sie einen Zeichentyp konfigurieren, der ein Feld für die Auflösungsverwendung aufweist, und dabei einen Wert für "Bestätigung/Zurückweisung" auswählen, werden zusätzliche Felder dynamisch angezeigt.

Feld	Erforderlich	Feldauswahl und Beschreibung
Gruppe	**Ja**	Geben Sie die Nummer der Gruppe ein, die Sie zum Kennzeichnen dieses Merkmals verwenden wollen.
Beschreibung	**Ja**	Geben Sie eine Kurzbeschreibung für diese Standardauflösungskonfiguration ein. Wenn Sie das Feld leer lassen, kann dies einen Fehler verursachen.
Merkmaltyp	**Ja**	Wählen Sie den Typ aus, den Sie bearbeiten. Die Liste enthält alle Typen, die Sie für Quellen konfiguriert haben.
Bestätigungsgewichtung	**Ja**	Ein beliebiger Wert von 0-100. Wirkt sich auf die Ähnlichkeitsbewertung aus.
Schwellenwert für Bestätigung des Plug-ins	**Nein**	Textfeld mit freiem Format. Dieses Feld wird bei Angabe eines Merkmaltyps angezeigt, dessen Auflösungsverwendung auf "Bestätigen/Zurückweisen" gesetzt ist, zum Beispiel wenn der Typ für ein angepasstes Plug-in gilt. Geben Sie hier einen Schwellenwert für die Bestätigung an, wenn der Merkmaltyp von einem Scoring-Plug-in während der Bestätigung bzw. Zurückweisung innerhalb des Prozesses der Entitätsauflösung bewertet wird. Wenn die vom Plug-in zugeordnete Bewertung diesem Wert entspricht oder ihn überschreitet, wird der Abgleich als Bestätigung angesehen. Dies hat zur Folge, dass der Wert des Felds **Bestätigungsgewichtung** der Bewertung der Übereinstimmungswahrscheinlichkeit hinzugefügt wird.

Zurückweisungsgewichtung	**Ja**	Ein beliebiger Wert von 0-100. Wirkt sich auf die Ähnlichkeitsbewertung aus.
Schwellenwert für Zurückweisung des Plug-ins	**Nein**	Textfeld mit freiem Format. Dieses Feld wird nur bei Angabe eines Merkmaltyps angezeigt, dessen Auflösungsverwendung auf "Bestätigen/Zurückweisen" gesetzt ist, zum Beispiel wenn der Typ für ein angepasstes Plug-in gilt. Wenn der Merkmaltyp von einem Scoring-Plug-in während der Bestätigung bzw. Zurückweisung innerhalb des Prozesses der Entitätsauflösung bewertet wird, dann geben Sie hier einen Schwellenwert für die Zurückweisung an (der vom Plug-in interpretiert wird). Wenn die vom Plug-in zugeordnete Bewertung diesem Wert entspricht oder ihn unterschreitet, wird der Abgleich als Zurückweisung angesehen. Dies hat zur Folge, dass der Wert des Felds **Zurückweisungsgewichtung** der Bewertung der Übereinstimmungswahrscheinlichkeit hinzugefügt wird.

Konfigurationsberichte für Attribut- und Scoring-Anpassung

Der Konfigurationsbericht in der Konfigurationskonsole enthält auch Elemente für die Attribut- und Scoring-Anpassung.

Zusätze zum Konfigurationsbericht sind:

- Eine neue Spalte "Scoring-Plug-in" im Berichtsabschnitt zu den Merkmaltypen, in der der Wert des entsprechenden Merkmaltyps für das Plug-in angezeigt werden.
- Ein neuer Plug-in-Berichtsabschnitt, in dem die konfigurierten Datensätze angezeigt werden. Zu den Spaltenüberschriften gehören: ID, Name, Typ, Version und Kurzname für Bibliothek.
- Zwei neue Spalten im Abschnitt "Entitätsauflösungsmerkmale" in denen die Werte für "Schwellenwert für Bestätigung des Plug-ins" und "Schwellenwert für Zurückweisung des Plug-ins" angezeigt werden.

Konfigurieren angepasster Scoring-Plug-ins

Verwenden Sie die Konfigurationskonsole zum Konfigurieren angepasster Scoring-Plug-ins.

Vorbereitende Schritte

Stellen Sie sicher, dass das neue Plug-in ordnungsgemäß für IBM InfoSphere Identity Insight adaptiert worden ist. Siehe Entwickeln angepasster Scoring-Plug-ins für IBM InfoSphere Identity Insight.

Informationen zu diesem Vorgang

In der Konfigurationskonsole können Sie Scoring-Plug-ins konfigurieren, die dem System hinzugefügt worden sind.

Vorgehensweise

1. Klicken Sie in der Konfigurationskonsole die Schaltfläche **Konfiguration** an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Plug-ins** an.
4. Klicken Sie zum Konfigurieren eines neuen Plug-ins die Schaltfläche **Neu** an.

5. Wählen Sie zum Bearbeiten eines vorhandenen Plug-ins das Plug-in, das Sie konfigurieren wollen, in der Liste in der Spalte der Plug-ins aus. Nur die kundenspezifischen Plug-ins sind bearbeitbar.
6. Füllen Sie auf der Registerkarte **Allgemein** die Felder entsprechend aus:

Feldname	Erforderlich	Beschreibung
Plug-in	**Ja**	Name des Plug-ins, der in den Menüoptionen von "Scoring-Plug-in" angezeigt wird.
Kurzname der Bibliothek	**Ja**	Der Name in diesem Feld wird in der Spalte LIBRARY_NAME der Plug-in-Tabelle verwendet. Das Feld **Kurzname der Bibliothek** wird für den Aufbau des Namens der Softwarebibliotheksdatei verwendet, die vom Pipeline-Code aufgerufen wird. Es wird empfohlen, die in der tatsächlichen, von der Pipeline aufgerufenen Bibliotheksdatei verwendete Groß-/Kleinschreibung zu übernehmen. Der Grund hierfür ist, dass bei einigen Systemen die Groß-/Kleinschreibung beachtet werden muss. Diesem Namen wird von EAS je nach Betriebssystem ein Präfix und/oder Suffix hinzugefügt.
Version	**Ja**	Diese Feld wird zum Protokollieren der Versionsnummer der Softwarebibliothek verwendet.

7. Klicken Sie **Speichern** an.

Ergebnisse

Auf der Registerkarte **Plug-in** werden der Plug-in-Name und zugehörige Informationen angezeigt.

Entwickeln angepasster Scoring-Plug-ins für IBM InfoSphere Identity Insight

Mit IBM InfoSphere Identity Insight haben Sie die Möglichkeit, angepasste Scoring-Plug-ins zu erstellen und zusätzliche Typen von Attributdaten in den Prozess der Entitätsauflösung einzuschließen.

Zum Erstellen eines Scoring-Plug-ins für IBM InfoSphere Identity Insight müssen Sie mehrere Basiselemente einschließen und eine gemeinsam genutzte Bibliothek erzeugen. Angepasste Plug-ins sollten in einem Verzeichnis installiert werden, das im Bibliotheksladepfad angegeben ist.

Entwicklungsschnittstelle für Scoring-Plug-in

Angepasste Scoring-Plug-ins erfordern eine Standardschnittstelle.

Verwenden Sie Basisobjekte, um unabhängig von Bibliotheksversionen und Compileroptionen zu sein. Auf diese Weise können Plug-ins mit mehreren Pipeline-Versionen verwendet werden, ohne dass das Plug-in erneut erstellt werden muss, wenn sich für die Pipeline die Bibliothek, Compilerversionen oder andere Optionen ändern. Sie müssen die folgenden C- oder C++-Schnittstellenprototypen einschließen:

```
#ifdef _WIN32
#define _DLEXPORT __declspec(dllexport)
#else
#define _DLEXPORT
#endif

extern "C"
```

```
{
  _DLEXPORT const int initPlugin(const char *configInfo,
                                 const uint configSize,
                                 char *errorStr,
                                 const uint maxStrSize);
  _DLEXPORT const char *getVersion();
  _DLEXPORT const int score(const char *thresholdStr,
                            const uint thresholdSize,
                            const char *inboundStr,
                            const uint inboundSize,
                            const char *candidateStr,
                            const uint candidateSize,
                            char *result,
                            const uint resultSize);
};
```

getVersion

Angepasste Scoring-Plug-ins erfordern die Funktion 'getVersion'.

Beispiel

Folgendes muss eingeschlossen werden:

```
const char *getVersion();
```

return char * enthält eine auf null endende Zeichenfolge, die die Plug-in-Version beschreibt.

Implementieren Sie diese Funktion, indem Sie die Versionsnummer des Plug-ins in einer statischen Zeichenfolge speichern, und führen Sie einen Zeiger auf den Basiszeiger der Zeichenfolge zurück.

myPlugin.h umfasst Folgendes:

```
class MyPlugin
{
public:
  static const std::string mVersion;

};

myPlugin.cpp includes the following
const std::string MyPlugin::mVersion = std::string("1.0");

const char *getVersion ()
{
  return MyPlugin::mVersion.c_str();
}
```

initPlugin

Angepasste Scoring-Plug-ins erfordern eine Funktion 'initPlugin'.

Beispiel

initPlugin ermöglicht dem Plug-in das Laden und Speichern von Konfigurationsdaten, die für das Scoring benötigt werden. Die Zeichenfolge für die Datenbankverbindung und der Name der INI-Datei werden in der Zeichenfolge **configInfo** bereitgestellt. 'initPlugin' wird ein Mal für jeden Attributtyp aufgerufen, der ein Plug-in verwendet. Hierbei handelt es sich um gemeinsam genutzte Objekte. Soll die Verwendung des Plug-ins für mehr als einen Attributtyp unterstützt werden,

müssen die Konfigurationsdaten für jeden Attributtyp gespeichert werden. Auf diese Weise können die Konfigurationsdaten für den jeweiligen Attributtyp beim Aufrufen von 'score' gesucht werden.

```
const int initPlugin(const char *configInfo,
                     const uint configSize,
                     char *errorStr,
                     const uint maxStrSize);
```

configSize
ist die Länge der in 'configInfo' enthaltenen Zeichenfolge.

errorStr
ist ein vorab zugeordneter Hauptspeicherpuffer zum Kopieren einer auf null endenden Zeichenfolge. Die Zeichenfolge enthält XML zur Beschreibung von Fehlern bei der Initialisierung. Der Fehler muss folgendes Format aufweisen:

```
<ERROR>Fehlertext</ERROR>
```

maxStrSize
ist die Größe des vorab zugeordneten Hauptspeicherpuffers, auf den 'errorStr' verweist. Die Größe der Fehlerzeichenfolge darf diesen Wert nicht überschreiten.

Es folgt ein Pseudocodebeispiel der Funktion 'score':

```
const int initPlugin(const char *configInfo, const uint configSize,
char *errorStr, const uint maxStrSize)
{
  //create string out of configInfo
  //parse string with XML parser
  //extract DB_CONNECTION and CONFIG_FILE
  //connect to database
  //select config info from database
  //open CONFIG_FILE
  //read config info from .ini file

  //if there was an error create null terminated error string and
  //strcpy into errorStr. Return -1.
  //if no error, return 0.
}
```

'initPlugin' sollte beim Auftreten eines Fehlers '-1' zurückgeben.

score

Angepasste Scoring-Plug-ins erfordern eine Funktion 'score'.

score enthält folgende Parameter:

```
const int score(const char *thresholdStr,
                const uint thresholdSize,
                const char *inboundStr,
                const uint inboundSize,
                const char *candidateStr,
                const uint candidateSize,
                char *result,
                const uint resultSize);
```

thresholdStr
enthält die Bestätigungs-/Zurückweisungsschwellenwerte. Diese Schwellenwerte sind nicht erforderlich.

thresholdSize
ist die Größe der Zeichenfolge, die in 'thresholdStr' enthalten ist.

inboundStr
enthält das Attribut aus der eingehenden Entität, die bewertet wird.

inboundSize
ist die Größe der Zeichenfolge, die in 'inboundStr' enthalten ist.

candidateStr
ist der Zeiger auf eine Zeichenfolge, die das zu bewertende Attribut aus der Kandidatenentität enthält.

candidateSize
ist die Größe der Zeichenfolge, die in 'candidateStr' enthalten ist.

result ist ein vorab zugeordneter Hauptspeicherpuffer zum Kopieren einer auf null endenden Zeichenfolge, die XML zur Beschreibung der Scoring-Ergebnisse enthält. Bei einem Fehler stellen die Ergebnisse eine Beschreibung des Fehlers dar. Das Format dieser zurückgegebenen Zeichenfolge ist wie folgt definiert:

```
<SCORE_RESULT>
  <MATCH_SCORE>ganze Zahl 0-100</MATCH_SCORE>
  <CONFIRMATION>TRUE/FALSE</CONFIRMATION>
</SCORE_RESULT>
```

Bei einem Fehler lautet das Ergebnisformat wie folgt:

```
<ERROR>Fehlertext</ERROR>
```

resultSize
ist die Größe des vorab zugeordneten Hauptspeicherpuffers, auf den 'result' verweist. Die Ergebniszeichenfolge darf diese Größe nicht überschreiten. Da das Ergebnisdokument relativ klein ist, sollte dies kein Problem darstellen, außer bei extrem langen Fehlernachrichten.

Es folgt ein Pseudocodebeispiel der Funktion 'score':

```
const int score(const char *thresholdStr,
       const uint thresholdSize,
                const char *inboundStr,
       const uint inboundSize,
             const char *candidateStr,
       const uint candidateSize,
       char *result,
              const uint resultSize)
{
  //create strings out of thresholdStr, inboundStr, and candidateStr
  //create XML documents out of thresholdStr, inboundStr, and candidateStr
  //parse thresholds out of threshold xml doc if thresholds are used
  //parse values out of inbound xml doc
  //parse values out of candidate xml doc

  //check for any errors such as attr type mismatches, bad data, etc.
  //un-encode attr_value and attr_large_data data fields if necessary
  //apply scoring algorithm to attribute data
  //scale score into 0-100 range
  //determine confirmation or denial (possibly using thresholds)

  //if there was an error, create null terminated error string and
  //strcpy into result. Return -1.
  //if no error, create null terminated result document and strcpy into
  //result.  Return 0.
}
```

Die Funktion 'score' sollte beim Auftreten eines Fehlers '-1' zurückgeben.

Datenformate

Angepasste Scoring-Plug-ins erfordern die Angabe eines Datenformats.

Beispiel

Datenformat für Schwellenwerte

```
<THRESHOLDS>
  <CONFIRMATION_THRESHOLD>zeichenfolge</CONFIRMATION_THRESHOLD>
  <DENY_THRESHOLD>zeichenfolge</DENY_THRESHOLD>
</THRESHOLDS>
```

Die Schwellenwerte sind frei wählbare Zeichenfolgen. Sie werden aus der Tabelle MATCH_MERGE_ATTR geladen und müssen dem Format entsprechen, das vom Plug-in erwartet wird. Das Format wird vom Verfasser des Plug-ins definiert und kann von Plug-in zu Plug-in variieren.

Datenformat für Attribute

```
<ATTRIBUTE>
  <ATTR_TYPE_ID>ganze Zahl ohne Vorzeichen</ATTR_TYPE_ID>
  <ATTR_VALUE>Zeichenfolge</ATTR_VALUE>
  <ATTR_LARGE_DATA>Zeichenfolge</ATTR_LARGE_DATA>
</ATTRIBUTE>
```

ATTR_LARGE_DATA kann abhängig vom Attributtyp und ETL-Prozess eine leere Zeichenfolge sein. ATTR_LARGE_DATA ist optional und sollte nur verwendet werden, wenn die Daten eines Attributs zu groß für die Spalte ATTR_VALUE sind. Dies muss während der Systemkonfiguration festgelegt werden, damit das UMF (Universal Message Format) ordnungsgemäß erstellt und Plug-ins so geschrieben werden können, dass sie die richtigen Felder verwenden.

ATTR_LARGE_DATA kann so formatiert werden, dass es dem gültigen Zeichensatz von XML entspricht. Base64-Codierung wird empfohlen, diese erfolgt jedoch im ETL-Prozess. Das Plug-in muss die Daten in ATTR_LARGE_DATA möglicherweise decodieren. Die Zeichenfolge sollte auch UTF-8-codiert sein. Wurde die Zeichenfolge im ETL-Prozess Base64-codiert, dann ist die UTF-8-Zeichenfolge identisch mit der ASCII7-Zeichenfolge.

Es folgt ein Pseudocodebeispiel der Funktion 'score':

```
const int score(const char *thresholdStr,
       const uint thresholdSize,
                const char *inboundStr,
       const uint inboundSize,
              const char *candidateStr,
       const uint candidateSize,
       char *result,
              const uint resultSize)
{
  //create strings out of thresholdStr, inboundStr, and candidateStr
  //create XML documents out of thresholdStr, inboundStr, and candidateStr
  //parse thresholds out of threshold xml doc if thresholds are used
  //parse values out of inbound xml doc
  //parse values out of candidate xml doc

  //check for any errors such as attr type mismatches, bad data, etc.
  //un-encode attr_value and attr_large_data data fields if necessary
  //apply scoring algorithm to attribute data
  //scale score into 0-100 range
  //determine confirmation or denial (possibly using thresholds)

  //if there was an error, create null terminated error string and
```

```
  //strcpy into result. Return -1.
  //if no error, create null terminated result document and strcpy into
  //result.  Return 0.
}
```

Die Funktion 'score' sollte beim Auftreten eines Fehlers '-1' zurückgeben.

Erstellen des Plug-in-Objekts

Das Plug-in-Objekt muss in einer gemeinsam genutzten Bibliothek erstellt werden.

Informationen zu diesem Vorgang

Erstellen Sie das Objekt in einer gemeinsam genutzten Bibliothek (.dll unter Windows, .so unter Linux/UNIX). Alle Bibliotheken sollten statisch verbunden sein. Hierdurch werden potenzielle Abweichungen der Bibliotheksversion und nicht aufgelöste Symbole vermieden.

Kapitel 6. Verwalten von Pipelines

Pipelines sind das Herzstück des Systems. Dort findet die Verarbeitung statt, d. h., in Pipelines werden Entitäten aufgelöst, Beziehungen erkannt und Alerts generiert. Pipelines sind die primäre Methode für das Laden von Daten in die Entitätendatenbank. Das Verwalten von Pipelines ist eine fortlaufende Betriebstask, die das Konfigurieren von Pipelines, das Starten und Stoppen von Pipelines, das Überwachen von Pipelines und das Weiterleiten von Nachrichten von Pipelines an andere Pipelines, Knoten oder externe Systeme einschließt.

Pipelines

Pipelines sind die Komponenten, die Namens- und Adressbereinigungsstandardisierung, Datenqualitätsmanagement und Entitätsauflösung ausführen. Basierend auf der Systemkonfiguration lösen Pipelines auch Beziehungen auf und generieren Alerts.

Pipelines führen drei Kernprozesse aus:

- Erkennen: Hierzu gehört das Optimieren eingehender Daten durch die Ausführung von Datenstandardisierung, -bereinigung, -erweiterung und -qualitätsprüfungen.
- Auflösen: Hierzu gehört das Auflösen von Entitäten.
- Beziehungen erkennen: Hierzu gehört das Erkennen von Beziehungen und Generieren von Alerts.

Pipelines werden von Pipelineknoten gehostet.

Sie können Pipelines für Parallelverarbeitung konfigurieren, damit ein Befehl 'pipeline' mehrere parallele Pipelineverarbeitungsthreads startet, mit deren Hilfe das System mehrere Datenanforderungen gleichzeitig verarbeiten kann. Diese Funktion kann dazu beitragen, dass die Systemleistung verbessert, die Datenverarbeitungszeit gesenkt und Hardwarespeichereinschränkungen reduziert werden.

Die Pipelineparallelverarbeitung wird an zwei Stellen konfiguriert:

- Die Einstellung für den globalen gemeinsamen Zugriff wird über den Parameter `Gemeinsamer Zugriff für Pipeline (Standard)` auf der Registerkarte **Systemkonfiguration** in der Konfigurationskonsole gesteuert. Der hierfür angegebene Wert bestimmt die Anzahl Parallelverarbeitungsthreads, die von einem Pipelinestartbefehl gestartet werden. Der Standardwert für diesen Parameter ist 1, das heißt, es wird nur ein Pipelineverarbeitungsthread gestartet, sofern dieser Parameter nicht bearbeitet wird.
- Eine Einstellung für lokalen gemeinsamen Zugriff (nach Pipelineknoten) kann in der Pipelinekonfigurationsdatei konfiguriert werden. Wenn Sie einen Parameter für gemeinsamen Zugriff und einen Wert in der Pipelinekonfigurationsdatei nach Pipelineknoten angeben, überschreibt dieser Wert den globalen Systemparameter. Wenn Sie auf diesem Pipelineknoten einen Pipelinestartbefehl absetzen, starten Sie die in der Pipelinekonfigurationsdatei angegebene Anzahl gleichzeitig ablaufender Pipelineverarbeitungsthreads.

Pipelinekonfigurationsprüfung

Das System führt vor dem Start eines neuen Pipelineprozesses und in häufigen Intervallen eine Pipelinekonfigurationsprüfung für jede aktive Pipeline aus, um sicherzustellen, dass die Konfiguration der Pipeline gültig ist.

Während der Pipelinekonfigurationsprüfung überprüft das System, ob die Pipeline eine gültige Konfiguration hat:

- Ist die Konfiguration dieser Pipeline mit der Konfiguration in der Konfigurationskonsole identisch?
- Ist eine angemessene Anzahl Datensätze für jede Konfigurationstabelle, die von der Pipeline verwendet wird, vorhanden?
- Gibt es Standardwerte in bestimmten Konfigurationstabellen?
- Sind Konfigurationskennungen und -werte in bestimmten Konfigurationstabellen definiert?

Wenn diese Konfigurationsprüfungen nicht bestanden werden, protokolliert das System eine Warnung in den Protokolldateien oder beendet die Pipeline automatisch bzw. startet die Pipeline nicht und protokolliert einen Fehler (je nach Ausmaß der Abweichung).

Pipelineknoten

Pipelineknoten sind die physischen Maschinen, auf denen mindestens ein Pipelineprozess stattfindet.

Der Pipelineknoten ist die Lokation, an der Sie die ausführbare Pipelinedatei installieren und starten, die die Pipelineprozesse ausführt. Sie konfigurieren und verwalten die Pipelinekonfigurationsdatei für alle Pipelines, die von dieser Maschine gehostet werden. Das System schreibt die Pipelinenachrichten außerdem in die Protokolldateien auf den Pipelineknoten.

Pipelineknoten verbinden Pipelineprozesse mit den folgenden Komponenten der Produktarchitektur:

Übernahmeprogramme
Im Rahmen des ETL-Prozesses (Extrahieren, Transformieren und Laden) verwenden Übernahmeprogramme Transportmethoden, um UMF-Daten zur Verarbeitung an Pipelines zu senden. Sie verwenden die Transportmethode, die für das Übernahmeprogramm geeignet ist, über das die Verbindung zu den Pipelines hergestellt wird. Wenn Sie z. B. das UMF-Dateidienstprogramm als Übernahmeprogramm einsetzen, verwenden Sie die Dateitransportmethode.

Entitätendatenbank
Die Entitätendatenbank enthält Entitätsinformationen. Pipelines greifen während der Verarbeitung von eingehenden Datensätzen für Entitäts- und Beziehungsauflösung auf Entitätsinformationen zu. Für den Pipelineknoten muss der entsprechende Datenbankclient installiert und konfiguriert sein, damit die Pipelines auf die Entitätendatenbank zugreifen können.

Warteschlangen
Wenn Ihr System Warteschlangen als Transportmethode für das Senden von Daten zur Verarbeitung an die Pipelines verwendet, müssen Sie die entsprechende Software zur Steuerung von Nachrichtenwarteschlangen auf jedem Pipelineknoten installieren und konfigurieren.

Adressbereinigungsserver
Wenn Ihr System zur zusätzlichen Adressbereinigung Adressbereinigungsprodukte anderer Firmen verwendet, muss jeder Pipelineknoten so konfiguriert werden, dass eine Verbindung zu den Adressbereinigungsservern hergestellt werden kann.

Web-Services
Sie müssen die Transportmethode HTTP verwenden, um die Pipelineprozesse auf dem Pipelineknoten mit den Web-Services zu verbinden.

Starten von Pipelines

Bevor eine Pipeline Daten empfangen und verarbeiten kann, muss sie gestartet werden. Es ist üblich, mehrere Pipelines auszuführen, um den Datendurchsatz zu erhöhen oder um unterschiedliche Typen von Quellendaten zu verarbeiten. Verwenden Sie die folgenden Schritte, um eine Pipeline zu starten oder um eine inaktive Pipeline erneut zu starten.

Vorbereitende Schritte

- Für den Pipelineknoten, von dem diese Pipeline gehostet wird, muss die ausführbare Datei für die Pipeline installiert sein.
- Es muss mindestens eine Pipelinekonfigurationsdatei für die Verwendung mit der Pipeline konfiguriert sein, die Sie starten wollen. Sie können die zu verwendende Pipelinekonfigurationsdatei als Teil des Befehls zum Starten der Pipeline angeben. Wenn Sie den Namen der Konfigurationsdatei nicht als Teil des Befehls 'pipeline' angeben, muss sich die Pipelinekonfigurationsdatei auf dem Pipelineknoten befinden und sie muss mit dem Namen der ausführbaren Datei (dem angegebenen Pipelinenamen) übereinstimmen. Beispiel: pipeline.ini.
- Die Datenbankumgebungsvariablen müssen festgelegt sein. Siehe Setzen der Umgebungsvariablen.
- Wenn Sie ein Script zum Starten von Pipelines verwenden, müssen Sie sicherstellen, dass sich das Script in demselben Verzeichnis befindet, in dem Sie die Pipeline starten.
- Wenn der Wert des Systemparameters *DEFAULT_CONCURRENCY* auf einen Wert größer-als 1 gesetzt ist oder Sie den Parameter *concurrency* in der Pipelinekonfigurationsdatei für den Pipelineknoten konfiguriert haben, können Sie mit *einem* Befehl zum Starten einer Pipeline mehrere parallel ablaufende Pipelineverarbeitungsthreads starten.

Informationen zu diesem Vorgang

Das Starten einer Pipeline erfolgt in drei Schritten:

Vorgehensweise

1. Jede Pipeline muss auf ihrem Pipelineknoten über einen eindeutigen Namen verfügen. Stellen Sie daher sicher, dass keine anderen Pipelines ausgeführt werden, die denselben Namen haben wie die Pipeline, die Sie starten wollen. (Der Standardpipelinename ist `pipeline`.) Geben Sie in einer Eingabeaufforderung den folgenden Befehl ein, um dies zu prüfen: `pipeline -n pipelinename -l`

   Dabei ist *`pipelinename`* der Name, mit dem Sie die neue Pipeline starten wollen. Stellen Sie sicher, dass dieser Name mit dem Namen übereinstimmt, der in der Konfigurationskonsole für diese Pipeline registriert ist.

2. Starten Sie an einer Eingabeaufforderung eine Pipeline oder mehrere Pipelines, indem Sie die entsprechenden Optionen und Parameter des Befehls 'pipeline' im folgenden Format eingeben:

   `pipeline -option parameter`

3. Prüfen Sie, ob der Befehl erfolgreich ausgeführt wurde und ob die Pipeline gestartet wurde und aktiv ist.
   a. Wenn Ihr System auf einer Microsoft Windows-Plattform ausgeführt wird und Sie die Pipelineoption für Services verwenden, können Sie den Status der Pipeline in der Microsoft Windows-Systemsteuerung unter **Dienste** sehen.
   b. Wenn Ihr System auf einer UNIX-Plattform ausgeführt wird und Sie die Pipelineoption für Dämonen verwenden, können Sie den folgenden Befehl eingeben, um auf aktive Prozesse zu prüfen:

      `ps -fu benutzer-id`

      Dabei ist *benutzer-id* die Kennung des Benutzers, der die Pipeline startet.
   c. Alternativ können Sie auch in einer Eingabeaufforderung den folgenden Befehl eingeben:

   `pipeline -n pipelinename -l`

   Dabei ist *pipelinename* der Name der Pipeline, die Sie gerade gestartet haben. Wenn die Pipeline aktiv ist, gibt die Eingabeaufforderung die Information `Aktiv` zurück.

Stoppen von Pipelines

Das Stoppen einer Pipeline bedeutet, dass ihr Status von **Aktiv** und **Offen** für die Verarbeitung von Daten in den Status **Inaktiv** und **Geschlossen** für eingehende Daten geändert wird. Sie können jeweils nur eine Pipeline manuell stoppen. Wenn Sie einen Hotfix oder ein Upgrade-Release installieren oder wenn Sie Konfigurationsänderungen am Pipelineknoten vornehmen, von dem die Pipeline gehostet wird, verwenden Sie die folgenden Anweisungen, um die Pipeline zu stoppen, nachdem Sie Änderungen an der Systemkonfiguration vorgenommen haben (starten Sie die Pipeline anschließend erneut, damit die Konfigurationsänderungen wirksam werden).

Vorgehensweise

1. Prüfen Sie, ob die Pipeline, die Sie stoppen wollen, gerade aktiv ist. Verwenden Sie dazu den folgenden Befehl: `pipeline -n pipelinename -l` Dabei ist *pipelinename* der Name der Pipeline, die Sie stoppen wollen. Die Eingabeaufforderung gibt `Aktiv` zurück, wenn die Pipeline aktiv ist.
2. Geben Sie in einer Befehlszeile den Befehl zum Stoppen einer Pipeline ein: `pipeline -e -n pipelinename` Dabei ist *pipelinename* der Name der Pipeline, die Sie stoppen wollen.

   Anmerkung: Wenn Sie die Pipeline mit der Befehlsoption für das Beheben von Pipelinefehlern gestartet haben, können Sie die Pipeline stoppen, indem Sie die Tastenkombination **Strg** + **C** in einer Befehlszeile drücken.
3. Prüfen Sie, ob der Befehl erfolgreich ausgeführt und die Pipeline gestoppt wurde: `pipeline -n pipelinename -l` Dabei ist *pipelinename* der Name der Pipeline, die Sie gerade gestoppt haben. Die Eingabeaufforderung gibt `Gestoppt` zurück, wenn die Pipeline gestoppt wurde.

Konfigurieren von Pipelines

Wenn eine Pipeline gestartet wird, sucht sie nach einer Pipelinekonfigurationsdatei, der sie ihre Startvariablen sowie die Konfigurationsdaten entnimmt, die für die Verarbeitung eingehender Daten erforderlich sind. Standardmäßig wird beim Installieren einer Pipeline auf dem Pipelineknoten auch eine Standarddatei für die Pipelinekonfiguration mit dem Namen pipeline.ini installiert. Diese kann von allen Pipelines auf diesem Pipelineknoten verwendet werden. Einige Abschnitte dieser Standarddatei müssen jedoch speziell für die auf dem Pipelineknoten ausgeführten Pipelines konfiguriert werden, sodass die Pipelines über die korrekten Verbindungen verfügen und auf die Entitätendatenbank zugreifen können. Verwenden Sie die folgenden Anweisungen, um die Pipelinekonfigurationsdatei zu konfigurieren.

Vorbereitende Schritte

- Sie müssen den genauen Namen der Entitätendatenbank und die Anmeldeinformationen kennen, die für den Zugriff auf die Entitätendatenbank erforderlich sind.
- Wenn Ihr System eine Verbindung zu einer externen Adresskorrektursoftware herstellt, müssen Sie den Namen des Hostsystems für die Adresskorrektursoftware kennen und die korrekten Einstellungen für diese Software auswählen können.
- Damit die Konfigurationsdateiänderungen in Kraft treten, müssen Sie alle aktiven Pipelines auf diesem Pipelineknoten stoppen und nach der Implementierung der Änderungen erneut starten.

Informationen zu diesem Vorgang

Die Konfigurationsdatei pipeline.ini ist eine normale ASCII-Textdatei. Sie können die Datei mit einem beliebigen ASCII-Texteditor bearbeiten.

Vorgehensweise

1. Erstellen Sie eine Kopie der Standardkonfigurationsdatei pipeline.ini und bewahren Sie die ursprüngliche Version der Datei auf. Wenn Sie die ursprüngliche Version der Datei aufbewahren, können Sie bei Bedarf jederzeit zu dieser Version zurückkehren.
2. Öffnen Sie die Kopie der Konfigurationsdatei pipeline.ini in einem beliebigen Texteditor.
3. Aktualisieren Sie die Datei so, dass sie die korrekte Konfiguration für die Pipelines angibt, die auf diesem Pipelineknoten ausgeführt werden. In der Regel sind die Standardwerte in der Standarddatei für die Pipelinekonfiguration korrekt; Sie müssen lediglich die Informationen zur Datenbankverbindung unter der Überschrift [SQL] und die Informationen zur Adresskorrektur im Abschnitt [OAC] eingeben bzw. aktualisieren, falls Ihr System eine externe Adresskorrektursoftware verwendet.
4. Speichern Sie die aktualisierte Pipelinekonfigurationsdatei. Es empfiehlt sich, die Datei in dem Verzeichnis zu speichern, das die ausführbare Datei für den Befehl 'pipeline' enthält. (Andernfalls müssen Sie jedes Mal, wenn Sie eine Pipeline auf diesem Pipelineknoten starten, den Namen der Pipelinekonfigurationsdatei mit vollständigem Pfad angeben.)

Nächste Schritte

Wenn Sie vor der Implementierung der Änderungen alle aktiven Pipelines auf diesem Pipelineknoten gestoppt haben, können Sie die Pipelines jetzt erneut starten.

Wenn Sie vor der Implementierung der Änderungen die aktiven Pipelines nicht gestoppt haben, sollten Sie sie jetzt stoppen und erneut starten. Bei aktiven Pipelines werden die Änderungen an der Pipelinekonfigurationsdatei erst angewendet, wenn sie erneut gestartet wurden. Werden Pipelinekonfigurationsdaten geändert, ohne die Pipelines zu stoppen, können auf Grund falscher Werte in der Pipelinekonfigurationsdatei Pipelinefehler auftreten oder sogar Pipelines beendet werden.

Pipelineregistrierung

Sie müssen Pipelines in der Konfigurationskonsole registrieren, bevor Sie ihre Status überwachen oder Ergebnisse weiterleiten können. Das Registrieren von Pipelines unterscheidet sich vom Installieren oder Konfigurieren einer Pipeline. Als Registrieren wird das Hinzufügen der Pipeline zur Registerkarte **Pipelines** in der Konfigurationskonsole bezeichnet.

Das System verwendet die auf der Registerkarte **Pipelines** registrierten Informationen, um die Pipeline eindeutig anzugeben. Diese Informationen werden vom Anwendungsmonitor verwendet, um den Status und Statistikdaten überwachter Pipelines aufzulisten oder Kommunikationen und Ergebnisse zwischen den Pipelines und anderen Systemen weiterzuleiten. Den Namen, den Sie für eine Pipeline registrieren, müssen Sie in derselben Form (einschließlich Groß-/Kleinschreibung) zum Starten der Pipeline verwenden. Wenn Sie einen anderen Namen verwenden oder beim Namen von der Groß-/Kleinschreibung des Namens der registrierten Pipeline abweichen, erkennt der Anwendungsmonitor die Pipeline nicht und leitet keine ihrer Daten weiter bzw. überwacht sie nicht.

Nach der Registrierung einer Pipeline auf der Registerkarte **Pipelines** können Sie auf der Registerkarte **Routing** Routing-Regeln für die Pipeline konfigurieren und/oder über die Registerkarte **Pipelinestatus** den Status und die Statistikdaten der Pipeline überwachen. Sie können den Status und die Statistikdaten einer Pipeline nur dann überwachen, wenn Sie beim Registrieren der Pipeline angeben, dass das System die Pipeline überwachen soll.

Sie können den Namen einer registrierten Pipeline nicht bearbeiten. Sie können jedoch die anderen Informationen zur Pipeline aktualisieren. Wenn sich z. B. der Name des Pipelineknotens ändert, oder wenn Sie die Überwachung des Status und der Statistikdaten für die Pipeline starten wollen, können Sie diese Informationen bearbeiten.

Registrieren von Pipelines

Für das Registrieren einer Pipeline gibt es drei Gründe: Sie wollen den Anwendungsmonitor zum Überwachen des Status und der Statistikdaten der Pipeline verwenden und/oder Routing-Regeln für die Pipeline konfigurieren. Sie können eine vollständig neue Pipelineregistrierung hinzufügen oder eine vorhandene registrierte Pipeline als Basis für die Registrierung verwenden.

Vorbereitende Schritte

Ihnen muss der eindeutige Name der Pipeline und der Name des Pipelineknotens bekannt sein, von dem die Pipeline gehostet wird. Es ist nicht erforderlich, dass die Pipeline auf dem Pipelineknoten installiert und konfiguriert ist, bevor Sie sie registrieren. (Sie muss jedoch installiert und konfiguriert sein, damit das System die Pipeline überwachen oder Daten an die Pipeline weiterleiten kann.)

Informationen zu diesem Vorgang

Tipp: Wenn Sie mehrere Pipelines hinzufügen, die alle auf demselben Pipelineknoten ausgeführt werden, empfiehlt es sich möglicherweise, zunächst eine Pipeline zu registrieren und anschließend die anderen Pipelines auf der Basis der ersten zu klonen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Pipelines** an.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie die Schaltfläche **Neu** an, um eine neue Pipeline zu registrieren.
   - Klicken Sie die Schaltfläche **Klonen** an, um eine neue Pipeline auf der Basis einer vorhandenen Pipeline zu registrieren.
5. Geben Sie auf der Registerkarte **Allgemein** einen eindeutigen Pipelinenamen, eine Beschreibung und einen Pipelineknotennamen an. Geben Sie zudem an, ob der Status und die Statistikdaten der Pipeline überwacht werden sollen.

   Anmerkung:
   - Der Pipelinename, den Sie eingeben, muss mit dem Namen identisch sein, den Sie zum Starten dieser Pipeline verwenden. Bei diesem Namen muss die Groß-/Kleinschreibung beachtet werden. Der Name, den Sie zum Starten der Pipeline angeben, muss also genau mit diesem registrierten Pipelinenamen übereinstimmen. Wenn die Namen nicht genau überstimmen (einschließlich Groß-/Kleinschreibung), funktionieren weder die für diese Pipeline konfigurierten Routing-Regeln noch die Anwendungsüberwachung für diese Pipeline.
   - Wenn der Status und die Statistikdaten für diese Pipeline auf der Registerkarte **Pipelinestatus** in der Konfigurationskonsole berichtet werden sollen, wählen Sie **Ja** im Feld **Überwacht** aus.
6. Klicken Sie die Schaltfläche **Speichern** an.

Nächste Schritte

Wenn die Pipeline erfolgreich hinzugefügt wurde, wird sie in der Liste auf der linken Seite angezeigt. Sie können nun Routing-Regeln für diese Pipeline konfigurieren oder das System zur Überwachung der Pipeline verwenden. Beachten Sie jedoch, dass der Name zum Starten der Pipeline genau mit dem im Feld **Pipelinename** registrierten Namen übereinstimmen muss (einschließlich Groß-/Kleinschreibung), damit Daten erfolgreich an die Pipeline weitergeleitet werden können bzw. die Pipeline erfolgreich überwacht werden kann.

Anzeigen von Details registrierter Pipelines

Sie können die Details einer in der Konfigurationskonsole registrierten Pipeline anzeigen, um sicherzustellen, dass die Registrierungsinformationen aktuell sind. Sie registrieren Pipelines, um dem System die Überwachung von Pipelineleistung und –statistikdaten und/oder die Weiterleitung an Pipelines zu ermöglichen.

Vorbereitende Schritte

- Die Pipeline muss in der Konfigurationskonsole registriert sein.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Status** an.
2. Klicken Sie die Schaltfläche **Status** an.
3. Klicken Sie die Registerkarte **Übersicht** an.
4. Klicken Sie den registrierten Namen der Pipeline an.

Ergebnisse

Überprüfen Sie im Fenster **Detail** die Details der ausgewählten Pipeline.

Bearbeiten von Pipelineregistrierungen

Bearbeiten Sie die Informationen zu einer registrierten Pipeline, sobald eine Schlüsselkomponente der Pipelineregistrierung, wie z. B. der Name des Pipelineknotens, geändert wurde. Die einzige Angabe, die Sie nicht ändern können, ist der für eine Pipeline registrierte Name. Wenn Sie den registrierten Namen für eine Pipeline ändern müssen, löschen Sie die Pipelineregistrierung und fügen sie mit den richtigen Informationen erneut hinzu. Sie können aber auch eine andere Pipelineregistrierung hinzufügen.

Informationen zu diesem Vorgang

Wenn die zu bearbeitende Pipeline aktiv ist (gerade ausgeführt wird), ist es sinnvoll, dass Sie die Pipeline stoppen, bevor Sie ihre Registrierung bearbeiten. Dies ist insbesondere dann wichtig, wenn Sie den Überwachungsstatus ändern.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Pipelines** an.
4. Wählen Sie die zu bearbeitende(n) Pipeline(s) aus und klicken Sie anschließend die Schaltfläche **Bearbeiten** an.
5. Ändern Sie die Informationen.

   Anmerkung: Beachten Sie, dass Sie das Feld **Überwacht** auf **Ja** setzen müssen, um den Status und die Statistikdaten der Pipeline auf der Registerkarte **Pipelinestatus** zu überwachen.
6. Klicken Sie die Schaltfläche **Speichern** an.

Ergebnisse

Sie können Ihre Änderungen auf der Registerkarte **Pipelines** anzeigen.

Nächste Schritte

Wenn Sie die Pipeline gestoppt haben, starten Sie sie erneut.

Löschen von Pipelineregistrierungen

Durch das Löschen einer Pipelineregistrierung in der Konfigurationskonsole wird die Pipeline nicht physisch aus dem System gelöscht. Die Pipeline wird lediglich auf den Registerkarten **Pipelines**, **Routing-Regeln** und **Pipelinestatus** entfernt. Es ist nicht mehr möglich, für diese gelöschten Registrierungen Daten unter Verwendung von Routing-Regeln weiterzuleiten oder Überwachungsinformationen zum

Status und Statistikdaten bereitzustellen. Einen registrierten Pipelinenamen können Sie nicht bearbeiten. Wenn Sie den Namen einer registrierten Pipeline ändern müssen, stehen zwei Verfahren zur Verfügung: Entweder Sie löschen die Pipelineregistrierung und fügen sie anschließend mit den korrekten Informationen wieder hinzu, oder Sie fügen eine neue Pipelineregistrierung hinzu.

Informationen zu diesem Vorgang

Wenn die zu löschende Pipeline aktiv ist (d. h., sie wird zurzeit ausgeführt) und vom System überwacht wird (d. h., auf der Registerkarte **Pipelinestatus** werden Daten angezeigt), ist es sinnvoll, die Pipeline zu stoppen, bevor Sie sie löschen. Außerdem sollten Sie auf der Registerkarte **Routing-Regeln** überprüfen, ob dieser Pipeline Routing-Regeln zugeordnet sind. Ist dies der Fall, empfiehlt es sich, diese Routing-Regeln vor dem Löschen dieser Pipeline einer anderen Pipeline zuzuordnen oder eine neue Pipeline hinzuzufügen, die diese Routing-Regeln verwendet.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** an.
2. Klicken Sie die Schaltfläche **Allgemein** an.
3. Klicken Sie die Registerkarte **Knoten** an.
4. Wählen Sie die Pipeline(s) aus, die Sie löschen wollen, und klicken Sie die Schaltfläche **Löschen** an.

Nächste Schritte

Die gelöschte Pipeline wird nicht mehr auf der Registerkarten für Knoten oder der Registerkarte **Routing-Regeln** angezeigt. Der Status der gelöschten Pipeline wird nicht mehr auf der Registerkarte **Pipelinestatus** berichtet. Das System leitet keine Daten mehr anhand der Routing-Regeln weiter, die der gelöschten Pipeline auf der Registerkarte **Routing-Regeln** zugeordnet waren.

Hilfethemen

Registerkarte 'Pipelines'

Über die Registerkarte **Pipelines** können Sie eine Pipeline registrieren oder registrierte Pipelines bearbeiten, löschen oder anzeigen. Sind Pipelines auf dieser Registerkarte registriert und ist ein SNMP-Agent auf dem Pipelineknoten, auf dem die registrierte Pipeline ausgeführt wird, installiert und konfiguriert, werden der Status, die Leistung sowie Statistikdaten für die Pipeline auf der Registerkarte **Status** angezeigt. Sie können außerdem die Registerkarte **Routing-Regeln** verwenden, um die Ergebnisse von einer registrierten Pipeline an andere Datenbanken oder externe Systeme weiterzuleiten.

Pipelinename
Listet die Namen aller Knoten in alphabetischer Reihenfolge auf, die in der Konfigurationskonsole für die Anwendungsüberwachung registriert sind.

Beschreibung
Stellt weiteren beschreibenden Text bereit, der Ihnen hilft, diesen Knoten von anderen Systemknoten zu unterscheiden.

Hostname
Zeigt den Namen des Pipelineknotens an, der diese Pipeline hostet. (Wenn Sie planen, diese Pipeline zu überwachen, ist dies zudem der Server, auf dem ein SNMP-Agent installiert und aktiv sein muss.)

Überwacht

Zeigt an, ob der Status und die Statistikdaten für diese Pipeline überwacht und auf der Registerkarte **Status** berichtet werden. (Dies entspricht nicht dem aktuellen Status der Pipeline; diese Spalte gibt an, wie diese Pipeline zurzeit registriert ist.)

- Ja gibt an, dass diese registrierte Pipeline vom Anwendungsmonitor überwacht wird.
- Nein gibt an, dass diese Pipeline nicht für die Anwendungsüberwachung konfiguriert ist. Sie kann jedoch für Routing konfiguriert sein.

Pipelines - Registerkarte 'Details'

Über diese Registerkarte können Sie eine Pipeline registrieren oder die Details einer vorhandenen registrierten Pipeline anzeigen. Sie müssen eine Pipeline registrieren, bevor Sie auf der Registerkarte **Routing** Routing-Regeln für die Pipeline konfigurieren oder auf der Registerkarte **Status** die Statistikdaten und den Status der Pipeline überwachen können.

Alle Felder auf dieser Registerkarte sind für die erfolgreiche Registrierung einer Pipeline erforderlich. Nachdem eine Pipeline registriert wurde, können Sie alle Daten mit Ausnahme des Pipelinenamens ändern. Müssen Sie beispielsweise den Namen des Pipelineknotens (Feld **Hostname**) ändern, bearbeiten Sie diesen Namen. Wollen Sie jedoch den Pipelinenamen ändern, löschen Sie zuerst den falschen, hier registrierten Pipelinenamen und fügen die Pipeline mit den korrekten Informationen anschließend erneut hinzu.

Pipelinename

Geben Sie einen eindeutigen Namen für die Pipeline ein, der aus maximal 15 Zeichen besteht. Wenn Sie diese Pipeline für Routing verwenden oder überwachen wollen, muss der Name, den Sie beim Starten der Pipeline angeben, genau mit diesem registrierten Pipelinenamen übereinstimmen, einschließlich Groß-/Kleinschreibung.

In der Liste auf der linken Seite werden die Namen aller Pipelines angezeigt, die bereits registriert sind.

Beschreibung

Geben Sie eine Beschreibung für die Pipeline ein, um sie von den anderen Pipelines zu unterscheiden. Verwenden Sie dabei maximal 50 Zeichen. Geben Sie in der Beschreibung beispielsweise den Zweck des Systems oder den Typ der Datenquellen an, den das System verarbeitet.

Hostname

Geben Sie den Namen des Pipelineknotens an, der diese Pipeline ausführt.

Überwacht

Wählen Sie aus, ob der Anwendungsmonitor den Status dieser Pipeline berichtet.

- **Ja** gibt an, dass Sie den Status und die Statistikdaten für diese Pipeline überwachen wollen. Wenn diese Pipeline ordnungsgemäß in der Konfigurationskonsole registriert wurde und der SNMP-Agent auf dem Pipelineknoten ausgeführt wird, werden der Status und die Statistikdaten für diese Pipeline auf der Registerkarte **Status** angezeigt.
- **Nein** gibt an, dass Sie die Pipeline für das Routing, jedoch nicht für die Überwachung registrieren wollen. Informationen zum Status oder Statistikdaten für diese Pipeline werden nicht auf der Registerkarte **Status** angezeigt; Sie können jedoch Routing-Regeln für die registrierte Pipeline konfigurieren.

Konfigurieren von Routing-Regeln

Mithilfe von Routing-Regeln können Sie die Ergebnisse der Pipelineverarbeitung oder des Übernahmeprogramms an eine Datenbank, eine Pipeline oder ein externes System weiterleiten. Routing-Regeln werden über die Registerkarte **Routing-Regeln** der Konfigurationskonsole konfiguriert. Sie können jedoch nur Daten von Pipelines oder Übernahmeprogrammen weiterleiten, die für den Anwendungsmonitor registriert wurden. Sie können entweder eine vollständig neue Routing-Regel konfigurieren oder eine vorhandene Routing-Regel als Basis verwenden.

Vorbereitende Schritte

- Die Pipeline oder das Übernahmeprogramm, von der bzw. dem Sie Daten weiterleiten wollen, muss für den Anwendungsmonitor registriert sein.
- Sie müssen den genauen eindeutigen Namen kennen, mit dem die Pipeline oder das Übernahmeprogramm registriert wurde.
- Sie müssen die Transportmethode und die genaue URI-Syntax kennen, die für die Weiterleitung an das Ziel zu verwenden sind.

Vorgehensweise

1. Klicken Sie die Registerkarte **Konfiguration** an.
2. Klicken Sie die Registerkarte **Allgemein** an.
3. Klicken Sie die Registerkarte **Routing-Regeln** an.
4. Führen Sie einen der folgenden Schritte durch:
   - Klicken Sie die Schaltfläche **Neu** an, um eine vollständig neue Routing-Regel zu konfigurieren.
   - Wählen Sie das Kontrollkästchen neben der Routing-Regel aus, auf der die neue Regel basieren soll, und klicken Sie die Schaltfläche **Klonen** an, um eine neue Routing-Regel auf der Basis einer vorhandenen Routing-Regel zu konfigurieren.
5. Erforderlich: Geben Sie in das Feld **Ausgangspipeline** den registrierten Namen der Pipeline oder des Anwendungsprogramms ein, von der bzw. dem Sie Daten weiterleiten wollen. Der Name, den Sie eingeben, muss genau mit dem Namen übereinstimmen, der auf der Registerkarte **Pipelines** registriert wurde.
6. Erforderlich: Geben Sie in das Feld **Reihenfolge** eine Zahl zwischen 0 und 999 ein. Diese Zahl gibt die Reihenfolge an, in der das System diese Routing-Regel verwendet. Der Systemstandardwert für dieses Feld ist 0. Diese Zahl gibt die erste Routing-Regel an, die für eine Pipeline oder ein Übernahmeprogramm verarbeitet wird. Die Zahl in diesem Feld muss für diese Pipeline bzw. dieses Übernahmeprogramm eindeutig sein, besonders wenn für die Pipeline oder das Übernahmeprogramm bereits mehrere Routing-Regeln konfiguriert sind.

   Anmerkung: Im linken Teilfenster dieser Registerkarte finden Sie eine Liste der Pipelines oder Übernahmeprogramme, für die konfigurierte Routing-Regeln vorhanden sind. Wenn diese Pipeline oder dieser Knoten in der Liste enthalten ist, suchen Sie die höchste Zahl hinter dem Doppelpunkt nach dem Namen der Pipeline oder des Übernahmeprogramms und geben Sie anschließend die nächsthöhere Zahl ein. Beispiel: Wenn Sie eine neue Routing-Regel für PIPE08 konfigurieren und die Liste im linken Teilfenster PIPE08:0 enthält, geben Sie in das Feld für die Reihenfolge die Zahl 1 oder eine höhere Zahl ein.
7. Erforderlich: Geben Sie in das Feld **Ziel** den Transport-URI für das Ziel der weitergeleiteten Informationen ein. Diese Information teilt dem System mit, wie die Daten an die Zielpipeline, die Zieldatenbank oder das externe Zielsystem weiterzuleiten sind.

Anmerkung: Damit die Weiterleitung erfolgreich ist, muss der Zugriff auf den Zielprozess mit dem angegebenen Transport-URI möglich sein. Beispiel: Ist das Ziel eine Pipeline, muss derselbe Transport-URI zum Starten der Pipeline verwendet werden.

8. Erforderlich: Wählen Sie in der Dropdown-Liste **Dokument** den UMF-Dokumenttyp aus, um den Nachrichtentyp anzugeben, der an das Ziel weitergeleitet wird.
9. Optional: Geben Sie in das Feld **Routenfilter** einen Filter ein, der auf die weiterzuleitenden Informationen angewendet werden soll, sodass das System nur bestimmte Informationen an das Ziel weiterleitet. Filter sind eine erweiterte Funktion der Routing-Regeln. Sie geben einen Filterausdruck `MODDIST(`*`UMF-tagname`* ein. Dabei gibt (*`UMF-tagname`* den Namen des UMF-Tags an, den das System zum Verteilen der Datensätze verwendet.
10. Erforderlich: Wählen Sie in der Dropdown-Liste **Aktiviert** die Option **Ja** aus, um diese Routing-Regel zu aktivieren.
11. Erforderlich: Klicken Sie die Schaltfläche **Speichern** an.

Beispiel

Nächste Schritte

Der Name der Pipeline oder des Übernahmeprogramms wird auf der Registerkarte **Routing-Regeln** zusammen mit den Details der Routing-Regel angezeigt, die Sie gerade konfiguriert haben. Das System beginnt mit der Weiterleitung der Daten von der Pipeline oder dem Übernahmeprogramm an das Ziel und verwendet dabei die konfigurierte Routing-Regel.

Routing-Regeln

Routing-Regeln weisen den Anwendungsmonitor an, Nachrichten aus einem Übernahmeprogramm an eine Pipeline oder aus einer Pipeline an eine Datenbank oder ein externes System zu senden. Routing-Regeln können nur für Pipelines konfiguriert werden, die für den Anwendungsmonitor registriert wurden. Die Ergebnisse können jedoch mit ordnungsgemäßer Transport-URI-Syntax (URI - Universal Resource Indicator) an ein beliebiges Ziel weitergeleitet werden.

Für Routing-Regeln gibt es viele Verwendungszwecke wie die folgenden gängigen Verwendungen:

- Gleichmäßiges Verteilen der Datenlast aus einem Übernahmeprogramm (wie dem UMF-Datenbankdienstprogramm) an mehrere Pipelines, die die Daten verarbeiten
- Übertragen der Ergebnisse der Pipelineverarbeitung (wie Alerts) für zusätzliche Untersuchungs- oder Berichterstellungszwecke in ein externes System oder eine Berichtsdatenbank

UMF-Dokumente und Routing-Regeln

Routing-Regeln sind für das Weiterleiten von Nachrichten unter Verwendung von mindestens einem UMF-Dokumenttyp konfiguriert. Ihre Auswahl hängt von den Informationen ab, die sich aus der Pipeline oder dem Systemknoten ergeben, aus der bzw. dem Sie Daten weiterleiten wollen. Beispielsweise ist UMF_ALERT ein UMF-Dokumenttyp, der Alerts darstellt, die aus der Verarbeitung von Identitäts- und Entitätsdatensätzen über eine Pipeline generiert wurden. Sie könnten von ei-

ner bestimmten Pipeline generierte Alerts an ein externes System weiterleiten, beispielsweise eine Benutzerschnittstelle, über die Analysten vom System erzeugte Alerts untersuchen.

Sie können eine Routing-Regel konfigurieren, um alle UMF-Dokumenttypen oder einen bestimmten UMF-Dokumenttyp einschließlich angepasster UMF-Dokumenttypen weiterzuleiten, die für Ihr System konfiguriert wurden.

Filter

Sie können die Informationen filtern, die an das Ziel weitergeleitet werden, in dem Sie beim Konfigurieren einer Routing-Regel einen Filterausdruck angeben. Filter geben an, dass nur bestimmte Informationen an das Ziel weitergeleitet werden sollen.

Sie erstellen einen Routing-Filter mit dem Ausdruck `MODDIST(`*`UMF-tagname`*`)`. Dabei gilt Folgendes:

`MODDIST`
: Ist der Ausdruck, der eine Modulusverteilung angibt.

`(`*`UMF-tagname`***`)`**
: Gibt den UMF-Tag an, der dem System mitteilt, wie die Datensätze verteilt werden sollen. Mithilfe des angegebenen UMF-Tags fasst das System die ASCII-Werte aller Zeichen in diesem Tag zusammen, um die Anzahl Leitwege zu ermitteln, die zum gleichmäßigen Verteilen der Datenverarbeitungslast erforderlich sind.

Wenn Sie alle Datensätze aus dem Datenquellencode „datenquelle5" an eine separate Berichtsdatenbank weiterleiten wollen, können Sie eine Routing-Regel mit dem Filterausdruck `MODDIST(datenquelle5)` konfigurieren. Dabei ist `datenquelle5` der Datenquellencode.

Routing-Prozess

Wenn für eine Pipeline oder ein Übernahmeprogramm eine Routing-Regel konfiguriert ist, schließt der Anwendungsmonitor den Routing-Prozess wie im Folgenden dargestellt ab:

1. Wenn die Pipeline oder das Übernahmeprogramm gestartet wird, sendet sie bzw. es über eine UMF-Nachricht eine Anforderung an den Anwendungsmonitor.
2. Der Anwendungsmonitor empfängt die Anforderung und sucht nach allen aktiven Routing-Regeln, die zur anfordernden Pipeline oder zum anfordernden Übernahmeprogramm gehören.
3. Wenn der Anwendungsmonitor eine aktive Routing-Regel für die anfordernde Pipeline oder das anfordernde Übernahmeprogramm findet, erstellt er ein UMF-Dokument, das die Routing-Anweisungen enthält, und sendet dieses UMF-Dokument an die anfordernde Pipeline oder das anfordernde Übernahmeprogramm zurück.
4. Die anfordernde Pipeline oder das anfordernde Übernahmeprogramm interpretiert die UMF-Dokumentennachricht und erstellt eine Routing-Datei mit der Dateierweiterung *.RTE (wobei * für den Namen der anfordernden Pipeline oder des anfordernden Übernahmeprogramms steht). Wenn die Pipeline bzw. das Übernahmeprogramm nach dem Start nicht mit dem Anwendungsmonitor kommunizieren kann, sucht sie bzw. es nach der Routing-Datei, um Anweisungen abzurufen.

5. Die anfordernde Pipeline oder das anfordernde Übernahmeprogramm öffnet die in der Routing-Regel konfigurierten Transportmethoden, die zum Kommunizieren mit dem Ziel erforderlich sind.
   - Wenn die Pipeline oder das Übernahmeprogramm die Transportmethode erfolgreich öffnen und das Ziel finden kann, leitet sie bzw. es die entsprechenden UMF-Dokumentnachrichten an das Ziel weiter, sofern es gestartet wurde und aktiv Daten verarbeitet.
   - Wenn die Pipeline oder das Übernahmeprogramm die Transportmethode nicht öffnen oder das Ziel nicht finden kann, wird die Pipeline bzw. das Übernahmeprogramm mit einem Fehler gestoppt.

Hilfethemen

Registerkarte 'Routing-Regeln'

Über diese Registerkarte können Sie vorhandene Routing-Regeln anzeigen oder löschen und neue Routing-Regeln für Pipelines konfigurieren, die auf der Registerkarte **Pipelines** registriert wurden. Eine Routing-Regel kann nach ihrer Konfiguration nicht mehr bearbeitet werden. Lediglich das Löschen der Regel ist möglich.

Ausgangspipeline
Zeigt den Namen der Pipeline an, für die eine Routing-Regel konfiguriert ist.

Reihenfolge
Zeigt die Reihenfolge an, in der diese Routing-Regel für die Pipeline verarbeitet wird, die in der Spalte **Ausgangspipeline** angegeben ist. Die Reihenfolge ist wichtig, wenn mehrere Routing-Regeln vorhanden sind; häufig wird die Reihenfolge auf 0 gesetzt.

Ziel Zeigt den Transport-URI der empfangenden Pipeline oder Datenbank bzw. des empfangenden externen Systems an.

Dokumenttyp
Zeigt den UMF-Dokumenttyp an, den diese Routing-Regel sendet. Dies ist der Dokumenttyp für die Ergebnisse, die von der in der Spalte **Ausgangspipeline** angegebenen Pipeline verarbeitet werden. Sie können einen bestimmten UMF-Dokumenttyp oder den Stern (*) auswählen. Der Stern gibt an, dass diese Routing-Regel alle UMF-Dokumenttypen weiterleitet.

Aktiviert
Gibt an, ob diese Routing-Regel aktiv ist:
- **Ja** gibt an, dass die Routing-Regel aktiviert ist. Immer wenn die Pipeline oder der Knoten, die oder der in der Spalte **Ausgangspipeline** angegeben ist, Ergebnisse für den angegebenen Dokumenttyp verarbeitet, leitet das System die diesem UMF-Dokumenttyp zugeordneten Daten an das Ziel weiter, das in der Spalte **Ziel** angegeben ist.
- **Nein** gibt an, dass die Routing-Regel nicht aktiviert ist.

Routing-Regeln - Registerkarte 'Details'

Über diese Registerkarte können Sie eine neue Routing-Regel konfigurieren oder die Details für eine vorhandene Routing-Regel anzeigen. Routing-Regeln werden normalerweise konfiguriert, um bestimmte Typen verarbeiteter Ergebnisse von einer Pipeline in einer anderen Datenbank oder in einem externen System zu veröffentlichen. Sie können Routing-Regeln nur für Pipelines konfigurieren, die auf der Registerkarte **Pipelines** registriert sind.

Alle Felder mit Ausnahme des Felds **Routenfilter** sind erforderlich, um eine neue Routing-Regel erfolgreich zu konfigurieren. Eine Routing-Regel kann nach ihrer Konfiguration nicht mehr bearbeitet werden. Zum Ändern einer Routing-Regel müssen Sie die Regel löschen und sie anschließend mit den korrigierten Informationen erneut hinzufügen.

Ausgangspipeline
Geben Sie den eindeutigen Namen der Pipeline ein, deren Ergebnisse Sie weiterleiten wollen. Der Name dieser Pipeline muss genau dem Namen entsprechen, der auf der Registerkarte **Pipelines** registriert ist, einschließlich Groß-/Kleinschreibung. Stimmt der Name nicht überein, zeigt das System eine Fehlernachricht an, aus der hervorgeht, dass die angegebene Pipeline nicht vorhanden ist.

Reihenfolge
Geben Sie eine Zahl zwischen 0 und 999 für die Reihenfolge an, in der das System diese Routing-Regel auf die registrierte Pipeline anwendet, die im Feld **Ausgangspipeline** angegeben ist. Der Standardwert für dieses Feld ist 0. Dieser Wert bewirkt, dass das System diese Routing-Regel zuerst verarbeitet. Sind für diese Pipeline bereits Routing-Regeln konfiguriert, geben Sie eine Zahl ein, die größer ist als der größte vorhandene Wert.

Prüfen Sie im linken Teilfenster die für diese Pipeline bereits konfigurierte Reihenfolge für vorhandene Routing-Regeln. Diese wird durch eine fortlaufende Zahl angegeben, die auf den Doppelpunkt hinter dem Pipelinenamen folgt. (PIPE08:0 beispielsweise gibt an, dass für die Pipeline PIPE08 bereits eine Routing-Regel konfiguriert ist, die zurzeit bei der Verarbeitung an erster Stelle steht. Wenn Sie eine neue Routing-Regel für PIPE08 konfiguriert haben, setzen Sie die Reihenfolge auf 1.)

Ziel Geben Sie den Transport-URI zu der Zielpipeline, der Zieldatenbank oder dem externen Zielsystem für die Weiterleitung der verarbeiteten Ergebnisse ein. Stellen Sie sicher, dass die Syntax für die verwendete Transportmethode korrekt ist.

Dropdown-Liste 'Dokumenttyp'
Wählen Sie in der Dropdown-Liste den UMF-Dokumenttyp aus, der von der registrierten Pipeline an das Ziel weitergeleitet werden soll. Wenn Sie alle verarbeiteten Ergebnisse an das Ziel weiterleiten wollen, wählen Sie den Stern (*) aus.

Routenfilter
Wenn Sie angeben wollen, dass nur bestimmte Informationen an das Ziel weitergeleitet werden sollen, geben Sie den Ausdruck ein, den das System verwenden soll, um die von dieser Routing-Regel weitergeleiteten UMF-Werte zu filtern. (Wenn Sie beispielsweise nur die Identitäts- oder Entitätsdatensätze aus einer bestimmten Datenquelle weiterleiten wollen, können Sie einen Filter wie DSRC_CODE=x eingeben. Dabei ist *x* der eindeutige Datenquellencode für die Datenquelle, die Sie herausfiltern wollen.)

Filter sind eine erweiterte Funktion der Routing-Regeln.

Dropdown-Liste 'Aktiviert'
Wählen Sie eine Option in der Dropdown-Liste aus:

- **Ja** bedeutet, dass der Anwendungsmonitor Informationen gemäß dieser Routing-Regel von der Pipeline an das Ziel weiterleitet.
- **Nein** bedeutet, dass der Anwendungsmonitor Informationen gemäß dieser Routing-Regel nicht von der Pipeline an das Ziel weiterleitet.

Löschen von Routing-Regeln

Eine Routing-Regel kann nach ihrer Konfiguration nicht mehr bearbeitet werden. Zum Korrigieren oder Aktualisieren der Informationen müssen Sie die vorhandene Routing-Regel löschen und eine neue Regel konfigurieren. Das Löschen einer Routing-Regel ist zudem sinnvoll, wenn sie nicht mehr benötigt oder verwendet wird. Sie können konfigurierte Routing-Regeln auf der Registerkarte **Routing-Regeln** in der Konfigurationskonsole löschen.

Vorgehensweise

1. Klicken Sie die Registerkarte **Konfiguration** an.
2. Klicken Sie die Registerkarte **Allgemein** an.
3. Klicken Sie die Registerkarte **Routing-Regeln** an.
4. Wählen Sie das Kontrollkästchen neben jeder konfigurierten Routing-Regel aus, die Sie löschen wollen.
5. Klicken Sie die Schaltfläche **Löschen** an.

Nächste Schritte

Das System löscht die ausgewählten Routing-Regeln und leitet keine Daten mehr anhand der gelöschten Routing-Regeln weiter.

Pipelinestatus und -statistikdaten

Die Überwachung des Status, der Statistikdaten und der Leistung ist für die fortlaufende Ausführung der Pipeline, das Ausgleichen von Pipelinedatenlasten und das Erkennen potenzieller Pipelineprobleme vor ihrem Auftreten wichtig.

Sie können den Status und die Statistikdaten zu einer Pipeline nur anzeigen, wenn die folgenden Bedingungen erfüllt sind:

1. Die Pipeline ist auf ihrem Pipelineknoten installiert und konfiguriert.

Anmerkung: (Nur für Windows-Plattformen) Wenn Sie die Pipeline als einen Service starten, können Sie in der Windows-Ereignisanzeige weitere Statusinformationen anzeigen, die Sie an keiner anderen Stelle anzeigen können.

Status- und Statistikinformationen

Nachdem eine Pipeline mit der Verarbeitung von Daten begonnen hat, können Sie in der Konfigurationskonsole UMF-Ausnahmebedingungsinformationen sehen.

- UMF-Ausnahmebedingungen auf der Registerkarte **UMF-Ausnahmebedingungen**

SNMP-Agenten

SNMP (Simple Network Management Protocol) ist ein Standardprotokoll, das für die Überwachung von Systemen und Netzeinheiten verwendet wird. SNMP-Agenten fordern periodisch den Status und Statistikdaten von jeder registrierten Pipeline im System an. Die vom SNMP-Agenten zusammengestellten Informationen zu jeder registrierten Pipeline werden auf der Registerkarte **Pipelinestatus** angezeigt.

Folgende Bedingungen müssen erfüllt sein, bevor SNMP-Agenten Pipelines überwachen können:

- Ein SNMP-Agent muss auf dem Pipelineknoten, der die zu überwachenden Pipelines ausführt, installiert und konfiguriert sein.
- Jede zu überwachende Pipeline muss in der Konfigurationskonsole registriert und für Überwachung konfiguriert sein.
- Der SNMP-Agent muss gestartet sein und auf dem Pipelineknoten ausgeführt werden. Dabei muss dieselbe Portnummer verwendet werden, die während der Pipeline-Installation konfiguriert wurde. Diese SNMP-Agentenportnummer gilt nicht pro Pipelineknoten, sondern systemweit. Die SNMP-Standardportnummer ist 13516. Sie können die Portnummer des SNMP-Agenten, die in der Datei server.xml auf jedem Pipelineknoten konfiguriert ist, jedoch suchen.

SNMP-Agenten sind Services und können nach Bedarf gestoppt und gestartet werden.

Beispiel für die Verwendung eines SNMP-Agenten

Das Unternehmen ABC überwacht alle Pipelines mit dem Anwendungsmonitor. Das Unternehmen hat einen weiteren Pipelineknoten (EAS-2) für drei neue Pipelines hinzugefügt: Pipeline300, Pipeline310 und Pipeline320. Zur Überwachung dieser Pipelines müssen Bediener des Unternehmens ABC die folgenden Tasks ausführen:

- Installieren und Konfigurieren eines SNMP-Agenten auf dem Pipelineknoten EAS-2.
- Registrieren jeder neuen Pipeline (Pipeline300, Pipeline310 und Pipeline320) auf der Registerkarte **Pipelines** in der Konfigurationskonsole.
- Starten des SNMP-Agenten auf dem Pipelineknoten EAS-2. Stellen Sie sicher, dass der SNMP-Agent die systemweite Portnummer verwendet, die bei der Installation der Pipelines auf diesem Pipelineknoten konfiguriert wurde.
- Starten jeder registrierten Pipeline für Verarbeitung. Stellen Sie sicher, dass Sie den für die Pipeline registrierten Namen exakt eingeben, da für registrierte Pipelinenamen die Groß-/Kleinschreibung beachtet werden muss.

Wenn die neuen Pipelines aktiv sind, können Bediener des Unternehmens ABC ihre Status und Statistikdaten über die Konfigurationskonsole überwachen.

Starten von SNMP-Agenten

Sie müssen einen SNMP-Agenten auf dem Pipelineknoten starten, auf dem die Pipelines ausgeführt werden, deren Status und Statistikdaten Sie in der Konfigurationskonsole überwachen wollen.

Vorbereitende Schritte

- Ein SNMP-Agent muss auf dem Pipelineknoten installiert und konfiguriert sein, auf dem die Pipelines ausgeführt werden.
- Pipelines müssen auf der Registerkarte **Pipelines** der Konfigurationskonsole registriert und für die Überwachung konfiguriert werden.

Vorgehensweise

1. Verwenden Sie in einer Befehlszeile auf dem Pipelineknoten den Befehl zum Wechseln des Verzeichnisses, um in das Ausgangsverzeichnis zu wechseln.
2. Geben Sie den folgenden Befehl ein: **`java -jar SNMPAgent`**-p *portnummer* Dabei ist *portnummer* die systemweite Portnummer, die während der Pipelineinstallation für SNMP-Agenten konfiguriert wurde. Der Standardwert für die Portnummer ist 13516.

Anmerkung: Sie finden die konfigurierte Portnummer des SNMP-Agenten in der Datei `server.xml` auf dem Pipelineknoten.

Ergebnisse

Der SNMP-Agent wird gestartet.

Nächste Schritte

Wählen Sie in der Konfigurationskonsole die Registerkarte **Pipelinestatus** aus, um zu überprüfen, ob der SNMP-Agent ausgeführt wird. Wenn der SNMP-Agent ausgeführt wird, meldet er den Status und die Statistikdaten zu allen Pipelines, die auf diesem Pipelineknoten ausgeführt werden. Sie müssen den SNMP-Agenten nicht erneut starten, wenn Sie weitere Pipelines hinzufügen, solange sich die SHM-Dateien in demselben Verzeichnis befinden. Dies ist in der Regel das Verzeichnis, in dem der SNMP-Agent gestartet wird.

Stoppen von SNMP-Agenten

Stoppen Sie einen SNMP-Agenten auf einem Pipelineknoten grundsätzlich, wenn Sie Änderungen auf dem Pipelineknoten, wie z. B. Konfigurationsaktualisierungen, vornehmen müssen.

Vorbereitende Schritte

Ein SNMP-Agent muss auf dem Pipelineknoten gerade ausgeführt werden. Es empfiehlt sich außerdem, alle Pipelines zu stoppen, die auf diesem Pipelineknoten ausgeführt und vom Anwendungsmonitor überwacht werden.

Vorgehensweise

Drücken Sie im Fenster, in dem der SNMP-Agent ausgeführt wird, die Tastenkombination **Strg** + **C**.

Nächste Schritte

- Der SNMP-Agent wird gestoppt.
- In der Konfigurationskonsole zeigt die Registerkarte **Pipelinestatus** einen Status `GESTOPPT` für alle Pipelines auf diesem Pipelineknoten an.

Überprüfen des Pipelinestatus in der Konfigurationskonsole

Es ist wichtig, den aktuellen Status von Pipelines zu überwachen, weil ein Teil des Systems nicht betriebsbereit ist, sobald eine Pipeline ausfällt. Auf der Registerkarte **Pipelinestatus** der Konfigurationskonsole sehen Sie auf einen Blick den aktuellen Pipelinestatus und die Leistungsstatistik. Der Anwendungsmonitor empfängt die Informationen von aktiven SNMP-Agenten, die alle 60 Sekunden abgefragt werden. Anschließend wird die Registerkarte **Pipelinestatus** aktualisiert.

Vorbereitende Schritte

- Auf dem Pipelineknoten, auf dem die zu überwachenden Pipelines ausgeführt werden, muss ein SNMP-Agent installiert und konfiguriert sein.
- Der SNMP-Agent muss gestartet sein und er muss die systemweite Portnummer verwenden, die während der Pipeline-Installation konfiguriert wurde. (Diese konfigurierte Portnummer können Sie der Datei server.xml entnehmen.)
- Die Pipeline muss auf der Registerkarte **Pipelines** der Konfigurationskonsole registriert und für die Überwachung konfiguriert sein.

- Der Pipelinename, den Sie zum Starten der Pipeline angeben, muss genau (einschließlich Groß-/Kleinschreibung) mit dem Pipelinenamen übereinstimmen, der auf der Registerkarte **Pipelines** registriert ist.

Informationen zu diesem Vorgang

Wenn der Status über die Konfigurationskonsole nicht angezeigt wird, können Sie den Pipelinestatus über die Befehlszeile überprüfen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Status** an.
2. Klicken Sie die Schaltfläche **Pipelinestatus** an.
3. Suchen Sie in der Spalte **Pipelinename** den Namen der Pipeline, die überprüft werden soll. (Die Pipelines sind in alphanumerischer Anordnung nach Name aufgeführt.) Prüfen Sie anschließend die Informationen zum Status und zur Transaktionsstatistik in der Zeile, die diesen Pipelinenamen enthält.

Nächste Schritte

Durch Anklicken der anderen Schaltflächen können Sie weitere Informationen zu dieser Pipeline anzeigen. Wenn Sie beispielsweise sehen wollen, wann die Pipeline zum letzten Mal gestartet wurde, klicken Sie die Registerkarte **Ereignisse** an.

Überprüfen des Pipelinestatus über die Befehlszeile

Es ist wichtig, den aktuellen Status von Pipelines zu überwachen, weil ein Teil des Systems nicht betriebsbereit ist, sobald eine Pipeline ausfällt. In den meisten Unternehmen werden die Pipelines über die Registerkarte **Pipelinestatus** in der Konfigurationskonsole überprüft. Auf dieser Registerkarte werden der aktuelle Pipelinestatus und Statistikdaten auf der Basis eines automatischen Systemsendeaufrufs angezeigt, der alle 60 Sekunden gesendet wird. Sie können den Status einer bestimmten Pipeline oder aller Pipelines auf einem bestimmten Pipelineknoten jedoch auch eine Befehlszeile überprüfen. (Bei Verwendung der Befehlszeile wird nur der Pipelinestatus, keine Leistungsstatistik für die Pipeline angezeigt.)

Vorbereitende Schritte

- Auf dem Pipelineknoten, auf dem die Pipeline ausgeführt wird, muss ein SNMP-Agent installiert und konfiguriert sein.
- Der SNMP-Agent muss gestartet sein und auf dem Pipelineknoten ausgeführt werden. Dabei muss dieselbe Portnummer verwendet werden, die während der Pipeline-Installation konfiguriert wurde. Diese SNMP-Agentenportnummer gilt nicht pro Pipelineknoten, sondern systemweit. Die SNMP-Standardportnummer ist 13516. Sie können die Portnummer des SNMP-Agenten, die in der Datei server.xml auf jedem Pipelineknoten konfiguriert ist, jedoch suchen.

Vorgehensweise

1. Führen Sie über eine Befehlszeile auf dem Pipelineknoten einen der folgenden Schritte durch:
   - Geben Sie den folgenden Befehl ein, um den Status aller Pipelines auf diesem Pipelineknoten zu überprüfen: **`pipeline -l`**
   - Geben Sie den folgenden Befehl ein, um den Status einer bestimmten Pipeline auf dem Pipelineknoten zu überprüfen: **`pipeline -n pipelinename -l`**

   Dabei ist *pipelinename* der eindeutige Name der Pipeline, die Sie überprüfen wollen.

Anmerkung: Der Name, den Sie eingeben, muss dem Namen entsprechen, den Sie zum Starten der Pipeline verwenden.

2. Drücken Sie die **Eingabetaste**.

Ergebnisse

Das System gibt einen der folgenden Status für jede Pipeline zurück:

- Aktiv für jede zurzeit aktive Pipeline.
- Gestoppt für jede zurzeit inaktive Pipeline.

Beispiel

Beispiel: Um den Status von pipeline08 zu überprüfen, geben Sie den folgenden Befehl ein: **`pipeline -n pipeline08 -l`**

Nächste Schritte

Wird der Status einer Pipeline unerwartet als Gestoppt angegeben, empfiehlt sich möglicherweise die Verwendung der Themen zur Fehlerbehebung, um die Ursache festzustellen.

Anzeigen von Anwendungsmonitorereignissen

Anwendungsmonitorereignisse treten jedes Mal auf, wenn zwischen dem Anwendungsmonitor und den auf der Registerkarte **Pipelines** der Konfigurationskonsole registrierten Pipelines eine Nachricht ausgetauscht wird. Diese Nachrichten umfassen eine Vielzahl von Informationen, wie das Starten und Stoppen einer Pipeline oder das Protokollieren von Fehlern und Warnungen durch das System. UMF-Ausnahmebedingungen (UMF - Universal Message Format) werden nicht berücksichtigt. Diese Informationen können Ihnen beim Beheben der Fehler helfen, die in einer bestimmten Pipeline auftreten.

Vorbereitende Schritte

- Die Pipeline muss auf der Registerkarte **Pipelines** der Konfigurationskonsole registriert werden.
- Die Pipeline muss auf dem Pipelineknoten, der auf der Registerkarte **Pipelines** registriert ist, mit demselben registrierten Pipelinenamen gestartet worden sein, der auf der Registerkarte **Pipelines** angezeigt wird.

Informationen zu diesem Vorgang

Wenn die Pipeline auf der Registerkarte **Pipelines** der Konfigurationskonsole registriert ist, können Sie aktuelle Ereignisse oder Langzeitereignisse auf der Registerkarte **Ereignisse** der Konfigurationskonsole anzeigen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Status** an.
2. Klicken Sie die Schaltfläche **Ereignisse** an.
3. Optional: Geben Sie in das Feld **Anfangsdatum** das Startdatum im Format mm/tt/jjjj ein, für das die Anwendungsmonitorereignisse angezeigt werden sollen. Wenn Sie dieses Feld leer lassen, zeigt das System alle Anwendungsmonitorereignisse, die die übrigen angegebenen Kriterien erfüllen, ab dem Datum

an, an dem das System in Betrieb genommen wurde. Wenn Sie in dieses Feld ein Datum eingeben, ist es nicht erforderlich, dass Sie in das Feld **Enddatum** ein Datum eingeben.

4. Optional: Geben Sie in das Feld **Enddatum** das Enddatum im Format mm/tt/jjjj ein, für das die Anwendungsmonitorereignisse angezeigt werden sollen. Wenn Sie dieses Feld leer lassen, zeigt das System alle Anwendungsmonitorereignisse, die die übrigen angegebenen Kriterien erfüllen, bis zum Datum des heutigen Tages an. Wenn Sie in dieses Feld ein Datum eingeben, ist es nicht erforderlich, dass Sie in das Feld **Anfangsdatum** ein Datum eingeben.
5. Optional: Geben Sie in das Feld **Ausgangspipeline** den registrierten Namen der Pipeline ein, für die die Anwendungsmonitorereignisse angezeigt werden sollen. Wenn Sie dieses Feld leer lassen, zeigt das System alle Anwendungsmonitorereignisse, die die übrigen angegebenen Kriterien erfüllen, für alle Pipelines nach registriertem Namen sortiert an.
6. Optional: Wählen Sie in der Dropdown-Liste **Max. Anzahl** die maximal anzuzeigende Anzahl von Anwendungsmonitorereignissen aus. Das System zeigt nur maximal diese Anzahl Anwendungsmonitorereignisse an, die alle übrigen angegebenen Kriterien erfüllen. Wenn die Ausnahmebedingungen die angegebene Anzahl übersteigen, zeigt das System sie nicht an. Ist die Zahl der Ausnahmebedingungen kleiner als die angegebene Anzahl, werden alle Anwendungsmonitorereignisse angezeigt, die alle weiteren angegebenen Kriterien erfüllen.
7. Erforderlich: Klicken Sie die Schaltfläche **Suchen** an.

Beispiel

Wenn Sie z. B. die letzten 500 Anwendungsmonitorereignisse anzeigen wollen, die am heutigen Tag für pipeline08 aufgetreten sind, würden Sie folgende Kriterien angeben:

- In das Feld **Anfangsdatum** geben Sie das Datum des heutigen Tages ein.
- In das Feld **Enddatum** geben Sie das Datum des heutigen Tages ein.
- In das Feld **Ausgangspipeline** geben Sie `pipeline08` ein.
- Wählen Sie **500** in der Dropdown-Liste **Max. Anzahl** aus.

Nächste Schritte

Sie können weitere Details zu einem Anwendungsmonitorereignis anzeigen, indem Sie das betreffende Ereignis anklicken. Die angezeigten Informationen entsprechen den Angaben, die beim Auftreten des Ereignisses zurückgemeldet wurden.

Anzeigen von UMF-Ausnahmebedingungen

UMF-Ausnahmebedingungen weisen auf Probleme bei der Verarbeitung von eingehenden Daten durch eine Pipeline hin. Diese Probleme treten auf, wenn die Struktur der eingehenden Daten nicht geparst werden kann. UMF-Ausnahmebedingungen werden in der Regel bei der maximalen Anzahl Pipelinefehler nicht berücksichtigt, d. h., das System protokolliert die UMF-Ausnahmebedingung und die Pipeline fährt normalerweise mit der Verarbeitung fort. Diese Informationen können Ihnen helfen, Fehler in eingehenden Daten für eine bestimmte Pipeline zu beheben.

Vorbereitende Schritte

- Die Pipeline muss auf der Registerkarte **Pipelines** der Konfigurationskonsole registriert werden.

- Die Pipeline muss auf dem Pipelineknoten, der auf der Registerkarte **Pipelines** registriert ist, mit dem registrierten Pipelinenamen gestartet worden sein, der auf der Registerkarte **Pipelines** angezeigt wird.

Informationen zu diesem Vorgang

Wenn die Pipeline auf der Registerkarte **Pipelines** der Konfigurationskonsole registriert ist, können Sie aktuelle UMF-Ausnahmebedindungen oder Langzeit-UMF-Ausnahmebedingungen auf der Registerkarte **UMF-Ausnahmebedingungen** der Konfigurationskonsole anzeigen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Status** an.
2. Klicken Sie die Schaltfläche **UMF-Ausnahmebedingungen** an.
3. Optional: Geben Sie in das Feld **Anfangsdatum** das Startdatum im Format mm/tt/jjjj ein, für das die UMF-Ausnahmebedingungen angezeigt werden sollen. Wenn Sie dieses Feld leer lassen, zeigt das System alle UMF-Ausnahmebedingungen, die die übrigen angegebenen Kriterien erfüllen, ab dem Datum an, an dem das System in Betrieb genommen wurde. Wenn Sie in dieses Feld ein Datum eingeben, ist es nicht erforderlich, dass Sie in das Feld **Enddatum** ein Datum eingeben.
4. Optional: Geben Sie in das Feld **Enddatum** das Enddatum im Format mm/tt/jjjj ein, für das die UMF-Ausnahmebedingungen angezeigt werden sollen. Wenn Sie dieses Feld leer lassen, zeigt das System alle UMF-Ausnahmebedingungen, die die anderen angegebenen Kriterien erfüllen, bis zum Datum des heutigen Tages an. Wenn Sie in dieses Feld ein Datum eingeben, ist es nicht erforderlich, dass Sie in das Feld **Anfangsdatum** ein Datum eingeben.
5. Optional: Geben Sie in das Feld **Ausgangspipeline** den registrierten Namen der Pipeline ein, für die die UMF-Ausnahmebedingungen angezeigt werden sollen. Wenn Sie dieses Feld leer lassen, zeigt das System alle UMF-Ausnahmebedingungen, die die anderen angegebenen Kriterien erfüllen, für alle Pipelines nach registriertem Namen sortiert an.
6. Optional: Wählen Sie in der Dropdown-Liste **Max. Anzahl** die maximal anzuzeigende Anzahl UMF-Ausnahmebedingungen aus. Das System zeigt nur maximal diese Anzahl UMF-Ausnahmebedingungen an, die alle übrigen angegebenen Kriterien erfüllen. Wenn die Ausnahmebedingungen die angegebene Anzahl übersteigen, zeigt das System sie nicht an. Ist die Zahl der Ausnahmebedingungen kleiner als die angegebene Anzahl, werden alle Anwendungsmonitorereignisse angezeigt, die alle weiteren angegebenen Kriterien erfüllen.
7. Erforderlich: Klicken Sie die Schaltfläche **Suchen** an.

Beispiel

Wenn Sie z. B. die letzten 50 UMF-Ausnahmebedingungen anzeigen wollen, die am heutigen Tag für pipeline08 aufgetreten sind, würden Sie folgende Kriterien angeben:

- In das Feld **Anfangsdatum** geben Sie das Datum des heutigen Tages ein.
- In das Feld **Enddatum** geben Sie das Datum des heutigen Tages ein.
- In das Feld **Ausgangsknoten** geben Sie `pipeline08` ein.
- Im Feld **Max. Anzahl** wählen Sie `50` aus.

Nächste Schritte

Sie können weitere Details zu einer UMF-Ausnahmebedingung anzeigen, indem Sie sie anklicken. Die angezeigten Informationen entsprechen den Angaben, die beim Auftreten der Ausnahmebedingung protokolliert wurden.

Anzeigen von neuen Identitäten

Die Registerkarte **Neue Identitäten** der Konfigurationskonsole zeigt die neuen Identitäten an, die von der Systempipeline innerhalb der letzten sieben Tage verarbeitet wurden. Sie können mit dieser Registerkarte die eingehenden Datenvolumina überprüfen und sicher sein, dass die Zahlen der Menge eingehender Daten bzw. der Anzahl aktiver Pipelines entsprechen. Sie können außerdem die Datenquellen stichprobenweise prüfen, die in die Pipeline geladen werden, um die Quellen anzuzeigen, die dem System Daten zuführen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Status** an.
2. Klicken Sie die Schaltfläche **Neue Identitäten** an.

Ergebnisse

Das System zeigt die Liste aller neuen Identitäten an, die innerhalb der letzten sieben Tage verarbeitet wurden.

Hilfethemen

Registerkarte 'Pipelinestatus'

Über diese Registerkarte können Sie den aktuellen Status sowie die Statistikdaten und Leistungsinformationen für registrierte Pipelines prüfen, die für die Überwachung durch den Anwendungsmonitor und den SNMP-Agenten konfiguriert sind. Einmal pro Minute ruft das System Status- und Statistikdaten vom SNMP-Agenten ab und aktualisiert die Registerkarte **Pipelinestatus**.

Anmerkung: Jeder SNMP-Agent, der auf den einzelnen Pipelineknoten ausgeführt wird, muss dieselbe systemweite Portnummer verwenden. Diese Portnummer wird beim Installieren von Pipelines auf einem Pipelineknoten konfiguriert. Der Standardwert für die Portnummer des SNMP-Agenten ist 13516; Sie können die konfigurierte SNMP-Portnummer jedoch der Datei server.xml entnehmen.

Gesamtanzahl Pipelines
Zeigt die Gesamtanzahl der Pipelines an, die in der Konfigurationskonsole für die Anwendungsüberwachung registriert sind. (Die Gesamtanzahl der Pipelines entspricht der Anzahl der aktiven Pipelines plus der Anzahl der veralteten Pipelines plus der Anzahl der inaktiven Pipelines.)

Aktive Pipelines
Zeigt die Gesamtanzahl der registrierten Pipelines an, die in der Konfigurationskonsole für die Überwachung konfiguriert und zurzeit aktiv sind.

Veraltete Pipelines
Zeigt die Gesamtanzahl der Pipelines an, deren Konfiguration nach dem Starten der Pipelines modifiziert wurde. Diese Pipelines müssen gestoppt und erneut gestartet werden, damit die neuen Konfigurationsänderungen in Kraft treten.

Inaktive Pipelines
Zeigt die Gesamtanzahl der registrierten Pipelines an, die in der Konfigu-

rationskonsole für die Überwachung konfiguriert sind, die jedoch zurzeit nicht aktiv sind oder keine Statistikdaten berichten. Dieser Wert berücksichtigt alle Pipelines, die zurzeit inaktiv sind. Ist ein Pipelineknoten nicht aktiv, werden also alle Pipelines, die auf diesem Server für die Überwachung konfiguriert sind, als inaktiv aufgeführt.

TPM Zeigt die durchschnittliche Gesamtanzahl der Transaktionen an, die pro Minute für alle aktiven Pipelines verarbeitet werden, die in der Konfigurationskonsole für die Überwachung konfiguriert sind. Diese Zahl gibt die Gesamtsystemleistung an; je höher die Zahl, desto besser die Leistung der aktiven Pipelines. Diese Zahl wird einmal pro Minute aktualisiert und auf der Basis der Informationen, die von den SNMP-Agenten empfangen werden, erneut berechnet. Ein SNMP-Agent ist auf jedem Pipelineknoten aktiv, auf dem aktive Pipelines ausgeführt werden. (Die TPM-Gesamtanzahl ergibt sich aus TPM für aktive Pipelines dividiert durch die Anzahl der aktiven Pipelines.)

TPS Zeigt die durchschnittliche Gesamtanzahl der Transaktionen an, die pro Sekunde für alle aktiven Knoten verarbeitet werden, die in der Konfigurationskonsole für die Überwachung konfiguriert sind. Diese Zahl gibt die Gesamtsystemleistung an; je höher die Zahl, desto besser die Leistung der aktiven Knoten. Diese Zahl wird einmal pro Minute aktualisiert und auf der Basis der Informationen, die von den SNMP-Agenten empfangen werden, erneut berechnet. Ein SNMP-Agent ist auf jedem Hostsystem aktiv, auf dem aktive Knoten ausgeführt werden. (Die TPS-Gesamtanzahl ergibt sich aus TPS für aktive Knoten dividiert durch die Anzahl der aktiven Knoten.)

Pipelinename
Listet die Namen aller Pipelines in alphanumerischer Anordnung auf, die in der Konfigurationskonsole für die Überwachung registriert sind.

Hostname
Zeigt den Namen des Pipelineknotens an, der für diese Pipeline registriert ist. Wird der Status dieser Pipeline unerwartet als `Inaktiv` angezeigt, unterstützt der Pipelineknotenname Sie bei der Fehlerbehebung. (Werden beispielsweise alle Pipelines auf einem bestimmten Pipelineknoten unerwartet als `Inaktiv` aufgelistet, sollten Sie bei diesem Pipelineknoten mit der Fehlerbehebung beginnen.)

Status Zeigt den letzten bekannten Status dieser Pipeline an: `Aktiv` (sie wird ausgeführt) oder `Inaktiv` (sie wird nicht ausgeführt.) Einmal pro Minute aktualisiert das System die Statusinformationen auf der Basis der Informationen, die von dem auf dem Pipelineknoten ausgeführten SNMP-Agenten empfangen werden.

TPM Zeigt die durchschnittliche Gesamtanzahl der Transaktionen an, die pro Minute für diese Pipeline verarbeitet werden. Wenn sich die Pipeline im Status `Inaktiv` befindet, zeigt das System `Nicht verfügbar` an. Diese Zahl gibt die Leistung der Pipeline an. Je größer die Zahl ist, desto besser ist die Leistung der Pipeline.

TPS Zeigt die Gesamtanzahl der Transaktionen an, die pro Sekunde für diese Pipeline verarbeitet wurden. Wenn sich die Pipeline im Status `Inaktiv` befindet, zeigt das System `Nicht verfügbar` an. Diese Zahl gibt die Leistung der Pipeline an. Je größer die Zahl ist, desto besser ist die Leistung der Pipeline.

Registerkarte 'UMF-Ausnahmebedingungen'

Über diese Registerkarte können Sie die UMF-Ausnahmebedingungen anzeigen, die beim Laden von Daten durch Pipelines protokolliert wurden, die für die Anwendungsüberwachung registriert sind. Zunächst generieren Sie auf dem Bildschirm einen Bericht zu UMF-Ausnahmebedingungen, die Sie anzeigen können. Anschließend können Sie eine bestimmte UMF-Ausnahmebedingung auswählen, um ihre Details aufzurufen. Diese Informationen können bei der Behebung von UMF-Ausnahmebedingungen in den Datendateien nützlich sein. Nachdem Sie einen dieser Fehler behoben haben, können Sie die korrigierten Datensätze in dieser Datei problemlos erneut verarbeiten.

UMF-Ausnahmebedingungen sind datengesteuerte Fehler. Sie treten auf, wenn in einer eingehenden Datenquellendatei, die von einer Pipeline verarbeitet wird, Probleme mit der UMF-Datenstruktur bestehen. Standardmäßig werden UMF-Ausnahmebedingungen bei der Fehlergrenze für die Pipeline (diese wird in der Konfigurationsdatei für die Pipeline festgelegt) nicht berücksichtigt. Daher wird die Pipeline in der Regel nicht auf Grund von UMF-Ausnahmebedingungen alleine beendet. Eine vollständige Liste von UMF-Ausnahmebedingungen finden Sie in der Tabelle UMF_EXCEPT oder im Protokoll *pipelinename*.msg. Dort finden Sie sogar UMF-Ausnahmebedingungen für Pipelines, die nicht für die Anwendungsüberwachung registriert sind.

Kriterien für den Bildschirmbericht

Verwenden Sie diese Felder, um die Kriterien für den auf dem Bildschirm angezeigten Bericht zu UMF-Ausnahmebedingungen anzugeben. Nach Angabe der Kriterien klicken Sie die Schaltfläche **Suchen** an, um den Bericht zu generieren.

Anfangsdatum

Das Anfangsdatum für den Bericht zu UMF-Ausnahmebedingungen, die den übrigen angegebenen Kriterien entsprechen. (Dieses Feld ist optional und kann leer sein. Wird das Feld leer gelassen, werden UMF-Ausnahmebedingungen, die den übrigen angegebenen Kriterien entsprechen, beginnend mit dem Tag angezeigt, an dem das System in Betrieb genommen wurde.)

In diesem Feld wird das heutige Datum als Standardwert angezeigt. Geben Sie das Datum im Format `mm/tt/jjjj` ein.

Enddatum

Das Enddatum für den Bericht zu UMF-Ausnahmebedingungen, die den übrigen angegebenen Kriterien entsprechen. (Dieses Feld ist optional und kann leer sein. Wird das Feld leer gelassen, werden UMF-Ausnahmebedingungen, die den übrigen angegebenen Kriterien entsprechen, bis zum heutigen Tag angezeigt.)

In diesem Feld wird das heutige Datum als Standardwert angezeigt. Geben Sie das Datum im Format `mm/tt/jjjj` ein.

Ausgangsknoten

Der Name der registrierten Pipeline, für die UMF-Ausnahmebedingungen angezeigt werden sollen. (Dieses Feld ist optional und kann leer sein. Wird das Feld leer gelassen, werden UMF-Ausnahmebedingungen, die den übrigen angegebenen Kriterien entsprechen, für alle registrierten Pipelines angezeigt.)

Beachten Sie, dass auf dieser Registerkarte nur UMF-Ausnahmebedingungen für Pipelines angezeigt werden, die für die Anwendungsüberwachung registriert sind. Wenn Sie alle UMF-Ausnahme-

bedingungen anzeigen wollen, verwenden Sie die Tabelle UMF_EXCEPT oder das Protokoll *pipelinename*.msg.

Datenquellencode
Der Datenquellencode (genaue Übereinstimmung), für den UMF-Ausnahmebedingungen angezeigt werden sollen. (Dieses Feld ist optional und kann leer sein. Wird das Feld leer gelassen, werden UMF-Ausnahmebedingungen, die den übrigen angegebenen Kriterien entsprechen, für alle Datenquellen angezeigt.)

Max. Anzahl
Diese Dropdown-Liste enthält Optionen für die maximal anzuzeigende Anzahl von UMF-Ausnahmebedingungen, die den übrigen angegebenen Kriterien entsprechen. Es werden höchstens so viele UMF-Ausnahmebedingungen angezeigt, wie über die maximale Anzahl angegeben ist. Sind weitere UMF-Ausnahmebedingungen vorhanden, die den Kriterien entsprechen, werden diese nicht angezeigt.

Schaltfläche 'Suchen'
Nach Anklicken dieser Schaltfläche wird die Suche ausgeführt. Das System sucht alle Datensätze, die den angegebenen Kriterien entsprechen, und zeigt sie an.

Bildschirmanzeige der Berichtsergebnisse
In diesem Teil des Fensters wird der Bericht zu den UMF-Ausnahmebedingungen auf der Basis der von Ihnen eingegebenen Kriterien angezeigt. Die Liste ist nach der UMF-ID sortiert.

UMF-ID
Zeigt die fortlaufende Zahl an, die das System dieser UMF-Ausnahmebedingung zugeordnet hat. Die UMF-ID ermöglicht eine direkte Zuordnung zur Tabelle UMF_EXCEPT, in der UMF-Ausnahmebedingungen protokolliert werden.

Ausgangspipeline
Zeigt den Namen der Pipeline an, die den Datensatz verarbeitet hat, als die UMF-Ausnahmebedingung aufgetreten ist.

Erstellungsdatum
Zeigt das Datum an, an dem die UMF-Ausnahmebedingung aufgetreten ist.

Ausgabedokument
Zeigt den Typ des UMF-Ausgabedokuments an, das dieser UMF-Ausnahmebedingungen zugeordnet ist.

Datenquellencode
Zeigt den Datenquellencode an, der der eingehenden Datendatei zugeordnet ist, bei der die UMF-Ausnahmebedingung aufgetreten ist.

Externe Referenz
Zeigt die externe Referenz für den Datensatz an, bei dem die UMF-Ausnahmebedingung aufgetreten ist. Mit dieser Information kann der genaue Datensatz in der Datendatei ermittelt werden, der korrigiert werden muss.

Aktion
Zeigt die Aktion an, die dem eingehenden Datensatz zugeordnet

ist, bei dem die UMF-Ausnahmebedingung aufgetreten ist. (Diese Aktion ist in UMF für den Datensatz codiert.)

- A: Hinzufügen (Add)
- C: Ändern (Change)
- D: Löschen (Delete)

Registerkarte 'Ereignisse'

Über diese Registerkarte können Sie die Nachrichten anzeigen, die zwischen dem Anwendungsmonitor und den für die Überwachung oder das Routing registrierten Pipelines ausgetauscht wurden. In der Regel werden diese Nachrichten auch in den Systemprotokolldateien aufgezeichnet, wenn die Protokollierung auf Ihrem System entsprechend konfiguriert ist. Zunächst generieren Sie auf dem Bildschirm einen Bericht zu Anwendungsmonitorereignissen, die Sie anzeigen können. Anschließend wählen Sie ein bestimmtes Ereignis aus, um seine Details aufzurufen. Dabei kann es sich um Informationsnachrichten handeln oder um Nachrichten, die Ihnen bei der Behebung von Problemen oder Warnungen zu Pipelines helfen können.

Anwendungsmonitorereignisse umfassen normalerweise Nachrichten oder Fehler, die während der Pipelineverarbeitung ausgegeben werden, z. B. Start oder Stopp der Pipeline, oder Warnungen bzw. Fehler, die bei der Pipelineverarbeitung generiert wurden. Der einzige Fehler- und Warnungstyp, der auf dieser Registerkarte nicht enthalten ist, sind UMF-Ausnahmebedingungen. Diese Ausnahmebedingungen sind datengesteuerte Ausnahmebedingungen, keine Informationen oder Fehler in Bezug auf die Verarbeitung.

Kriterien für den Bildschirmbericht

Verwenden Sie diese Felder, um die Kriterien für den auf dem Bildschirm angezeigten Bericht zu Anwendungsmonitorereignissen anzugeben. Nach Angabe der Kriterien klicken Sie die Schaltfläche **Suchen** an, um den Bericht zu generieren. Standardmäßig werden auf dieser Registerkarte Anwendungsmonitorereignisse angezeigt, die heute für Pipelines aufgetreten sind, die für die Anwendungsüberwachung registriert sind.

Anfangsdatum

Das Anfangsdatum für den Bericht zu Anwendungsmonitorereignissen, die den übrigen angegebenen Kriterien entsprechen. (Dieses Feld ist optional und kann leer sein. Wird das Feld leer gelassen, werden Anwendungsmonitorereignisse, die den übrigen angegebenen Kriterien entsprechen, beginnend mit dem Tag angezeigt, an dem das System in Betrieb genommen wurde.)

Enddatum

Das Enddatum für den Bericht zu Anwendungsmonitorereignissen, die den übrigen angegebenen Kriterien entsprechen. (Dieses Feld ist optional und kann leer sein. Wird das Feld leer gelassen, werden Anwendungsmonitorereignisse, die den übrigen angegebenen Kriterien entsprechen, bis zum heutigen Tag angezeigt.)

Ausgangspipeline

Der Name der registrierten Pipeline, für die Anwendungsmonitorereignisse angezeigt werden sollen. (Dieses Feld ist optional und kann leer sein. Wird das Feld leer gelassen, werden Anwendungsmonitorereignisse, die den übrigen angegebenen Kriterien entsprechen, für alle registrierten Pipelines angezeigt.)

Beachten Sie, dass auf dieser Registerkarte nur Anwendungsmonitorereignisse für Pipelines angezeigt werden, die für die Anwendungsüberwachung registriert sind.

Max. Anzahl
Diese Dropdown-Liste enthält Optionen für die maximal anzuzeigende Anzahl von Anwendungsmonitorereignissen, die den übrigen angegebenen Kriterien entsprechen. Es werden höchstens so viele Anwendungsereignisse angezeigt, wie über die maximale Anzahl angegeben ist. Sind weitere Anwendungsereignisse vorhanden, die den Kriterien entsprechen, werden diese nicht angezeigt.

Schaltfläche 'Suchen'
Nach Anklicken dieser Schaltfläche wird die Suche ausgeführt. Das System sucht alle Datensätze zur Anwendungsereignisüberwachung, die den angegebenen Kriterien entsprechen, und zeigt sie an.

Bildschirmanzeige der Berichtsergebnisse
In diesem Teil des Fensters wird der Bericht zu den Anwendungsmonitorereignissen auf der Basis der von Ihnen eingegebenen Kriterien angezeigt. Die Liste ist nach der ID-Nummer sortiert.

ID Zeigt die fortlaufende Zahl an, die das System diesem Anwendungsmonitorereignis zugeordnet hat.

Ausgangspipeline
Zeigt die registrierte Pipeline an, die von dem Anwendungsmonitorereignis betroffen ist bzw. mit diesem Anwendungsmonitorereignis in Zusammenhang steht. Bei dieser Pipeline müssen Sie möglicherweise eine Fehlerbehebung ausführen.

Datum/Zeit
Zeigt das Datum und die Zeit für das Auftreten des Anwendungsmonitorereignisses an.

Ereignis
Zeigt den Typ des aufgetretenen Anwendungsmonitorereignisses an. Die Spalten **Ereignisbeschreibung** und **Fehlerkategorie** enthalten weitere Informationen zu diesem Ereignis und geben die Wertigkeit des Ereignistyps an. Zurzeit sind zwei Typen von Anwendungsmonitorereignissen verfügbar:

- `NODE-INFO` ist eine Anmerkung oder ein anderer Typ von Informationsereignis, das in der betroffenen Pipeline aufgetreten ist. Dieser Ereignistyp wird in der Regel angezeigt, wenn die betroffene Pipeline gestartet oder gestoppt wird.
- `NODE-ERROR` ist ein Fehler, der in der betroffenen Pipeline aufgetreten ist. Prüfen Sie die Spalte **Fehlerkategorie**, um festzustellen, ob eine sofortige Aktion erforderlich ist. Normalerweise empfiehlt sich ein genauerer Blick auf die Informationen zu diesem Anwendungsmonitorereignis; sie können Ihnen möglicherweise bei der Behebung eines Problems mit dieser Pipeline helfen.

Ereignisbeschreibung
Stellt bis zu 30 Zeichen weiterer Informationen zu dem Anwendungsmonitorereignis zur Verfügung.

Fehlerkategorie

Zeigt den Typ der Fehlerkategorie für das Anwendungsmonitorereignis an. Zurzeit sind zwei Typen von Ereignissen verfügbar:

- `NOTE` ist die Fehlerkategorie, die dem Ereignis `NODE-INFO` zugeordnet ist. In der Regel handelt es sich bei diesem Fehlerkategorietyp um eine Informationsnachricht, sodass im Allgemeinen keine Benutzeraktion erforderlich ist.
- `ERR` ist die Fehlerkategorie, die dem Ereignis `NODE-ERROR` zugeordnet ist. Dieser Typ der Fehlerkategorie weist normalerweise darauf hin, dass sich ein genauerer Blick auf die Details zu diesem Anwendungsmonitorereignis empfiehlt, um den Fehler zu beheben. Sie können die vollständigen Details des Ereignisses anzeigen, indem Sie das Ereignis anklicken.

Ereignisse - Registerkarte 'Details'

Wenn Sie ein bestimmtes Anwendungsmonitorereignis auf der Registerkarte **Ereignisse** auswählen, werden in einer neuen Anzeige die Details zu dem ausgewählten Ereignis angezeigt. Diese Details stammen direkt aus den Systemprotokolldateien, mit Ausnahme der Protokolldatei für UMF-Ausnahmebedingungen. (Diese Protokolldatei können Sie über eine eigene Registerkarte, die Registerkarte **UMF-Ausnahmebedingungen**, anzeigen.) Die hier angezeigten Details helfen Ihnen möglicherweise bei der Behebung eines Pipelinefehlers.

ID Die fortlaufende Zahl, die diesem Anwendungsmonitorereignis vom System zugeordnet wird.

Pipeline

Listet den Namen der Pipeline auf, bei der dieses Anwendungsmonitorereignis aufgetreten ist.

Datum/Zeit

Zeigt das Datum und die Zeit dieses CME-Ereignisses im Format `Monat, TT, JJJJ HH:MM:SS AM/PM Zeitzone` an. Dieses Datum/diese Zeit entspricht dem Datum/der Zeit der Aufzeichnung des Ereignisses in der Protokolldatei.

Ereignis

Zeigt den Typ des Anwendungsmonitorereignisses an:

- `NODE-INFO` ist eine Anmerkung oder ein anderer Typ von Informationsereignis, das in der betroffenen Pipeline aufgetreten ist. Dieser Ereignistyp wird in der Regel angezeigt, wenn die betroffene Pipeline gestartet oder gestoppt wird.
- `NODE-ERROR` ist ein Fehler, der in der betroffenen Pipeline aufgetreten ist. Prüfen Sie die Spalte **Fehlerkategorie**, um festzustellen, ob eine sofortige Aktion erforderlich ist. Normalerweise empfiehlt sich ein genauerer Blick auf die Informationen zu diesem Ereignis; sie können Ihnen möglicherweise bei der Behebung eines Problems mit dieser Pipeline helfen.

Ereignisbeschreibung

Zeigt die ersten Zeichen des Anwendungsmonitorereignisses so wie in der Protokolldatei aufgezeichnet an. Diese Beschreibung soll genauere Informationen zum Auslöser des Ereignistyps bereitstellen.

Fehlerkategorie

Zeigt den Typ der Fehlerkategorie des Anwendungsmonitorereignisses an:

- NOTE ist die Fehlerkategorie, die dem Ereignis NODE-INFO zugeordnet ist. In der Regel handelt es sich bei diesem Fehlerkategorietyp um eine Informationsnachricht, sodass im Allgemeinen keine Benutzeraktion erforderlich ist.
- ERR ist die Fehlerkategorie, die dem Ereignis NODE-ERROR zugeordnet ist. Dieser Typ der Fehlerkategorie weist normalerweise darauf hin, dass sich ein genauerer Blick auf die Details zu diesem Ereignis empfiehlt, um den Fehler zu beheben. Sie können die vollständigen Details des Ereignisses anzeigen, indem Sie das Ereignis anklicken.

Registerkarte 'Neue Benutzerkonten'

Über diese Registerkarte können Sie die Datenladevorgänge der letzten sieben Tage prüfen. Auf einen Blick können Sie feststellen, aus welchen Datenquellen Dateien zur Verarbeitung angekommen sind und wie viele neue Identitäten das Ergebnis dieser Verarbeitung sind. Auf der Basis dieser Statistikdaten können Sie das Verarbeitungsvolumen abschätzen und schnell feststellen, ob die eingehenden Datenvolumen den Erwartungen entsprechen.

Nach Anklicken dieser Registerkarte werden die Daten der letzten sieben Tage angezeigt. Sind mehr Datensätze verfügbar als auf der Seite angezeigt werden, verwenden Sie die Bildlaufleiste, um die übrigen Datensätze anzuzeigen. Die Registerkarte **Neue Benutzerkonten** ist in alphanumerischer Anordnung nach Datenquellencode sortiert.

Datenquellencode
Zeigt den Datenquellencode an, der diesem neuen Identitätsdatensatz zugeordnet ist. Diese Informationen basieren auf dem UMF-Tag (Universal Message Format) für den Datenquellencode, der in der eingehenden Datei enthalten war, die verarbeitet wurde.

Anmerkung: Sie können eine vollständige Liste aller Datenquellencodes in der Konfigurationskonsole anzeigen, indem Sie die Registerkarte **Konfiguration** und anschließend die Registerkarte **Quellen** anklicken.

Beschreibung
Zeigt die Datenquellenbeschreibung an, wie sie in der Konfigurationskonsole für diese Datenquelle definiert wurde. Die Beschreibung stellt normalerweise weitere Informationen zur Verfügung, mit deren Hilfe Sie die Datenquelle identifizieren können, aus der diese Identitätsdatensätze stammen.

Ladedatum
Zeigt das Datum an, an dem diese Datenquellendatei verarbeitet wurde und an dem sie die Anzahl der neuen Identitäten beigetragen hat, die in der Spalte **Datensatzanzahl** angegeben ist. Das Datum wird im Format Monat TT, JJJJ dargestellt.

Datensatzanzahl
Zeigt die Gesamtzahl neuer Identitäten an, die an dem in der Spalte **Ladedatum** angegebenen Datum von diesem Datenquellencode verarbeitet wurden. Diese Zahl kann einen Hinweis auf das Verarbeitungsvolumen geben.

Kapitel 7. Laden von Daten

Sie müssen Daten in das UMF-Format (Universal Message Format) konvertieren und in das System laden, um IBM InfoSphere Identity Insight verwenden zu können.

Hinzufügen einer neuen Datenquelle

Sie müssen eine neue Datenquelle hinzufügen, wenn Sie über eine neue Quelle von Daten für die Entitätendatenbank verfügen.

Informationen zu diesem Vorgang

Alle Ergebnisse sind von der Qualität der Daten abhängig. Daher ist der Import qualitativ hochwertiger Daten in die Entitätendatenbank eine der wichtigsten Aufgaben überhaupt. Diese Aufgabe setzt jedoch eine sorgfältige Analyse der Daten und der Konfiguration voraus.

Vorgehensweise

1. Identifizieren Sie die Quelle der Daten. Es ist wichtig zu wissen, wo die Datenprobleme zu beheben sind.
2. Analysieren Sie die Metadaten. Jede in der Entitätendatenbank konfigurierte Datenquelle muss über eindeutige Kennungen für ihre Datensätze verfügen, damit die Entitätendatenbank alle Daten vollständig zu ihrer ursprünglichen Quelle zurückverfolgen kann. Suchen Sie nach dem Feld, das die Eindeutigkeit des Datensatzes gewährleistet, und stellen Sie sicher, dass es tatsächlich eindeutig ist.
3. Verwenden Sie ein Übernahmeprogramm, um die Daten aus dem nativen Format in UMF umzusetzen.
4. Konfigurieren Sie die Daten.
   a. Definieren Sie eine Rolle für die Datenquelle.
   b. Konfigurieren Sie die Datenquelle.
   c. Erstellen Sie die erforderlichen Nummerntypen.
   d. Erstellen Sie die erforderlichen Merkmaltypen.
   e. Prüfen Sie die Auflösungskonfiguration und passen Sie sie ggf. an.
   f. Konfigurieren Sie neue DQM-Regeln.
   g. Validieren Sie die neuen DQM-Regeln.
   h. Konfigurieren Sie die Rollenalertregeln.
5. Überprüfen Sie die Daten.
   a. Überprüfen Sie, ob die Pipeline gestartet wurde.
   b. Überprüfen Sie, ob die Pipeline die konfigurierten Transportmethoden verwenden konnte und ob sie Daten im UMF-Format vom Übernahmeprogramm empfangen hat.
   c. Überprüfen Sie die `.bad`-Datei, um festzustellen, ob der Übernahmeknoten korrekt formatierte XML-Nachrichten generiert hat.
   d. Überprüfen Sie, ob als Ergebnis ungültiger Zuordnungen oder Konfigurationen UMF-Ausnahmebedingungen aufgetreten sind.

e. Überprüfen Sie, ob die Ergebnisse den Erwartungen entsprechen, indem Sie die Ergebnisberichte zu Datenquellen und Ladevorgängen anzeigen.
f. Suchen Sie in Visualizer nach mindestens einer aufgelösten Entität.
g. Analysieren Sie Rollenalerts, falls vorhanden.

Konvertieren von Daten in UMF

Das System kann eingehende Daten nur verarbeiten, wenn sie in UMF (Universal Message Format) konvertiert werden. Die Konvertierung eingehender Daten in UMF kann durch eine Vielzahl von Tools wie die mit dem Produkt ausgelieferten Basisdienstprogramme oder Standard-XML-Umsetzungsprodukte erzielt werden.

Vorgehensweise

1. Analysieren Sie Ihre eingehenden Daten mit dem Entitätsmodell, das Sie für das System erstellt haben, um zu überprüfen, inwieweit sie dem UMF-Standard entsprechen. Sie müssen eine konkrete Vorstellung der vorhandenen UMF-Segmente und -Tags haben, bevor Sie mit dem nächsten Schritt fortfahren.
2. Konfigurieren Sie Ihr Konvertierungsdienstprogramm so, dass es UMF-Datensätze erstellt, die mit Ihrem Entitätsmodell übereinstimmen.
3. Führen Sie das Konvertierungsdienstprogramm aus.

Nächste Schritte

Nach der Konvertierung Ihrer Daten in UMF können Sie die UMF-Datensätze zur Verarbeitung an die Pipeline senden.

Übernahmeprogramme

Ein Übernahmeprogramm enthält die Tools und Programme, die Daten übernehmen, sie in UMF (Universal Message Format) umsetzen und die umgesetzten Daten anschließend zur Verarbeitung an die Pipeline übergeben.

Sie können die mit dem Produkt ausgelieferten Übernahmedienstprogramme verwenden, um Daten in UMF umzusetzen, oder Sie können ETL-Tools (ETL - Extrahieren, Transformieren und Laden) wie WebSphere QualityStage als Ihre Übernahmeprogramme verwenden.

Übertragen von UMF-Dateien in eine Warteschlange

Sie können UMF-Dateien mit dem Warteschlangendienstprogramm in eine Warteschlange übertragen.

Vorgehensweise

1. Stellen Sie sicher, dass die Daten, die Sie senden wollen, in Breitformat (ein Datensatz pro Zeile) vorliegen.
2. Geben Sie Konfigurationseinstellungen in der Konfigurationsdatei an.
3. Führen Sie das Warteschlangendienstprogramm aus.

Warteschlangendienstprogramm

IBM stellt ein Warteschlangendienstprogramm bereit, das die Übertragung von UMF-Daten von einem Prozess oder einer Datei an eine Warteschlange verwaltet.

Seine Hauptaufgabe besteht zwar darin, Daten in mindestens eine Warteschlange zu versetzen. Sie können das Warteschlangendienstprogram jedoch auch für andere Aufgaben verwenden:

- Erstellen von Warteschlangen
- Entfernen von Datensätzen aus einer Warteschlange
- Anzeigen des Warteschlangenstatus
- Anzeigen der Datensätze in einer Warteschlange

Das Warteschlangendienstprogramm erwartet die Daten in einem bestimmten Format:

- Breitformat-UMF, d. h. eine Zeile pro Datensatz
- Ein Zeilenumbruch am Ende jedes Datensatzes
- Keine weiteren Zeilenumbrüche innerhalb eines Datensatzes

Für das Warteschlangendienstprogramm müssen Sie einen der folgenden Warteschlangenmanager verwenden.

Microsoft Windows Server x86
: Microsoft Message Queuing, eine Komponente von Microsoft Windows Server 2003 oder 2008.

  IBM Websphere MQ 6.0

Microsoft Windows Server x86_64
: Microsoft Message Queuing, eine Komponente von Microsoft Windows Server 2003 oder 2008.

  IBM Websphere MQ 7.0

Solaris-Betriebsumgebung
: IBM Websphere MQ 6.0

Linux IBM Websphere MQ 6.0

AIX IBM Websphere MQ 6.0

Wird eine Pipeline im Warteschlangenmodus ausgeführt, ist der Warteschlangenmanager grundsätzlich erforderlich und muss installiert und aktiv sein. Wird eine Pipeline im Dateimodus ausgeführt, muss der Warteschlangenmanager auf Windows- und AIX-Plattformen installiert sein, er muss jedoch nicht aktiv sein. Auf Solaris- oder Linux-Plattformen muss er weder installiert noch aktiv sein.

Konfigurationsdatei für das Warteschlangendienstprogramm

Mit einer Konfigurationsdatei können Sie über das Warteschlangendienstprogramm Datensätze an mehrere Warteschlangen senden.

Wenn Sie eine Datengruppe an mehrere Warteschlangen senden, müssen Sie den Warteschlangenmanager anweisen, wie die Verteilung erfolgen soll. Die Grundidee ist die Erstellung eines Verteilungstyps, bei dem die erste Warteschlange einen Datensatz erhält, dann erhält die nächste einen und so weiter.

Die Konfigurationsdatei des Warteschlangendienstprogramms heißt qutil.ini und muss sich im selben Verzeichnis befinden wie die ausführbare Datei des Warteschlangendienstprogramms.

Parameter

[abschnittsname]

Name des Abschnitts. Sie können mehrere Gruppen von Konfigurationseinstellungen in einer einzelnen Konfigurationsdatei angeben und dann in der Befehlszeile auf diese Einstellungen verweisen, indem Sie den entsprechenden Abschnittsnamen angeben. Sie können z. B. die Abschnitte CFG1 (Konfiguration 1) und CFG2 (Konfiguration 2) benennen und beim Absetzen von Befehlen für das Warteschlangendienstprogramm auf diese Abschnitte verweisen.

MessageCountMax

Maximale Anzahl Datensätze, die zu jedem beliebigen Zeitpunkt in jeder Warteschlange zulässig ist. Ist die Warteschlange voll, hört das Dienstprogramm mit der Verarbeitung von Datensätzen auf.

FullCountMax

Gibt die Gesamtzahl Datensätze an, die in allen Warteschlangen enthalten sein dürfen (im Gegensatz zu den Datensätzen in einer einzelnen Warteschlange). Wenn alle Warteschlangen voll sind, hält das Dienstprogramm den Datenfluss an und wartet darauf, dass Datensätze zum Verarbeiten in Pipelines übernommen werden, sodass in den Warteschlangen wieder Platz frei wird. Arbeitet mit `FullPause` zusammen.

FullPause

Die Anzahl Millisekunden, während derer das Warteschlangendienstprogramm bei Erreichen von `FullCountMax` den Datenfluss anhält, damit die Daten in den Warteschlangen verarbeitet werden können.

Qout*n*=wsname

Die Namen der Ausgabewarteschlangen für diesen Abschnitt. Die Namen der Ausgabewarteschlangen können beliebig gewählt werden, der Parameter muss jedoch Qout*n* lauten, wobei n eine ganze Zahl ist, die bei 0 beginnt. Der Wert von *n* muss von 0 bis *n* fortlaufend sein, wobei n die letzte definierte Warteschlange ist. Dieses Format ist erforderlich. Ändern Sie nur die Zahl der Qout*n*-Kennung und die Warteschlangennamen.

Beispiel

Im folgenden Beispiel werden zwei Gruppen mit Anweisungen dargestellt (eine verwendet 2 Warteschlangen, die andere verwendet 4 Warteschlangen). Zu jedem beliebigen Zeitpunkt dürfen maximal 2.500 Datensätze in jeder einzelnen Warteschlange enthalten sein, in allen Warteschlangen dürfen höchstens 10.000 Datensätze sein. Wenn FullCountMax erreicht wird, hält das Warteschlangendienstprogramm 3 Sekunden an, bevor es versucht, weitere Datensätze in eine der Warteschlangen zu laden. Anschließend werden die Namen der 4 Warteschlangen aufgelistet, die verwendet werden sollen.

```
[CFG1]
MessageCountMax=2500
FullCountMax=10000
FullPause=3000
Qout0=wsnameA
Qout1=wsnameB
[CFG2]
MessageCountMax=2500
FullCountMax=10000
FullPause=3000
```

```
Qout0=wsnameA
Qout1=wsnameB
Qout2=wsnameC
Qout3=wsnameD
```

Befehlssyntax des Warteschlangendienstprogramms

Befehle des Warteschlangendienstprogramms bestehen aus Operationen und Modifikatoren.

Die Basissyntax eines Befehls des Warteschlangendienstprogramms lautet wie folgt:

qutil -operation *wsname* **-modifikator**

wsname ist der Name der Warteschlange.

Befehlsoperationen

Operationen definieren die verschiedenen Funktionen des Warteschlangendienstprogramms. Sie können einem Qutil-Befehl nur eine Operation hinzufügen.

-C Erstellt eine neue Warteschlange.

Für **wsname** ist ein eindeutiger Name erforderlich.

Muss der Großbuchstabe C sein.

-f Kopiert die Standardeingabe in die Warteschlange.

Ein Warteschlangenname (wsname) ist erforderlich.

-i Kopiert die Standardeingabe in mehrere Warteschlangen.

Der in der Datei qutil.ini definierte Abschnittsname ist erforderlich. Gibt einen Abschnitt aus qutil.ini zum Laden an, um Nachrichten an mehrere Warteschlangen zu senden.

-k Anzahl der aus der Warteschlange zu löschenden Datensätze.

Ein Warteschlangenname (*wsname*) ist erforderlich.

Kann mit dem Modifikator -c kombiniert werden, um die Anzahl der verarbeiteten Datensätze zu begrenzen.

-p Anzahl der in der Warteschlange anzuzeigenden Datensätze.

Entfernt keine Datensätze aus der Warteschlange.

Ein Warteschlangenname (*wsname*) ist erforderlich.

Schreibt in die Standardausgabe.

Kann mit dem Modifikator -c kombiniert werden, um die Anzahl der verarbeiteten Datensätze zu begrenzen.

-r Anzahl der in der Warteschlange zu lesenden Datensätze.

Entfernt Datensätze aus der Warteschlange.

Ein Warteschlangenname (*wsname*) ist erforderlich.

Schreibt in die Standardausgabe.

Kann mit dem Modifikator -c kombiniert werden, um die Anzahl der verarbeiteten Datensätze zu begrenzen.

-s Warteschlangenstatus.

Ein Warteschlangenname (*wsname*) ist erforderlich.

-x *wsname* löschen.

Ein Warteschlangenname (*wsname*) ist erforderlich.

Befehlsmodifikatoren

Modifikatoren konfigurieren zusätzliche Parameter für eine Operation des Warteschlangendienstprogramms. Sie können mehrere Modifikatoren pro Qutil-Befehl verwenden.

-T Gibt an, ob eine Warteschlange transaktionsorientiert ist.

Standardmäßig sind alle neuen Warteschlangen nicht transaktionsorientiert, es sei denn, es wird bei der Erstellung mit dem Modifikator -T angegeben.

Transaktionsorientierte Warteschlangen dürfen nicht verwendet werden, wenn die Möglichkeit besteht, dass eine Warteschlange Routing-Informationen von einem Anwendungsmonitor empfängt.

Transaktionsorientierte Warteschlangen in Microsoft Message Queueing lassen nicht zu, dass Prioritäten für Nachrichten vergeben werden oder dass Nachrichten in einer anderen Reihenfolge als der Reihenfolge ihres Empfangs verarbeitet werden.

-c Gibt einen Stopp nach der Verarbeitung der angegebenen Anzahl Datensätze an.

Erfordert eine ganze Zahl.

Muss der Kleinbuchstabe c sein.

-l Gibt die Prioritätsstufe für jeden Datensatz an.

Erfordert eine ganze Zahl.

Folgende ganzzahlige Werte sind gültig:

0 - 7
Microsoft Message Queueing
Die Prioritätsstufen sind 0 - 7, wobei 0 die niedrigste und 7 die höchste Stufe ist.

3 ist der Standardwert.

0 - 9
IBM Websphere MQ
Die Prioritätsstufen sind 0 - 9, wobei 0 die niedrigste und 9 die höchste Stufe ist.

Der Standardwert hängt von einer Eigenschaft der Warteschlange ab. Sie können diese Eigenschaft im IBM Websphere MQ-Manager ändern.

-m Gibt den Warteschlangenmanager an.

Nur AIX, HP-UX, Linux und Solaris

-o Gibt die Anzahl Sekunden an, nach der eine Nachricht abläuft.

Erfordert eine ganze Zahl.

-q Gibt den Warteschlangentyp an.

Nur Microsoft Windows

Folgende Werte sind gültig:

mq IBM WebSphere MQ

msmq Microsoft Message Queueing (MSMQ)

-t Gibt die Anzahl Millisekunden zwischen den einzelnen Datensätzen an.

Erfordert eine ganze Zahl.

Beziehungen zwischen Befehlsoperationen und -modifikatoren

Bestimmte Modifikatoren werden nur für die Verwendung mit bestimmten Operationen empfohlen. In der folgenden Tabelle werden die Beziehungen zwischen jeder Operation und ihren potenziellen Modifikatoren beschrieben:

Tabelle 31. Beziehungen zwischen Befehlsoperationen und -modifikatoren des Warteschlangendienstprogramms

Operation	Gültige Modifikatoren
`-C`	`-T, -q` *BEISPIEL:* qutil -C *wsname* -T -q mq
`-f`	`-c, -t, -l, -o, -q` *BEISPIEL::* qutil -f *wsname* -c 50 -t 20 -l 4 -o 10 -q msmq
`-i`	KEINE *BEISPIEL:* qutil -i konfigabschnitt
`-k`	`-c` *BEISPIEL:* qutil -k *wsname* -c 50
`-p`	`-c` *BEISPIEL:* qutil -p *wsname* -c 50
`-r`	`-c` *BEISPIEL:* qutil -r *wsname* -c 50
`-s`	KEINE *BEISPIEL:* qutil -s *wsname*
`-x`	KEINE *BEISPIEL:* qutil -x *wsname*

Konvertieren von UMF-Dateien in geeignete Formate

Mit dem UMF-Formatierungsdienstprogramm können Sie die UMF-Datensätze von Breitformat in Hochformat konvertieren und umgekehrt.

UMF-Formatierungsdienstprogramm

Mit dem UMF-Formatierungsdienstprogramm können Sie UMF-Datensätze in und aus Breit- und Hochformaten konvertieren. Darüber hinaus kann das UMF-Formatierungsdienstprogramm UMF-Daten extrahieren, die durch einen bestimmten Tag definiert sind.

UMF-Datensätze können als einzelne Zeile (Breitformat) oder als eine Reihe eingerückter Zeilen, bei denen jede Zeile ein XML-Element und einen Wert enthält (Hochformat), angezeigt werden.

Beispiel: Breitformat

```
<name><name_type>M</name_type><first_name>John</first_name>
<last_name>Smith</last_name></name>
```

Beispiel: Hochformat

```
<name>
  <name_type>M</name_type>
  <first_name>John</first_name>
  <last_name>Smith</last_name>
</name>
```

Befehlssyntax des UMF-Formatierungsdienstprogramms

Das UMF-Formatierungsdienstprogramm verwendet eine Reihe von Befehlen zum Formatieren und Extrahieren von Daten.

Die Basissyntax eines Befehls des UMF-Formatierungsdienstprogramms lautet wie folgt:

```
xutil -o[schalter] option
```

Parameter

-o **Ausgabe**: Sendet die Ausgabe an die Standardausgabe. Erforderlicher Parameter. Parameterschalter:

- **w** Definiert das Ausgabeformat. Das gesamte UMF eines Datensatzes ist in einer Zeile. Alle Zeilenwechsel und Zeilenvorschübe werden entfernt.
- **t** Definiert das Ausgabeformat. Das UMF eines Datensatzes befindet sich in mehreren Zeilen. Setzt pro Zeile einen Tag und verwendet Tabulatoren im Dokument, damit es besser lesbar wird.

-t **Tagname:** Filtert Datensätze anhand eines Tagnamens. Nur Datensätze, die mit diesem Tagnamen gekennzeichnet sind, werden an die Standardausgabe gesendet. Fehler werden an die Standardfehlerausgabe gesendet.

Verwenden Sie den Parameter für den Tagnamen, wenn Sie Datensätze filtern wollen. So gibt es z. B. Dateien mit gemischten Datensätzen aus Entitäten und Aktivitäten. Es ist allerdings sinnvoll, erst die Entitäten zu verarbeiten und dann die Aktivitäten, damit es für die Aktivitäten auch vorhandene Entitäten zum Abgleichen gibt.

Beispiele

Der folgende Befehl filtert die Ausgabe nur auf Entitäten und verwendet dabei mixedlist.xml als Eingabequelle und entity.xml als Ausgabedatei.

```
xutil -ow -t UMF_ENTITY < mixedlist.xml > entity.xml
```

Der folgende Befehl überträgt die Ausgabe des UMF-Formatierungsdienstprogrammprozesses an eine Pipeline oder an das Warteschlangendienstprogramm.

```
xutil -ow < datei.xml |qutil -f wsname
```

Erweitern des Entitätsmodells

Ein Entitätsmodell ist eine Datengruppe, über die Sie eine Entität definieren. Verwenden Sie die folgenden Anweisungen, um das Standardentitätsmodell zu erweitern. Dies ist keine Aufgabe, die häufig ausgeführt wird; es ist jedoch möglich, das Entitätsmodell für Ihre Umgebung zu erweitern.

Universal Message Format (UMF)

UMF ist eine erweiterbare XML-Version, die für das Strukturieren von Datenquellendateien verwendet wird. UMF enthält Standardtags, die Schlüsselteile von Identitäten, Beziehungen und Aktivitäten darstellen. Daten müssen in UMF konvertiert werden und der UMF-Spezifikation entsprechen, bevor sie von den Pipelines verarbeitet werden können.

UMF besteht aus den folgenden hierarchischen Komponenten:

UMF-Dokumente
Die Sammlung von UMF-Segmenten, die die Daten strukturiert und den Typ für den Datenquellensatz angibt.

UMF-Segmente
Die Komponente des UMF-Dokuments, die die Daten für die Datenquelle strukturiert.

UMF-Elemente
XML-Tags und -Werte, die die Daten in einem UMF-Segment eines UMF-Dokuments definieren.

Die UMF-Spezifikation listet die UMF-Dokumenttypen, die UMF-Segmente in jedem UMF-Dokumenttyp und die gültigen UMF-Elemente in jedem UMF-Segment auf.

Analysieren von Quellendaten

Wenn Sie Ihre Quellendaten in die Entitätendatenbank aufnehmen wollen, müssen Sie als Erstes Ihre Quellendaten für die Zuordnung zu UMF analysieren.

Vorgehensweise

1. Identifizieren Sie die Daten, die Sie in die Entitätendatenbank laden wollen.
2. Stellen Sie sicher, dass die Daten konsistent und vollständig sind.
3. Stellen Sie die Breite der Elementwerte der eingehenden UMF-Segmente im Vergleich zur Breite der entsprechenden Datenbanktabellenspalten fest.
4. Stellen Sie ungültige Zeichen in den Quellendaten fest.

Ergebnisse

Je nach den Ergebnissen Ihrer Analyse sind mehrere Optionen denkbar, z. B.:

- Verwenden von DQM-Regeln zum Korrigieren von Daten, die ungültige Zeichen enthalten.
- Verwenden von DQM-Regeln zum Abschneiden von Daten, die breiter sind als ihre entsprechenden Datenbanktabellenspalten.
- Anfordern vollständigerer Daten von externen Datenquellenprovidern.
- Ausschließliches Laden von Feldern mit gültigen Daten.

Überprüfen der UMF-Standardspezifikation

Sie sollten die UMF-Standardspezifikation überprüfen, die Sie beim Erstellen Ihrer angepassten UMF-Spezifikation und des Entitätsmodells unterstützt. Diese Elemente stellen die Datenübertragung zwischen Datenquellen und UMF-Tags schematisch dar, die von der Entitätendatenbank aufgenommen wird.

Zuordnen von UMF-Segmenten zum Format der Entitätendatenbank

Immer wenn Ihre Daten neue UMF-Segmente erfordern, müssen Sie neue Datenzuordnungen für die Daten in diesen UMF-Segmenten erstellen. Ohne gültige Datenzuordnung können Sie Daten nicht erfolgreich in die Entitätendatenbank laden.

Risiken beim Modifizieren der Entitätendatenbank

Das Modifizieren der Entitätendatenbank birgt Risiken in sich und sollte nicht ohne ausreichende Erfahrung und entsprechendes Fachwissen ausgeführt werden.

- Tabellen sollten der Entitätendatenbank nicht ohne ausreichende Erfahrung oder entsprechendes Fachwissen hinzugefügt werden.
- Beim Hinzufügen von Feldern zu einer Datenbanktabelle wird mehr als nur die betreffende Tabelle in den Prozess einbezogen. Es wird empfohlen, die vorhandenen Tabellen und Felder zu verwenden, um neue Daten zu klassifizieren, sofern dies möglich ist.
- Indizes von Datenbanktabellen dürfen nicht modifiziert werden. Das Modifizieren von Indizes in den Datenbanktabellen kann zu unvorhersehbaren und unerwünschten Ergebnissen wie einer Blockierung von Visualizer führen.
- Es wird empfohlen, dass DQM-Änderungen nur mit ausreichendem Fachwissen oder mit der Hilfe von IBM vorgenommen werden.
- Prüfen Sie die neuen Konfigurationen vor der Anwendung auf Ihre Produktionsumgebung immer in einer Testdatenbank.

Hinzufügen von Tabellen zur Entitätendatenbank

Wenn Sie eine neue Datenquelle hinzufügen, müssen Sie möglicherweise auch eine neue Datenbanktabelle hinzufügen.

Informationen zu diesem Vorgang

Wenn Sie der Entitätendatenbank Tabellen hinzufügen, werden die neuen Daten bei der Auflösung nicht berücksichtigt; die Tabellen ermöglichen lediglich die Speicherung von Daten.

Es wird empfohlen, die neuen Konfigurationen vor der Anwendung auf Ihre Produktionsumgebung in einer Testdatenbank zu prüfen.

Es wird empfohlen, die vorhandenen Tabellen und Felder zu verwenden, um neue Daten zu klassifizieren, sofern dies möglich ist.

Wenn Sie eine neue Tabelle hinzufügen, können Sie erwartete Daten speichern, die noch nicht im System konfiguriert sind. Erstellen Sie die neue Datenbanktabelle so, dass sie mit Ihrem aktuellen Datenmodell konsistent ist.

Stellen Sie sicher, dass Sie die jeweils erforderlichen Felder einschließen:

- ENTITY_ID
- DSRC_ACCT_ID
- HIST_STAT - erforderlich, wenn Sie sequenzielle Verlaufsverfolgung verwenden
- SYS_CREATE_DT
- SYS_DELETE_DT
- SYS_LSTUPD_DT
- SYS_LSTUPD_US

Vorgehensweise

1. Erstellen Sie die neue Tabelle in der Entitätendatenbank.
2. Erstellen Sie die Datenzuordnung für die neue Tabelle.
3. Fügen Sie dem Wörterverzeichnis neue Datenbanktabellen hinzu.
4. Definieren Sie die Datenzuordnungen für die neue Tabelle.
5. Bestimmen Sie die entsprechenden DQM-Regeln, die auf das neue Segment angewendet werden sollen, und konfigurieren Sie diese Regeln über die Konsole.
6. Prüfen Sie die neue Konfiguration, indem Sie bekannte Testdaten über eine Pipeline laufen lassen und die Ergebnisprotokolldateien überprüfen.
   a. Prüfen Sie, ob der Test fehlerfrei ausgeführt wird.
   b. Überprüfen Sie die Konsole auf UMF-Ausnahmebedingungen.
   c. Überprüfen Sie die Protokolldateien `knotenname.Sql.Err.log` und `knotenname.err` auf Fehler.
   d. Prüfen Sie, ob die Testergebnisse mit den erwarteten Ergebnissen übereinstimmen.
   e. Überprüfen Sie die Tabelle UMF_LOG, um sicherzustellen, dass alle Datensätze ordnungsgemäß geladen wurden.

Hinzufügen von Feldern zu Entitätendatenbanktabellen:

Für neue Daten müssen Sie möglicherweise einer vorhandenen Entitätendatenbanktabelle ein neues Feld hinzufügen.

Informationen zu diesem Vorgang

Einer vorhandenen Tabelle kann ein neues Feld hinzugefügt werden, wenn für ein neues UMF-Segment keine vollständig neue Tabelle erforderlich ist.

Wenn Sie einer vorhandenen Entitätendatenbanktabelle Felder hinzufügen, werden die neuen Daten bei der Auflösung nicht berücksichtigt; die Felder ermöglichen lediglich die Speicherung von Daten.

Es wird empfohlen, die neuen Konfigurationen vor der Anwendung auf Ihre Produktionsumgebung in einer Testdatenbank zu prüfen.

Es wird empfohlen, die vorhandenen Tabellen und Felder zu verwenden, um neue Daten zu klassifizieren, sofern dies möglich ist.

Vorgehensweise

1. Fügen Sie das neue Feld der entsprechenden Datenbanktabelle hinzu.
2. Erstellen Sie in der Konsole die Datenzuordnung für das neue Feld.
3. Bestimmen Sie die geeigneten DQM-Regeln für die Anwendung auf das neue Feld und konfigurieren Sie diese Regeln über die Konsole.
4. Prüfen Sie die neue Konfiguration, indem Sie bekannte Testdaten über eine Pipeline laufen lassen und die Ergebnisprotokolldateien überprüfen.
   a. Prüfen Sie, ob der Test fehlerfrei ausgeführt wird.
   b. Überprüfen Sie die Konsole auf UMF-Ausnahmebedingungen.
   c. Überprüfen Sie die Protokolldateien `knotenname.Sql.Err.log` und `knotenname.err` auf Fehler.
   d. Prüfen Sie, ob die Testergebnisse mit den erwarteten Ergebnissen übereinstimmen.

e. Überprüfen Sie die Tabelle UMF_LOG, um sicherzustellen, dass alle Datensätze ordnungsgemäß geladen wurden.

Hinzufügen neuer Datenbanktabellen zum Wörterverzeichnis:

Wenn die Daten (und UMF) die Erstellung einer neuen Datenbanktabelle erfordern, müssen Sie diese Tabelle dem Wörterverzeichnis der Datenbanktabellen hinzufügen, das das System verwendet. Ist die Tabelle nicht im Wörterverzeichnis vorhanden, können Sie keine Datenzuordnung für UMF und die Tabelle erstellen.

Vorbereitende Schritte

Der Benutzer muss über die Berechtigung zum Lesen der Datenbanktabelle und zum Speichern von Daten in der Datenbanktabelle verfügen.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **Wörterverzeichnis** an.
4. Klicken Sie die Schaltfläche **Neu** an.
5. Geben Sie in das Feld **Tabellenname** den Namen der neuen Datenbanktabelle ein.

Definieren von Datenzuordnungen

Sie müssen eine Datenzuordnung für neue UMF-Segmente und -Tags erstellen. Beim Hinzufügen neuer Quellensysteme zum Produkt werden manchmal auch neue UMF-Segmente und -Tags erstellt. Eine Datenzuordnung ordnet die Daten im UMF-Format den entsprechenden Tabellen und Tabellenspalten in der Entitätendatenbank zu.

Datenzuordnungen:

Eine Datenzuordnung ordnet Daten in einer UMF-Datei den entsprechenden Tabellen und Tabellenspalten in der Entitätendatenbank zu.

Ohne gültige Datenzuordnung können Sie Daten nicht erfolgreich in die Entitätendatenbank laden. Immer wenn Ihre Daten neue UMF-Segmente erfordern, müssen Sie neue Datenzuordnungen für die Daten in diesen UMF-Segmenten erstellen.

Beispiel

Franks Autoservice hat kürzlich mit dem Sammeln von Daten von Versicherungsunternehmen für seine Kunden angefangen. Beispielsweise könnten für die die UMF-Daten für ein neues Versicherungsunternehmen die folgenden UMF-Segmente verwendet werden:

```
<ATTRIBUTE>
<INSURANCECOMPANY>Mooninite Casualty Company</INSURANCECOMPANY>
</ATTRIBUTE>
```

Sie müssen eine neue Datenzuordnung für den UMF-Datenpfad von <ATTRIBUTE><INSURANCECOMPANY> in die entsprechende Tabellenspalte in der Entitätendatenbank erstellen. Der XPath-Wert für den UMF-Datenpfad ist `./ATTRIBUTE/INSURANCECOMPANY/`.

Anzeigen von Datenzuordnungen:

Eine Datenzuordnung ordnet Daten in einer UMF-Datei den entsprechenden Tabellen und Tabellenspalten in der Entitätendatenbank zu.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **Datenzuordnung** an.
4. Wählen Sie in der Dropdown-Liste **Segment** das UMF-Segment aus, das Sie anzeigen wollen.
5. Wählen Sie in der Dropdown-Liste **Tabelle** die UMF-Segmenttabelle aus, deren Zuordnung Sie anzeigen wollen.

Erstellen von Datenzuordnungen:

Eine Datenzuordnung ordnet UMF-Daten den entsprechenden Tabellen und Tabellenspalten in der Entitätendatenbank zu. Eine neue Datenzuordnung ist erforderlich, wenn eingehende Daten mit neuen UMF-Tags vom System verarbeitet werden sollen.

Vorbereitende Schritte

Wenn über diese Datenzuordnung Daten mehreren Tabellen zugeordnet werden, müssen Sie überprüfen, ob die Tabellen bei der Verarbeitung durch die Pipeline in der korrekten Reihenfolge geladen werden. Ist die Tabelle nicht im Wörterverzeichnis vorhanden, müssen Sie dem Wörterverzeichnis die neue Tabelle hinzufügen, damit Sie eine Datenzuordnung für UMF und die Tabelle erstellen können.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **Datenzuordnung** an.
4. Wählen Sie in der Dropdown-Liste **Segment** das UMF-Segment aus, für das Sie einer Tabelle eine neue Datenzuordnung hinzufügen wollen.
5. Wählen Sie in der Dropdown-Liste **Tabelle** die UMF-Segmenttabelle aus, der Sie eine neue Datenzuordnung hinzufügen wollen.
6. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie die Schaltfläche **Neu** an, um eine neue Datenzuordnung zu erstellen.
   - Wählen Sie eine Datenzuordnung in der Liste aus und klicken Sie anschließend die Schaltfläche **Klonen** an, um eine Datenzuordnung auf der Basis einer vorhandenen Datenzuordnung zu erstellen.
7. Handelt es sich um ein neues Segment, geben Sie den Namen des UMF-Segments in das Feld **Segment** ein.
8. Wählen Sie die gewünschte Datenbanktabelle in der Dropdown-Liste **Tabelle** aus.
9. Geben Sie in das Feld **Tabellenspalte** den Namen der Datenbanktabellenspalte ein, der Sie den UMF-Datenpfad zuordnen wollen.
10. Wählen Sie in der Dropdown-Liste **Feldtyp** den korrekten Feldtyp für die Tabellenspalte in der Datenbank aus.

11. Wählen Sie in der Dropdown-Liste **Datentyp** den korrekten Datentyp für die Datenwerte aus.
12. Geben Sie in das Feld **UMF-Datenpfad** den UMF-Tag ein.
13. Wählen Sie in der Dropdown-Liste **Aktualisierungsverfahren** die gewünschte Aktualisierungsmethode aus. Diese legt fest, ob der eingehende Wert oder der bereits gespeicherte Wert beibehalten wird.
14. Wählen Sie in der Dropdown-Liste des Felds **Status** den Status der Datenzuordnung aus.
15. Klicken Sie die Schaltfläche **Speichern** an.

Löschen von Datenzuordnungen:

Eine Datenzuordnung ordnet UMF-Daten den entsprechenden Tabellen und Tabellenspalten in der Entitätendatenbank zu. Sie können eine Datenzuordnung löschen, die nicht mehr vom System verwendet wird.

Vorgehensweise

1. Klicken Sie die Schaltfläche **Konfiguration** an.
2. Klicken Sie die Schaltfläche **UMF** an.
3. Klicken Sie die Registerkarte **Datenzuordnung** an.
4. Wählen Sie in der Dropdown-Liste **Segment** das UMF-Segment aus, für das Sie eine Tabelle zum Löschen einer Datenzuordnung auswählen wollen.
5. Wählen Sie in der Dropdown-Liste **Tabelle** die UMF-Segmenttabelle aus, in der Sie eine Datenzuordnung löschen wollen.
6. Wählen Sie in der Liste eine Datenzuordnung aus und klicken Sie anschließend die Schaltfläche **Löschen** an.

Hilfethemen:

Datenzuordnungen - Registerkarte 'Allgemein':

Über die Registerkarte **Allgemein** können Sie die Details für die Datenzuordnung angeben.

Segment
: Geben Sie den Namen des Segments ein, für das Sie eine Datenzuordnung erstellen wollen. Der Segmentname muss in Großbuchstaben eingegeben werden.

Tabelle
: Wählen Sie in der Dropdown-Liste die Tabelle für die Datenzuordnung aus, die Sie erstellen wollen.

Tabellenspaltenname
: Geben Sie den Namen der Tabellenspalte ein, die Sie erstellen wollen.

Tabellenspaltentyp
: Wählen Sie in der Dropdown-Liste den Tabellenspaltentyp für den Tabellenspaltennamen aus.

  Eindeutige ID
  : Die Tabellenspalte enthält einen von der DatenbankEngine generierten eindeutigen Schlüssel, der automatisch erhöht wird. Nur eine Tabellenspalte kann mit diesem Wert konfiguriert werden.

Entitätsschlüssel
Falls ausgewählt, ist diese Tabellenspalte immer auf die Entitäts-ID (ENTITY_ID) gesetzt.

Geschäftsschlüssel
Die Tabellenspalte ergibt zusammen mit anderen angegebenen Geschäftsschlüsseltabellenspalten einen zusammengesetzten Suchschlüssel, mit dem festgestellt werden kann, ob bereits ein identischer Datensatz vorhanden ist.

Attribut
Die Tabellenspalte wird nur zum Speichern von Daten verwendet und hat keinerlei funktionelle Auswirkungen auf Einfüge-, Aktualisierungs- und Löschvorgänge in der Tabelle.

Schlüsselattribut
Der Wert der Tabellenspalte wird verwendet, um festzustellen, ob bereits ein Datensatz mit demselben Wert vorhanden ist. Die Datenbank verfolgt die im Laufe der Zeit an diesen Werten vorgenommenen Änderungen. Beispiel: Wenn Sie eine Version des Datensatzes behalten wollen, wenn der Wert von ADDR1 geändert wird, geben Sie den Wert von ADDR1 als Schlüsselattribut an.

Dieser Wert hat nichts mit Indizes zu tun.

Protokollfolge
Die Tabellenspalte wird verwendet, um zu ermitteln, welcher Datensatz, der von einer bestimmten Quelle bereitgestellt wurde, der aktuelle ist und welche Datensätze schon älter sind.

Protokollfolge wird stets der Tabellenspalte HIST_STAT zugewiesen.

Löschzeitmarke
Die Tabellenspalte wird zum Speichern des letzten Datums/Zeitpunkts einer Löschung des Datensatzes verwendet.

Aktualisierungszeitmarke
Die Tabellenspalte wird zum Speichern des letzten Datums/Zeitpunkts einer Aktualisierung des Datensatzes verwendet.

Datentyp
Wählen Sie in der Dropdown-Liste den Datentyp für die Tabellenspalte aus.

CHAR
Zeichendaten (alphanumerisch).

INT Ganzzahlige Daten.

DATE Datumsdaten. Beispiel: jjjj-mm-tt oder mm-tt-jjjj.

DATE/TIME
Datums-/Zeitdaten. Beispiel: jjjj-mm-tt hh:mm:ss oder mm-tt-jjjj hh:mm:ss.

UMF-Datenpfad
Geben Sie die XPath-Position des UMF-Tags ein.

Aktualisierungsverfahren
Wählen Sie in der Dropdown-Liste das Aktualisierungsverfahren für die

Datenzuordnung aus, die Sie erstellen wollen. Das Aktualisierungsverfahren bestimmt, ob der eingehende oder der gespeicherte Wert beibehalten wird.

Nie Wenn ein Wert für das UMF-Element in der Datenbanktabelle vorhanden ist, kann dieser Wert nicht aktualisiert werden.

Immer
Wenn ein Wert für das UMF-Element in der Datenbanktabelle vorhanden ist, kann dieser Wert aktualisiert werden.

Maximalwert
Der jeweils größere Wert, eingehend oder gespeichert, wird beibehalten oder aktualisiert.

Nur für die Datentypen INT, DATE oder DATE/TIME von Tabellenspalten.

Mindestwert
Der jeweils kleinere Wert, eingehend oder gespeichert, wird beibehalten oder aktualisiert.

Nur für die Datentypen INT, DATE oder DATE/TIME von Tabellenspalten.

Status Wählen Sie in der Dropdown-Liste den Status für die Datenzuordnung aus, die Sie erstellen wollen.

Aktiv Die Datenzuordnung ist aktiv.

Inaktiv
Die Datenzuordnung ist inaktiv.

Adressvereinheitlichung mit IBM InfoSphere QualityStage und AddressDoctor

Die Adressbereinigung und -vereinheitlichung ist ein Pipelineprozess, mit dem Sie Adressinformationen korrigieren und vereinheitlichen können, um eine optimale Entitätsauflösungsverarbeitung zu erzielen. Diese neue IBM® InfoSphere™ Identity Insight-Funktion ermöglicht die Verwendung einer Branchenstandardlösung für die Vereinheitlichung von Adressdaten, die AddressDoctor®, IBM InfoSphere Information Server, IBM InfoSphere DataStage® und IBM WebSphere® QualityStage™ umfasst.

Die Unterstützung für ein von AddressDoctor bereitgestelltes Adressvereinheitlichungsmodul beseitigt die Abhängigkeiten von anderen Modulen wie WAVES (Worldwide Address Verification and Enhancement System) und deren Einschränkungen. Das Adressvereinheitlichungsmodul AddressDoctor kann unter Einsatz von DataStage und der QS-AVI-Schnittstelle (QualityStage Address Verification Interface) für die Identity Insight-Entitätsauflösung verwendet werden. QualityStage ist eine Komponente von IBM Information Server.

AddressDoctor® bietet die folgenden Vorteile:

- Unterstützung für mehr als 240 Länder und Gebiete
- Bessere Abdeckung von Straßennamen
- Unicode-Aktivierung und Unterstützung aller wichtigen Zeichensätze
- Bereitstellung von Transliteration
- Bereitstellung eines Prüfungsstatus für die Richtigkeit der Adresse

- Bereitstellung von Formaten für den lokalen Poststandard

Die Implementierung von AddressDoctor mit QS-AVI ist keine einfache Task. Es wird daher empfohlen, den IBM Ansprechpartner um Unterstützung zu bitten.

Voraussetzungen für die QS-AVI-Adressbereinigung und Taskübersicht

Die detaillierten Prozessschritte für die Verwendung der IBM QualityStage- und AddressDoctor-Schnittstellen (QS-AVI) für die Identity Insight-Adressbereinigung sind in einem Techdoc unter ibm.com beschrieben. Dieser Abschnitt enthält eine Übersicht über den Prozess und die Voraussetzungen sowie einen Link zu den detaillierten Informationen.

Vorbereitende Schritte

Die folgenden Produkte sind erforderlich:

- IBM InfoSphere Information Server einschließlich IBM InfoSphere DataStage und IBM InfoSphere QualityStage Version 8.0.1
- QS-AVI-DataQuality-Stages
- AddressDoctor(R)-Datenbank für das erforderliche Land

Informationen zu diesem Vorgang

Der Prozess wird mit den folgenden allgemeinen Schritten ausgeführt:

Vorgehensweise

1. Definieren Sie einen QS-AVI-Stage-Job in DataStage und QualityStage Designer.
2. Importieren Sie die Datei "AddressValidateWS.dsx" in die Stage. (Dies ist ein vordefinierter Adressbereinigungsjob und wurde für die EAS- und QS-AVI-Integration konzipiert.) Die Datei befindet sich auf dem Datenträger mit der Fixpackinstallation: `<ii-installation>/srd-home/qsavi/AddressValidateWS.dsx`
3. Modifizieren Sie die Adressprüfungsstage und aktivieren Sie den DataStage-Job für Information Services.
4. Definieren Sie den DataStage-Job als Service in der Information Server-Konsole.
5. Prüfen Sie die Bereitstellung mithilfe von WISD (WebSphere Information Services Director), um ein WSDL-Dokument (Web Service Definition Language) für diesen neuen Service zu generieren und zu prüfen.
6. Testen Sie den Service in einer Umgebung wie WebSphere Integration Developer.
7. Aktivieren Sie die QS-AVI-Komponente durch Ändern von AddrConnection im Abschnitt [OAC] der Datei `pipeline.ini` in folgendes Format:

   ```
   [OAC]
   AddrConnection=qsavi://host:port/?timeout=ms
   ```

   host Hostname oder IP-Adresse von Information Server.

   port Portnummer. Der Standardport ist 9080.

   timeout
   Optionaler Parameter. Sie können die Verbindungszeitlimitparameter extern festlegen. Der Standardwert für das Verbindungszeitlimit beträgt 10.000 ms (10 Sekunden).

Nächste Schritte

Die detaillierten Schritte dieses Prozesses werden in QS-AVI address cleansing as a Web process for IBM InfoSphere Identity Insight beschrieben.

Fehlerbehebung für QS-AVI

QS-AVI gibt 'valstatus_qsav' zurück, was die Qualität der Adressbereinigung beschreibt und eine Fehlerbehebung für verwandte Probleme ermöglicht.

Ausnahmebedingungen

Eine Ausnahmebedingung wird auf der Basis des Bearbeitungswertstatus generiert:

```
// Bearbeitungswertstatus
// V  - Geprüft
// C  - Korrigiert
// P3 - Nicht korrigiert - Hohe Zustellbarkeit
// P2 - Nicht korrigiert - Ausreichende Zustellbarkeit
// P1 - Nicht korrigiert - Niedrige Zustellbarkeit
// N1 - Nicht überprüft - Land nicht erkannt
// N2 - Nicht überprüft - Länderdatenbank nicht gefunden
// N3 - Nicht überprüft - Land nicht freigegeben
// N4 - Nicht überprüft - Prüfung nicht aufgerufen
// N5 - Unzureichende Informationen
// Q1 - Keine Vorschläge
// Q2 - Unvollständige Vorschläge
// Q3 – Vorschläge
```

QS-AVI gibt außerdem 'resultstatus_qsav' zurück, was die Wahrscheinlichkeit der Adressbereinigung beschreibt:

```
// Behandlung der Wahrscheinlichkeit der Zustellbarkeit
// 0 - Leer
// 1 - Nicht überprüft
// 2 - Nicht überprüft, jedoch standardisiert
// 3 - Überprüft und korrigiert
// 4 - Geprüft, jedoch geändert
// 5 - Geprüft, jedoch standardisiert
// 6 - Geprüft und nicht geändert
// 7 - Aufgrund mehrerer Übereinstimmungen wurde kein Wert zugewiesen
```

Fehlernachrichten

6301E - Invalid response.

6302E - Cannot connect to InfoServer server
Diese Nachricht wird generiert, wenn EAS keine Verbindung zu InfoServer herstellen kann. Es wird auch eine Antwort 'soapenv:Fault' von InfoServer generiert, die als ungültige Antwort behandelt wird.

6303E - Error, failure to connect to the server : {0}", __serverName
Diese Nachricht wird generiert, wenn EAS keine Verbindung zum korrekten InfoServer-Server herstellen kann.

Kapitel 8. Analysieren von Daten

Analyst Toolkit stellt ein Funktionsset zur Anwendungsentwicklung und -anpassung für Identity Insight bereit. Hierbei handelt es sich um eine Gruppe von Benutzerschnittstellen und Berichten, die je nach Bedarf modifiziert oder von anderen Anwendungen referenziert werden können.

Analysieren von Daten mit Visualizer

Mit Visualizer können Sie eine Reihe von Analysetasks ausführen. Sie können Alerts prüfen und die Disposition von Alerts ausführen, Entitäten suchen, Entitätsdaten anzeigen, Diagramme zu Entitäten und deren Beziehungen zu anderen Entitäten anzeigen, Attributalertgeneratoren erstellen und verwalten, eine einzelne Entität oder eine kleine Datei mit Entitäten hinzufügen, Beziehungen zwischen Entitäten offenlegen und Berichte drucken.

Konfigurieren von Visualizer

Damit Sie Visualizer erfolgreich verwenden können, müssen Sie wissen, wie Sie auf Visualizer zugreifen und wie Sie die Darstellung der von Visualizer angezeigten Informationen an Ihre Bedürfnisse anpassen können.

Visualizer

Visualizer ist eine grafische Benutzerschnittstelle, die Analysten und Prüfer zum Analysieren der Ergebnisse von Alerts, Beziehungen und Entitätsauflösungen verwenden.

Visualizer wird von einer integrierten Version von IBM WebSphere Application Server gehostet. Sie konfigurieren Visualizer über die Konfigurationskonsole und die Auswahl **Benutzervorgaben** im Menü **Datei** von Visualizer.

Visualizer-Benutzer können verschiedene Analysetasks ausführen:

Ausführen von Analysen und Dispositionen für Alerts
Von der Entitätsauflösungsverarbeitung generierte Alerts stellen Beziehungs- und Entitätsauflösungen dar, die für ein Unternehmen von Interesse sind. In der Regel überprüfen Analysten Alerts und entscheiden auf Grundlage der Alertinformationen, welche Maßnahme ergriffen werden soll oder dass keine Maßnahme erforderlich ist. Es gibt die folgenden drei Alerttypen: Rollenalerts, Attributalerts und Ereignisalerts.

Visualizer zeigt die Alerts an und stellt Analysten Textsichten und grafisch orientierte Sichten der Alerts und der an den Alerts beteiligten Entitäten bereit. Analysten können die Details abrufen und anschließend den Dispositionsstatus des Alerts entsprechend festlegen.

Erstellen und Verwalten von Attributalertgeneratoren
Mit Visualizer können Analysten über die Komponente 'Attributalertgenerator' persistente Suchen erstellen und verwalten sowie die Anzeige und den Emfpang von Attributalerts verwalten. Analysten können Attributalertgeneratoren basierend auf Attributdaten erstellen, um Identitäten zu suchen, die basierend auf diesen Attributdaten in Entitäten aufgelöst wurden. Analysten können auch einen Attributalertgenerator erstellen, um eine persistente Suche nach einer bestimmten Entität in der Entitätendatenbank durchzuführen.

Suchen von Entitäten

Visualizer-Benutzer können auch nach verschiedenen Methoden Entitäten für die weitere Analyse suchen:

- Nach Attributen
- Nach Datenquellenbenutzerkonto
- Nach Entitäts-ID
- Nach Auflösung (wie stark das eingegebene Kriterium mit den Identitäten und Entitäten in der Entitätendatenbank basierend auf den Schwellenwerten für die Mindestauflösungsbewertung übereinstimmt)

Hinzufügen von Entitäten und offengelegten Beziehungen

Mit Visualizer können Analysten Datensätze für Entitätsauflösung und Beziehungserkennung hinzufügen. Sie können einen einzelnen Identitätsdatensatz hinzufügen oder eine UMF-Datei laden, die Tausende von Identitätsdatensätzen enthält. Wie beim Hinzufügen von Identitäten durch Übernahmeprogramme werden durch Visualizer hinzugefügte Datensätze von einer Pipeline für Entitätsauflösung und Beziehungserkennung verarbeitet. Die Verarbeitungsergebnisse werden in die Entitätendatenbank geschrieben und Alerts werden in Visualizer veröffentlicht.

Analysten können auch Beziehungen zwischen Entitäten (nach Identität) offenlegen, wenn sie eine Verknüpfung zwischen den Identitäten kennen. Offengelegte Beziehungen sind beispielsweise das Zuordnen von Entitäten zu einander auf der Grundlage von Kontaktdaten für den Notfall oder von in einer Bewerbung aufgelisteten Referenzen. Diese Beziehungen wurden von der Entität in der Anwendung offengelegt.

Generieren und Drucken von Berichten

Visualizer enthält auch mehrere Berichte, die Analysten anzeigen und drucken können, damit sie ihre Arbeit mit Visualizer einfacher verwalten und überwachen können.

Konfigurieren von Visualizer

Sie können Visualizer-Einstellungen konfigurieren, um die Darstellung von Informationen in Ihren Visualizer-Sitzungen anzupassen.

Konfigurieren von Visualizer-Anzeigeoptionen:

Sie können die Visualizer-Anzeige anpassen, indem Sie die Hintergrundfarbe, Schriftart und andere Anzeigeoptionen auf der Registerkarte **Fenstervorgaben** ändern.

Informationen zu diesem Vorgang

Die Visualizer-Anzeigeoptionen werden für jeden Visualizer-Client konfiguriert. Durch Ausführen der folgenden Anweisungen ändern Sie nur die Anzeige des Visualizer-Clients, an dem Sie zurzeit angemeldet sind.

Vorgehensweise

1. Wählen Sie in Visualizer **Datei** > **Benutzervorgaben** > **Fenstervorgaben** aus.
2. Wählen Sie die zu verwendenden Anzeigeoptionen aus, um die gewünschte Darstellung und Funktionsweise zu erreichen. Die Einstellungen in den Dropdown-Listen **Thema**, **Schriftart** und **Größe** können Sie nur ändern, wenn Sie die Option *Metal* in**Darstellung und Funktionsweise** auswählen.

3. Klicken Sie **Übergeben** an. Sie werden mit einer Bestätigungsnachricht informiert, dass Sie Visualizer erneut starten müssen, damit Ihre Änderungen wirksam werden.
4. Klicken Sie **OK** an.
5. Schließen Sie Visualizer. Starten Sie Visualizer und melden Sie sich erneut an.

Ergebnisse

Visualizer wird nun unter Verwendung der neuen, von Ihnen ausgewählten Fensteranzeigeoptionen angezeigt.

Festlegen des Standardpfads für UMF-Dateien:

Wenn Sie regelmäßig Identitätsdatensätze in UMF-Datendateien zur Verarbeitung durch den Visualizer laden, sparen Sie sich durch das Festlegen des Standardpfads einen Arbeitsschritt.

Informationen zu diesem Vorgang

Für jeden Visualizer-Client werden Standardpfadeinstellungen konfiguriert. Der über diese Task angegebene Standardpfad gilt nur für die Visualizer-Instanz, an der Sie zurzeit angemeldet sind.

Vorgehensweise

1. Wählen Sie in Visualizer **Datei** > **Benutzervorgaben** > **Benutzervorgaben für das System** aus.
2. Führen Sie im Bereich **Standardpfad für Laden von Datei** einen der folgenden Schritte aus:
   - Geben Sie den vollständigen Pfad des zu verwendenden Verzeichnisses ein.
   - Navigieren Sie zum Verzeichnis, um es auszuwählen.
3. Klicken Sie **Übergeben** an. Sie werden mit einer Bestätigungsnachricht informiert, dass Sie Visualizer erneut starten müssen, damit Ihre Änderungen wirksam werden.
4. Klicken Sie in der Bestätigungsnachricht **OK** an.
5. Schließen Sie Visualizer, starten Sie ihn wieder und melden Sie sich erneut an.

Ergebnisse

Bei jedem Laden einer UMF-Datei ist der Standardpfad das Verzeichnis, das Sie angegeben haben.

Festlegen des Standardpfads für Centrifuge:

Wenn Sie den optionalen Centrifuge Desktop aus Centrifuge Systems zum Darstellen und Anzeigen von Entitätsdiagrammen verwenden, müssen Sie den Dateipfad für Centrifuge Desktop in den Visualizer-Vorgaben angeben.

Informationen zu diesem Vorgang

Für jeden Visualizer-Client werden Standardpfadeinstellungen konfiguriert. Der über diese Task angegebene Standardpfad gilt nur für die Visualizer-Instanz, an der Sie zurzeit angemeldet sind.

Vorgehensweise

1. Klicken Sie in Visualizer **Datei** > **Benutzervorgaben** > **Benutzervorgaben für das System** an.
2. Führen Sie unter dem Abschnitt **Dateipfade** in **Centrifuge-Pfad** einen der folgenden Schritte aus:
   - Geben Sie den Dateipfad oder die URL (Uniform Resource Locator) für die Centrifuge Desktop-Anwendung in das Feld ein.
   - Navigieren Sie zur Centrifuge Desktop-Anwendung und öffnen Sie sie.
3. Klicken Sie **Übergeben** an. Sie werden mit einer Bestätigungsnachricht informiert, dass Sie Visualizer erneut starten müssen, damit Ihre Änderungen wirksam werden.
4. Klicken Sie in der Bestätigungsnachricht **OK** an.
5. Schließen Sie Visualizer, öffnen Sie ihn wieder und melden Sie sich erneut an.

Ergebnisse

Nachdem der Pfad konfiguriert ist, wird die Schaltfläche **Centrifuge** in den Anzeigen **Rollenalert-Detail** und **Entitätszusammenfassung** im Prüffenster angezeigt. Klicken Sie die Schaltfläche an, um Ihre Centrifuge Desktop-Anwendung direkt in Visualizer zu starten.

Konfigurieren von Mindestwerten für die Schwellenwertbewertung bei Visualizer-Abfragen:

Wenn Sie in Visualizer entweder über die Funktion **Auflösungsbasierte Suche** oder über einen Attributalertgenerator nach einer Entität suchen, wählen Sie im Rahmen der Kriterien eine Mindestähnlichkeitsbewertung aus. Mit Ihrer Auswahl legen Sie die Entitäts- und Beziehungsauflösungsstärke fest, die das System bei der Suche und Rückgabe von Entitäten verwendet. Sie können die Standardwerte für einen oder mehrere dieser Schwellenwerte in Visualizer über die Registerkarte **Benutzervorgaben für das System** ändern.

Informationen zu diesem Vorgang

Diese Einstellungen werden für jeden Visualizer-Client konfiguriert. Mit der folgenden Task ändern Sie den Mindestbewertungsschwellenwert nur für die Visualizer-Instanz, an der Sie zurzeit angemeldet sind.

Vorgehensweise

1. Klicken Sie in Visualizer **Datei** > **Benutzervorgaben** > **Benutzervorgaben für das System** an.
2. Geben Sie im Abschnitt **Mindestbewertungswert** die niedrigste Ähnlichkeitsbewertung an, mit der festgelegt werden soll, welche Suchergebnisse angezeigt werden. Je höher die Zahl, desto mehr Entitätsdaten müssen mit den Suchkriterien übereinstimmen, wodurch sich die Anzahl der zurückgegebenen Ergebnisse reduzieren kann.
3. Klicken Sie **Übergeben** an. Sie werden mit einer Bestätigungsnachricht informiert, dass Sie Visualizer erneut starten müssen, damit Ihre Änderungen wirksam werden.
4. Klicken Sie in der Bestätigungsnachricht **OK** an.
5. Schließen Sie Visualizer, öffnen Sie ihn wieder und melden Sie sich erneut an.

Konfigurieren von Standardfilteroptionen für das Fenster 'Alertzusammenfassung':

Über die Registerkarte **Filtereinstellungen für Alertanzeige** der Anzeige **Benutzervorgaben für das System** können Sie die Standardeinstellungen für die Filteroptionen in Ihrem Fenster **Alertzusammenfassung** anpassen.

Informationen zu diesem Vorgang

Diese Einstellungen steuern die folgenden Standardwerte in Visualizer:

- Die maximale Anzahl in der Alertliste anzuzeigende Alerts
- Die Mindestbeziehungsbewertung für anzuzeigende Rollenalerts
- Die Anzahl der Tage, für die Alertzusammenfassungen angezeigt werden sollen (ab dem aktuellen Datum rückwärts)

Die Werte, die Sie hier festlegen, bestimmen die Standardfilterwerte, die Ihre Visualizer-Instanz immer verwendet, wenn Sie ein neues Fenster **Alertzusammenfassung** öffnen.

Vorgehensweise

1. Wählen Sie in Visualizer **Datei** > **Benutzervorgaben** > **Benutzervorgaben für das System** aus.
2. Geben Sie unter dem Abschnitt **Filtereinstellungen für Alertanzeige** in **Maximale Anzahl in Alertliste anzuzeigende Alerts** eine Zahl für die maximale Anzahl Alerts ein, die in der Tabelle mit der Alertliste angezeigt werden soll. Die Standardeinstellung ist 100. Das heißt, wenn Sie eine Alertzusammenfassung auswählen, werden in der Alertliste die ersten 100 zugeordneten Alerts angezeigt. Die Standardeinstellung können Sie bei Bedarf ändern, um weniger Alerts anzuzeigen.
3. Geben Sie in **Mindestbeziehungsbewertung** die niedrigste Beziehungsbewertung an, die als Schwellenwert für die Anzeige von Rollenalerts verwendet werden soll. Je höher die Beziehungsbewertung, umso weniger Rollenalerts und Rollenalertzusammenfassungen werden angezeigt.
4. Geben Sie in **Anzahl Tage, die Alerts angezeigt werden sollen (einschließlich heute)** eine Zahl von 1-99 ein, die angibt, wie viele Tage Alerts angezeigt werden sollen. Die Zahl beginnt mit dem aktuellen Datum und läuft rückwärts; das heißt, wenn Sie 1 eingeben, werden nur Alerts angezeigt, die an dem aktuellen Tag generiert wurden. Wenn Sie 10 eingeben, werden nur Alerts für den Zeitraum von 10 Tagen angezeigt – die des aktuellen Tages und der neun Tage zuvor. Der Standardwert ist 99.
5. Optional: Wenn Ihr Systemadministrator die Schwellenwertüberschreibung in der Konfigurationskonsole aktiviert hat, wird das Kontrollkästchen**Rollenalerts einschließen** angezeigt.
   - Wählen Sie das Kontrollkästchen **Rollenalerts einschließen** aus, um alle Rollenalerts und Rollenalertzusammenfassungen im Fenster **Alertzusammenfassung** anzuzeigen, deren Beziehungsbewertung außerhalb des in der Rollenalertregel definierten Mindestgrenzwerts für Alerts liegt.
   - Nehmen Sie die Auswahl des Kontrollkästchens **Rollenalerts einschließen** zurück, um nur die Rollenalerts und Rollenalertzusammenfassungen im Fenster **Alertzusammenfassung** anzuzeigen, deren Beziehungsbewertung innerhalb des Mindestgrenzwerts für Alerts liegt.

6. Klicken Sie **Übergeben** an. Sie werden mit einer Bestätigungsnachricht informiert, dass Sie Visualizer erneut starten müssen, damit Ihre Änderungen wirksam werden.
7. Klicken Sie in der Bestätigungsnachricht **OK** an.
8. Schließen Sie Ihre Visualizer-Sitzung, starten Sie Visualizer erneut und melden Sie sich erneut an.

Konfigurieren von Visualizer-Protokolloptionen:

Durch Konfigurieren von Visualizer-Protokollierungsoptionen können Sie die Visualizer-Clientprotokollierung aktivieren bzw. inaktivieren. Die Visualizer-Clientprotokollierung ist standardmäßig inaktiviert. Im Allgemeinen aktivieren Sie die Visualizer-Clientprotokollierung nur zur Unterstützung, wenn Sie und Ihr Administrator eine Fehlerbehebung durchführen.

Informationen zu diesem Vorgang

Diese Einstellungen werden für jeden Visualizer-Client konfiguriert. Mit der folgenden Task ändern Sie die Protokollierungsoptionen nur für die Visualizer-Instanz, an der Sie zurzeit angemeldet sind.

Vorgehensweise

1. Klicken Sie in Visualizer **Datei** > **Benutzervorgaben** > **Log Protokoll- und Linkeinstellungen** an.
2. Führen Sie im Kontrollkästchen **Protokollierung aktivieren** eine der folgenden Aktionen aus:
   - Wählen Sie das Kontrollkästchen aus, um die Visualizer-Clientprotokollierung zu aktivieren.
   - Nehmen Sie die Auswahl des Kontrollkästchens zurück, um die Visualizer-Clientprotokollierung zu inaktivieren.
3. Wenn Sie die Protokollierung aktiviert haben, geben Sie durch Auswahl einer Option in **Protokolldetailebene** den Protokollierungstyp an. Wenn Sie sich nicht sicher sind, welche Ebene Sie auswählen sollen, wenden Sie sich an Ihren Systemadministrator. Da die Visualizer-Clientprotokollierung in der Regel nur im Rahmen einer Fehlerbehebung aktiviert wird, wählen Sie in der Regel die Debugstufe aus. Die Debugstufe protokolliert jede Aktion, die Sie in Visualizer ausführen, sowie jede Nachricht (Fehlernachricht, Warnung oder Informationsnachricht), die ausgegeben wird. Bei dieser Protokollstufe wird die Visualizer-Protokolldatei rasch voll, sodass Sie die Datei möglicherweise von Zeit zu Zeit löschen müssen.
4. Im **Verzeichnispfad der Protokolldatei**:
   - Geben Sie den Pfad ein, in dem Visualizer-Protokolldateien gespeichert werden sollen.
   - Oder navigieren Sie zu dem Verzeichnis und wählen Sie es aus.
5. Klicken Sie **Übergeben** an. Sie werden mit einer Bestätigungsnachricht informiert, dass Sie Visualizer erneut starten müssen, damit Ihre Änderungen wirksam werden.
6. Klicken Sie in der Bestätigungsnachricht **OK** an.
7. Schließen Sie Visualizer, starten Sie ihn wieder und melden Sie sich erneut an.

Konfigurieren von Visualizer-Hyperlinkoptionen für die Anzeige von angepassten Attributen:

Wenn in Ihrem Unternehmen Links zu Dateien oder Bildern in anderen System vorhanden sind, die Bestandteil von Identitätsdatensatzattributen sind, kann Visualizer Hyperlinks zu diesen Dateien anzeigen. Sie klicken den Hyperlink an, um Ihren Web-Browser oder Ihre Anwendung zu starten, über den bzw. über die die ausgewählte Datei oder das ausgewählte Bild angezeigt werden soll. Über die Visualizer-Systembenutzervorgaben wählen Sie den Browser bzw. das Programm aus, mit dem die Dateien geöffnet werden, wenn Sie einen Hyperlink anklicken.

Informationen zu diesem Vorgang

Diese Einstellungen werden für jeden Visualizer-Client konfiguriert. Mit der folgenden Task ändern Sie die Hyperlinkoptionen nur für die Visualizer-Instanz, an der Sie zurzeit angemeldet sind.

Vorgehensweise

1. Wählen Sie in Visualizer **Datei** > **Benutzervorgaben** > **Log Protokoll- und Linkeinstellungen** aus.
2. Wählen Sie unter **Einstellungen für Verarbeitung von Hyperlinks** eine der folgenden Optionen aus:
   - **Standardsystembrowser verwenden**
   - Oder **Programm verwenden** und geben Sie einen Browser oder ein Programm an, der bzw. das zum Öffnen von Hyperlinks verwendet werden soll.

   Anmerkung: Sie müssen möglicherweise nur einen Web-Browser oder ein anderes Programm zum Öffnen von Links angeben, die auf sicheren Websites (https://) gespeichert sind.
3. Klicken Sie **Übergeben** an. Sie werden mit einer Bestätigungsnachricht informiert, dass Sie Visualizer erneut starten müssen, damit Ihre Änderungen wirksam werden.
4. Klicken Sie in der Bestätigungsnachricht **OK** an.
5. Schließen Sie Visualizer, starten Sie ihn wieder und melden Sie sich erneut an.

Konfigurieren von Visualizer-Diagrammoptionen:

Sie können die in Visualizer angezeigten Diagrammeinstellungen anpassen, indem Sie die Farbe oder Stärke von Linien auf der Registerkarte **Benutzervorgaben für Diagramme** ändern.

Informationen zu diesem Vorgang

Die Anzeigeeinstellungen für Visualizer-Diagramme werden für jeden Visualizer-Client konfiguriert. Durch Ausführen der folgenden Anweisungen werden nur die Einstellungen für den Visualizer-Client beeinflusst, an dem Sie zurzeit angemeldet sind.

Vorgehensweise

1. Klicken Sie in Visualizer **Datei** > **Benutzervorgaben** > **Graph Benutzervorgaben** an.
2. Wählen Sie die zu verwendende Strichstärke und Farbe aus.

3. Klicken Sie **Übergeben** an. Sie werden mit einer Bestätigungsnachricht informiert, dass Sie Visualizer erneut starten müssen, damit Ihre Änderungen wirksam werden.
4. Klicken Sie in der Bestätigungsnachricht **OK** an.
5. Schließen Sie Visualizer, öffnen Sie ihn wieder und melden Sie sich erneut an.

Ergebnisse

In Visualizer werden Diagramme nun unter Verwendung der neuen, von Ihnen ausgewählten Anzeigeoptionen angezeigt.

Hilfethemen:

Registerkarte 'Fenstervorgaben':

Über diese Registerkarte können Sie die Anzeige der Hintergrundfarben, der Schriftarten und der Navigationssymbole in Visualizer für Ihre Visualizer-Sitzungen konfigurieren. Die Konfiguration von Vorgaben wirkt sich nur auf die Einstellungen für den lokalen Visualizer-Client aus. Wenn Sie diese Einstellungen ändern, müssen Sie Visualizer beenden, erneut öffnen und sich an Visualizer anmelden, um die Änderungen sehen zu können.

Darstellung und Funktionsweise
Wählen Sie eine vordefinierte Gruppe von Anzeigeeinstellungen aus. Die Gruppe der Anzeigeeinstellungen steuert die in den Feldern **Thema**, **Schriftart** und **Größe** verfügbaren Auswahlmöglichkeiten.

Anmerkung: Die meisten Anzeigeeinstellungen lassen keine Auswahl anderer Felder zu. Zurzeit ist **Metal** die einzige Option, bei der weitere Anzeigeeinstellungen ausgewählt werden können.

Die Gruppe der Standardanzeigeeinstellung ist **EAS Visualizer**.

Thema
Wählen Sie eine vordefinierte Anzeigenfarbkombination für die Gruppe der Anzeigeeinstellung, die Sie in **Darstellung und Funktionsweise** ausgewählt haben.

Schriftart
Wählen Sie eine Schriftart für die Anzeige aus.

Größe
Wählen Sie eine Schriftgröße aus.

Beispiel
Zeigt basierend auf Ihren Auswahlen eine Visualizer-Beispielanzeige.

Hintergrundfarbe
Klicken Sie diese Schaltfläche an, um eine Hintergrundfarbe auszuwählen. Dieses Feld ist nur verfügbar, wenn Sie **Metal** im Feld **Darstellung und Funktionsweise** ausgewählt haben.

Steuerelementfarbe
Klicken Sie diese Schaltfläche an, um eine Steuerelementfarbe für den Umriss auszuwählen.

Textfarbe
Klicken Sie diese Schaltfläche an, um eine Textfarbe auszuwählen.

Registerkarte 'Benutzervorgaben für das System':

Über diese Registerkarte können Sie für Ihre Visualizer-Sitzungen Benutzervorgaben für das System konfigurieren. Die Konfiguration von Vorgaben wirkt sich hier nur auf die Systemeinstellungen für Ihren lokalen Visualizer-Client aus. Wenn Sie diese Einstellungen ändern, müssen Sie Visualizer beenden, erneut öffnen und sich an Visualizer anmelden, um die Änderungen sehen zu können.

Abschnitt 'Dateipfade'
Geben Sie die Standarddateipfade an, die Visualizer zum Laden von UMF-Dateien verwendet und öffnen Sie das Diagrammtool 'Centrifuge Desktop'. Wenn Sie die Anwendung 'Centrifuge Desktop' zum Anzeigen von Entitätsdiagrammen und -daten verwenden, geben Sie den vollständigen Pfad der Anwendung ein. Wenn Sie den vollständigen Pfad hier eingeben, haben Sie von Visualizer direkten Zugriff auf Centrifuge.

Abschnitt 'Mindestbewertungswerte'
Definieren Sie die Mindestschwellenwerte für die Ähnlichkeitsbewertung, aus denen Sie beim Erstellen einer auflösungsbasierten Abfrage oder eines Attributalertgenerators eine Auswahl treffen können.

Standardmäßig enthält dieser Abschnitt die empfohlenen Werte für jeden Schwellenwert. Diese empfohlenen Werte stellen konservative Werte dar, die dazu dienen, die Anzahl der zurückgegebenen falschen positiven Werte zu mindern. Sie können die Werte entsprechend Ihrer Ziele neu definieren.

Allgemein gilt Folgendes: Je höher Sie den Wert für einen Mindestbewertungsschwellenwert setzen, desto weniger Ergebnisse werden zurückgegeben. Je niedriger der Wert ist, desto mehr Ergebnisse werden zurückgegeben.

Ist Entität
Geben Sie die niedrigste Auflösungsbewertung ein, die definiert, wann es sich bei der in einer auflösungsbasierten Abfrage oder in einem Attributalertgenerator definierten Suchentität und einer Entität in der Entitätendatenbank um dieselbe Entität handelt.

Der Standardwert ist 100. Für den Standardwert gilt Folgendes: Wenn die Suchentität und eine Identität verglichen werden und die Auflösungsbewertung den Wert 100 aufweist, stimmt die zurückgegebene Entität mit der Suchentität überein.

Starke Entitätsübereinstimmung
Geben Sie die niedrigste Auflösungsbewertung ein, die definiert, wann es sich bei der in einer auflösungsbasierten Abfrage oder in einem Attributalertgenerator definierten Suchentität und einer Entität in der Entitätendatenbank um eine "enge Übereinstimmung" handelt.

Der Standardwert ist 85. Für den Standardwert gilt Folgendes: Wenn die Suchentität und eine Entität aus der Entitätendatenbank verglichen werden und die Mindestauflösungsbewertung größergleich 85 ist, jedoch unter der Bewertung **Ist Entität** liegt, weist die zurückgegebene Entität eine enge Übereinstimmung mit der Suchentität auf.

Gute Beziehung
Geben Sie die niedrigste Bewertung ein, die definiert, wann zwischen der in einer auflösungsbasierten Abfrage oder in einem Attributalertgenerator definierten Suchentität und einer Entität in der

Entitätendatenbank eine enge oder starke Beziehung vorliegt. Der Wert stellt den Umfang der Beziehung dar.

Der Standardwert ist 35. Für den Standardwert gilt Folgendes: Wenn die Suchentität und eine Entität aus der Entitätendatenbank verglichen werden und die Mindestauflösungsbewertung größer-gleich 35 ist, liegt eine gute Beziehung zwischen den beiden Entitäten vor.

Beliebige Beziehung
Geben Sie die niedrigste Bewertung ein, die definiert, wann zwischen der in einer auflösungsbasierten Abfrage oder in einem Attributalertgenerator definierten Suchentität und einer Entität in der Entitätendatenbank eine beliebige Beziehung vorliegt. (Der Wert stellt den Umfang der Beziehung dar.)

Der Standardwert ist 1. Für den Standardwert gilt Folgendes: Wenn die Suchentität und eine Entität aus der Entitätendatenbank verglichen werden und die Mindestauflösungsbewertung größer-gleich 1 ist, liegt eine Beziehung zwischen den beiden Entitäten vor.

Abschnitt 'Filtereinstellungen für Alertanzeige'
In diesem Abschnitt können Sie die Standardfiltereinstellungen für Alerts konfigurieren, die Auswirkungen darauf haben, welche Alertzusammenfassungen im Fenster **Alertzusammenfassung** angezeigt werden. Immer wenn Sie ein neues Fenster **Alertzusammenfassung** öffnen, verwendet das System diese Standardeinstellungen.

Maximale Anzahl in Alertliste anzuzeigender Alerts
Geben Sie eine Nummer ein, die die höchste Anzahl von Alerts angibt, die in der Tabelle **Alertliste** des Fensters **Alertzusammenfassung** angezeigt wird.

Der Standardfilterwert ist 100, d. h., es werden standardmäßig nur die ersten 100 Alerts jeder ausgewählten Alertzusammenfassung angezeigt.

Mindestbeziehungsbewertung
Geben Sie die niedrigste Beziehungsbewertung ein, um nicht zugeordnete Rollenalertzusammenfassungen aus der Anzeige im Fenster **Alertzusammenfassung** zu filtern, deren Wert unter diesem Mindestwert liegen.

Wenn beispielsweise nur Rollenalertzusammenfassungen angezeigt werden sollen, bei denen die Beziehungsbewertung zwischen den zwei verglichenen Entitäten größer-gleich 50 ist, geben Sie `50` in dieses Feld ein.

Der Standardwert ist 0, d. h., es werden standardmäßig alle Alertzusammenfassungen für Ihre Visualizer-Analystengruppe angezeigt, die zurzeit den Status 'Nicht zugeordnet' aufweisen.

Anzahl Tage, die Alerts angezeigt werden sollen (einschließlich heute)
Geben Sie eine Zahl zwischen 1 und 99 ein, die den Zeitraum in Tagen angibt, über den Alerts ab dem aktuellen Datum angezeigt werden sollen. Beachten Sie dabei, dass dieser "Tag" ein vollständiger Kalendertag ist, der um 0:00:00 beginnt und um 23:59:59 endet.

Die Zahl beginnt mit dem aktuellen Datum und es wird zurückgezählt. Wenn Sie Alerts anzeigen wollen, die innerhalb der letzten 90 Tage generiert wurden (aktueller Tag und die 89 vorhergehenden Tage), geben Sie `90` ein.

Der Standardwert ist `99`, d. h., es werden Alerts angezeigt, die heute und an den 98 Kalendertagen vor dem heutigen Tag generiert wurden.

Kontrollkästchen 'Rollenalerts einschließen'
(Optional) Wählen Sie dieses Kontrollkästchen aus, um alle generierten und nicht zugeordneten Rollenalerts anzuzeigen, einschließlich der Alerts, die unter dem Mindestschwellenwert für Alerts liegen, der in der Konfiguration der Rollenalertregeln angegeben ist. Dieses Kontrollkästchen wird nur angezeigt, wenn Ihr Systemadministrator diese Funktion aktiviert hat.

Die Standardauswahl ist gelöscht, d. h., es werden nur die Rollenalerts in Visualizer angezeigt, die zurzeit nicht zugeordnet sind und den für Alerts geltenden Mindestschwellenwert oder einen höheren Wert aufweisen.

Abschnitt 'Sonstige Einstellungen'
In diesem Abschnitt können Sie die Kurzinfo und das Fenster zur Bestätigung der Beendigung aktivieren.

Tooltips aktivieren
Wenn Tooltips aktiviert sind, wird eine Kurzinfo immer dann angezeigt, wenn Sie Ihren Cursor über ein Symbolleistensymbol oder über einen Bereich bewegen, zu dem zusätzliche Informationen bereitstehen. Standardmäßig sind die Tooltips aktiviert.

Dialog zur Bestätigung der Beendigung anzeigen:
Diese Option legt fest, ob das System einen Bestätigungsdialog anzeigt, wenn Sie Visualizer beenden.

- Wählen Sie dieses Kontrollkästchen immer aus, wenn Sie Ihre Entscheidung, Visualizer zu beenden, bestätigen wollen. Standardmäßig ist diese Einstellung ausgewählt.
- Nehmen Sie die Auswahl dieses Kontrollkästchens zurück, wenn Sie Visualizer beenden wollen, ohne dass bei jeder Beendigung und Abmeldung von Visualizer der Dialog zur Bestätigung der Beendigung angezeigt wird.

Registerkarte 'Protokoll- und Linkeinstellungen':

Über diese Registerkarte können Sie die Protokoll- und Hyperlinkeinstellungen für den Visualizer-Client konfigurieren. Die Konfiguration von Vorgaben wirkt sich hier nur auf die Einstellungen für den lokalen Visualizer-Client aus. Wenn Sie diese Einstellungen ändern, müssen Sie Visualizer beenden, erneut öffnen und sich an Visualizer anmelden, um die Änderungen sehen zu können.

Protokolleinstellungen
Wählen Sie das Kontrollkästchen aus, um die Visualizer-Clientprotokollierung zu aktivieren. Nehmen Sie die Auswahl des Kontrollkästchens zurück, wenn Sie die Clientprotokollierung inaktivieren wollen. Die Visualizer-Clientprotokollierung wird in der Regel nur aktiviert, wenn Sie mit Ihrem Systemadministrator an der Behebung der Ursache für eine Fehler-

nachricht oder eines Problems arbeiten, die bzw. das während Ihrer Visualizer-Sitzung aufgetreten ist. Die Visualizer-Clientprotokollierung ist standardmäßig inaktiviert.

Protokolldetailebene
Wählen Sie die Protokolldetailebene aus. Diese Option ist nur verfügbar, wenn die Visualizer-Clientprotokollierung aktiviert ist. Die Detailebene steuert die Menge der Informationen, die im Visualizer-Protokoll während der Verwendung von Visualizer erfasst werden. Fragen Sie Ihren Systemadministrator, bevor Sie eine Auswahl treffen. In der Regel aktivieren Sie die Protokollierung, um ein Problem in Visualizer zu beheben. Sie wählen dabei in der Regel die Debugstufe aus, die der höchsten Protokolldetailebene entspricht. Bei der Debugstufe werden alle Aktionen und Nachrichten protokolliert, die während der Verwendung von Visualizer auftreten. Diese Protokollebene füllt jedoch auch die Protokolldatei für den Visualizer-Client sehr schnell, sodass Sie möglicherweise ihren Inhalt gelegentlich löschen müssen. Aus diesem Grund inaktivieren Sie normalerweise die Protokollierung, wenn das Problem behoben ist.

Verzeichnispfad der Protokolldatei
Geben Sie die Datei und die Verzeichnisposition der Protokolldateien für den Visualizer-Client an. In der Regel müssen Sie Protokolldateien nur prüfen, wenn Sie die Ursache für eine Fehlernachricht oder ein Problem beheben wollen. Protokolldateien können schnell mit Informationen gefüllt sein, insbesondere bei aktivierter Debugstufe. Wenn die Visualizer-Clientprotokollierung aktiviert ist, müssen Sie möglicherweise die Protokolldateien gelegentlich bereinigen, damit die Dateien nicht allzu groß werden.

Einstellungen für Verarbeitung von Hyperlinks
Wählen Sie eine Option aus, um zu ermitteln, welches Programm oder welcher Browser von Visualizer zum Öffnen und Anzeigen von Hyperlinks verwendet wird. Eingehende Identitätsdatensätze können Hyperlinks enthalten, die auf andere Dateien, Websites oder Systeme führen, die für Ihre Analyse relevante Identitäts- oder Entitätsinformationen enthalten. Hyperlinks gehören zum Identitätsdatensatz und werden in der Entitätszusammenfassung und im Entitätsauflösungsdiagramm als Attribute angezeigt.

Wenn Sie Probleme beim Anklicken eines Hyperlinks haben oder dies zu einem Fehler führt, wählen Sie die Option **Programm verwenden** aus und geben Sie an, welcher Browser oder welches Programm zum Öffnen von Hyperlinks verwendet werden soll. Wenn Ihr Unternehmen beispielsweise Dateien mit elektronischen Fingerabdrücken auf einer sicheren Website speichert (https://), verwenden Sie diese Option, um Ihren Web-Browser oder ein anderes Programm zum Öffnen von Links anzugeben, die auf die sichere Website mit den Fingerabdruckdateien führen.

Registerkarte 'Benutzervorgaben für Diagramme':

Geben Sie auf dieser Registerkarte die Anzeigeeigenschaften für die Linien an, die Entitäten in Visualizer-Diagrammen verbinden. Die Konfiguration von Vorgaben wirkt sich hier nur auf die Einstellungen für den lokalen Visualizer-Client aus. Wenn Sie diese Einstellungen ändern, müssen Sie Visualizer beenden, erneut öffnen und sich daran anmelden, um die Änderungen sehen zu können.

Linienstärke
Wählen Sie eine Linienstärke aus. Die Standardlinienstärke beträgt 2 Pixel.

Linienfarbe
Wählen Sie eine Linienfarbe aus. Die Standardlinienfarbe ist mittelblau.

Beispiellinie
Zeigt basierend auf Ihrer Auswahl eine Beispiellinie im Diagramm an.

Starten von Visualizer

Bevor Sie Entitäten und Entitätsdaten aus der Entitätendatenbank in Visualizer anzeigen zu können, müssen Sie zuerst Visualizer starten und sich anmelden.

Die Standardsystemversion von Java verarbeitet beim Starten von Visualizer eine JNLP-Datei (Java Network Launch Protocol) von Java Web Start, die der Produktanwendungsserver auf Ihren Workstation-Client herunterlädt. Es gibt viele Möglichkeiten des Zugriffs auf die JNLP-Datei. Um Visualizer jedoch erfolgreich öffnen zu können, muss die erforderliche Clientversion von Java Web Start die JNLP-Datei öffnen.

Wenn Sie mehrere Versionen von Java auf Ihrer Clientmaschine installiert haben, könnte die Standardsystemversion von Java Web Start auf eine andere als die erforderliche Clientversion gesetzt sein. Sie können Visualizer weiterhin erfolgreich öffnen und ausführen, müssen jedoch zuerst Ihren Web-Browser konfigurieren, um die erforderliche Clientversion von Java Web Start verwenden zu können.

Anmerkung: Die für das Öffnen und Ausführen von Visualizer erforderliche Clientversion von Java ist möglicherweise nicht die neueste Version von Java.

Anmelden an Visualizer

Sie müssen über ein Visualizer-Benutzerkonto (Benutzername und Kennwort) verfügen, bevor Sie sich an Visualizer anmelden. Ihr Systemadministrator kann Ihnen die Informationen zu Ihrem Visualizer-Benutzerkonto bereitstellen.

Vorgehensweise

1. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie das Visualizer-Symbol auf Ihrer Arbeitsoberfläche doppelt an.
   - Oder öffnen Sie Ihren Internet-Browser und geben Sie die URL (Uniform Resource Locator) für Visualizer in die Adresszeile ein.

   Die URL zum Starten von Visualizer lautet:

   `http://server:installationsport`

   Beispiel: `http://localhost:13510`. Wenn Visualizer installiert ist, ist der *installationsport* standardmäßig 13510, die Portnummer kann jedoch geändert werden. Setzen Sie sich mit Ihrem Systemadministrator in Verbindung, wenn Sie sich bezüglich des richtigen Servernamens oder der richtigen Portnummer nicht sicher sind.
2. Melden Sie sich an, indem Sie Ihren Benutzernamen und Ihr Kennwort eingeben.

   Anmerkung: Bei den Feldern für den Benutzernamen und das Kennwort muss die Groß-/Kleinschreibung beachtet werden. Verwenden Sie bei Ihrer ersten Anmeldung das Kennwort, das Ihnen Ihr Systemadministrator zugewiesen hat. Nach der ersten erfolgreichen Anmeldung ändern Sie normalerweise Ihr Visualizer-Kennwort, um die Sicherheit Ihres Visualizer-Benutzerkontos zu wahren.
3. Klicken Sie **Anmelden** an.

Einrichten des Web-Browsers für Verwendung der erforderlichen Clientversion von Java Web Start:

Wenn Ihre Workstation mehrere Versionen von Java enthält und Sie Probleme beim Öffnen von Visualizer haben, richten Sie Ihre Web-Browser-Vorgaben so ein, dass die erforderliche Clientversion von Java Web Start ausgewählt wird. Dadurch verwendet Ihr Web-Browser automatisch die erforderliche Clientversion von Java Web Start und Sie können Visualizer immer erfolgreich öffnen.

Konfigurieren von Microsoft Windows Internet Explorer für Verwendung der erforderlichen Java Web Start-Version:

Microsoft Internet Explorer verwendet die für das Microsoft Windows-Betriebssystem definierten Standarddateizuordnungen, um zu bestimmen, wie JNLP-Dateien (Java Network Launch Protocol) zu verarbeiten sind. Durch Definieren oder Modifizieren der für die Verarbeitung von JNLP-Dateien zugeordneten Standarddateianwendung können Sie Internet Explorer auf die richtige, zu verwendende Java Web Start-Version verweisen. Sind mehrere Java-Versionen installiert, können durch Modifizieren dieser Einstellung Probleme beim Öffnen von Visualizer verhindert werden.

Informationen zu diesem Vorgang

Mit der folgenden Prozedur wird Internet Explorer angewiesen, die Java Web Start-Version beim Öffnen aller Webanwendungen zu verwenden. Wenn Sie andere Java Web Start-Anwendungen ausführen, die neuere Java-Versionen erfordern, verwenden Sie stattdessen die Direktstartmethode.

Anmerkung: Bei Java Version 1.6 gibt es folgende bekannte Probleme zu beachten:

- Java Version 1.6 überschreibt zuweilen die Windows-Standarddateizuordnung für JNLP-Dateien. Wenn Sie Java Version 1.6 als System-JVM (Java Virtual Machine) verwenden und es Ihnen auch nach Durchführen der folgenden Schritte nicht möglich ist, Visualizer erfolgreich zu starten und zu öffnen, verwenden Sie entweder einen anderen Web-Browser zum Starten von Visualizer oder verwenden Sie stattdessen die Direktstartmethode.
- Wenn Ihre Workstation Java Version 1.6 verwendet, müssen Sie möglicherweise auch Ihre JRE (Java Runtime Environment) entsprechend konfigurieren, dass automatische Downloads akzeptiert werden. Tritt dieses Problem bei Ihrer Workstation auf, wenn Sie versuchen, Visualizer zu starten, informiert Sie eine Fehlernachricht darüber, dass die Anwendung eine JRE-Version angefordert hat, die nicht lokal installiert ist.

Vorgehensweise

1. Führen Sie über die Systemsteuerung von Windows einen der folgenden Schritte aus:
   - Klicken Sie **Leistung und Wartung** in der Kategoriesicht doppelt an. Wählen Sie **Dateitypen** im Navigationsteilfenster **Siehe auch** links oben im Fenster aus.
   - Klicken Sie **Ordneroptionen** in der klassischen Sicht doppelt an.
2. Klicken Sie im Dialog **Ordneroptionen** die Registerkarte **Dateitypen** an.
3. Navigieren Sie unter der Spalte **Erweiterungen** zum Eintrag **JNLP** und wählen Sie diesen aus. Die Einträge sind alphabetisch nach der Erweiterung sortiert.

Anmerkung: Ist der JNLP-Eintrag nicht vorhanden, klicken Sie **Neu** an, um den Eintrag zu erstellen.

4. Klicken Sie **Ändern** an.
5. Vergewissern Sie sich, dass **Java WebStart Executable** im Dialog **Öffnen mit** ausgewählt ist. Klicken Sie **Durchsuchen** an, um zu Ihrem installierten Java-Verzeichnis zu navigieren.
6. Wählen Sie die ausführbare Datei mit dem Namen `javaws` aus und klicken Sie **OK** an.
7. Klicken Sie **OK** an, um den Dialog **Ordneroptionen** zu schließen. (Sie können auch das Fenster **Systemsteuerung** schließen.)

Ergebnisse

Internet Explorer verwendet nun die zugeordnete Java Web Start-Datei, sodass Visualizer erfolgreich verarbeitet und geöffnet werden kann.

Konfigurieren von Mozilla Firefox für Verwendung der erforderlichen Java Web Start-Version:

Durch Einstellen oder Modifizieren der Art und Weise, wie Mozilla Firefox JNLP-Dateien (JNLP - Java Network Launch Protocol) verarbeitet, können Sie Firefox anweisen, beim Starten von Visualizer automatisch die erforderliche Java Web Start-Clientversion zu verwenden. Sind mehrere Java-Versionen installiert, können durch Modifizieren dieser Einstellung Probleme beim Öffnen von Visualizer verhindert werden.

Informationen zu diesem Vorgang

Mit der folgenden Prozedur wird Firefox angewiesen, die Java Web Start-Version beim Öffnen aller Webanwendungen zu verwenden. Wenn Sie andere Java Web Start-Anwendungen ausführen, die neuere Java-Versionen erfordern, verwenden Sie stattdessen die Direktstartmethode.

Vorgehensweise

1. Starten Sie Mozilla Firefox.
2. Wählen Sie **Extras** > **Einstellungen** aus.
3. Wählen Sie **Anwendungen** aus.
4. Navigieren Sie unter **Dateityp** zu dem Eintrag für die JNLP-Datei.

   Anmerkung: Wenn kein Eintrag für JNLP-Dateien vorhanden ist, schließen Sie den Dialog **Einstellungen**. Versuchen Sie Visualizer über die Visualizer Web Start-Seite zu starten, indem Sie den Link **Klicken Sie hier, um IBM Identity Insight Visualizer zu starten** anklicken. Beginnen Sie daraufhin wieder bei Schritt 1.
5. Wählen Sie den Eintrag für JNLP-Dateien aus.
6. Wählen Sie unter **Aktion** die Option **Andere Anwendung** aus.
7. Klicken Sie **Durchsuchen**im Dialog **Hilfsanwendung wählen** an, navigieren Sie zu dem Verzeichnis, in dem die erforderliche Java-Clientversion installiert ist und wählen Sie die ausführbare Datei `javaws` aus.
8. Klicken Sie **OK** an, um den Dialog **Hilfsanwendung wählen** zu schließen.
9. Klicken Sie **OK** an, um den Dialog **Einstelllungen** zu schließen.

Ergebnisse

Mozilla Firefox verwendet nun die ausgewählte Java Web Start-Datei zur Verarbeitung aller JNLP-Dateitypen. Visualizer wird erfolgreich geöffnet.

Starten von Visualizer direkt über die ausführbare Java Web Start-Datei:

Wenn Sie Visualizer starten wollen, ohne Java-Einstellungen oder andere Systemeinstellungen zu ändern, können Sie dies über die Direktstartmethode tun. Bei dieser Methode startet Visualizer direkt über die ausführbare Java Web Start-Datei. Die Verwendung der Direktstartmethode ist zu empfehlen, wenn auf Ihrer Workstation mehrere Java-Versionen installiert sind und Sie neben Visualizer noch andere Web Start-Anwendungen verwenden.

Vorbereitende Schritte

Navigieren Sie zu dem Pfad, in dem sich die erforderliche ausführbare Java Web Start-Datei (`javaws`) auf Ihrer Workstation befindet.

Informationen zu diesem Vorgang

Sie können auf Ihrem Desktop auch eine Verknüpfung zu der ausführbaren Java Web Start-Datei erstellen. Wählen Sie hierzu die Datei `javaws` aus und geben Sie die URL zu Visualizer in das Feld für das Ziel ein.

Vorgehensweise

1. Öffnen Sie über Ihren Desktop ein DOS-Befehlsfenster.
2. Geben Sie in die Befehlszeile den folgenden Direktstartbefehl ein:
   java-installationspfadpfad_zur_javaws_exe-datei>javaws.exe *visualizer-URL* Beispiel: **C:/IBM/Java60/jre/bin>javaws.exe http://localhost:13510/docs/rrmdi.jnlp**

   Wichtig: Beachten Sie das Leerzeichen zwischen der ausführbaren Java Web Start-Dateierweiterung und der URL.

Ergebnisse

Visualizer wird erfolgreich geöffnet.

Konfigurieren von Java Version 1.6 für das Ausführen von Visualizer auf Microsoft Windows-Workstations:

Wenn beim Starten von Visualizer eine Fehlernachricht angezeigt wird, die darauf hinweist, dass die Anwendung eine Version von JRE angefordert hat, die nicht lokal installiert ist, versuchen Sie, die automatischen Download-Einstellungen für Java zu ändern. Diese Fehlernachricht ist ein bekanntes Problem bei Microsoft Windows-Workstations, auf denen Java Version 1.6 installiert ist.

Vorgehensweise

1. Wählen Sie in der **Windows-Systemsteuerung** eine der folgenden Optionen aus:
   - Bei IBM Installation von Java wählen Sie **IBM Control Panel for Java** aus.
   - Bei Sun-Installation von Java wählen Sie **Java** aus.
2. Erweitern Sie auf der Registerkarte **Erweitert** die Einstellung **Automatischer JRE-Download**. Wird diese Option nicht angezeigt und sind auf dieser Work-

station mehrere Versionen von Java installiert, schließen Sie die **Java-Systemsteuerung** und wählen Sie den anderen Eintrag aus.

3. Stellen Sie sicher, dass für die Einstellung **Automatischer JRE-Download** entweder **Immer automatisch herunterladen** (empfohlen) oder **Benutzer fragen** festgelegt ist. Die Einstellung **Nie automatisch herunterladen** verhindert das Öffnen der Visualizer- und Konfigurationskonsole.
4. Klicken Sie **Anwenden** an.
5. Klicken Sie **OK** an.
6. Schließen Sie das Fenster **Systemsteuerung**.

Schließen von Visualizer

Wenn Sie Ihre Arbeit mit Visualizer beendet haben, schließen Sie die Anwendung. Beim Schließen von Visualizer melden Sie sich gleichzeitig ab. Wenn Sie ein Pause machen und Ihre Workstation lediglich für einige Minuten sichern wollen, können Sie Visualizer auch sperren.

Vorgehensweise

Gehen Sie wie folgt vor, um Visualizer zu schließen und sich abzumelden:

- Wählen Sie **Datei** > **Beenden** aus.
- Oder drücken Sie **Strg** + **Q**.

Sperren von Visualizer

Wenn Sie eine kurze Pause einlegen oder sich einige Minuten von Ihrer Workstation entfernen wollen, müssen Sie Visualizer nicht notwendigerweise schließen und sich abmelden, sondern können Visualizer stattdessen auch sperren. Das Sperren von Visualizer entspricht einem gesicherten Bildschirmschoner und schützt so Ihre Arbeit. Wenn Sie Visualizer sperren, wird das Fenster **Anmelden** angezeigt. In Ihre Visualizer-Sitzung gelangen Sie wieder durch Eingabe Ihres Benutzerkennworts.

Vorgehensweise

Gehen Sie wie folgt vor, um Visualizer zu sperren:

- Wählen Sie **Datei** > **Anwendung sperren** aus.
- Oder drücken Sie **Strg** + **L**.

Ergebnisse

Ihre Visualizer-Sitzung ist jetzt sicher gesperrt.

Nächste Schritte

Wenn Sie Ihre Arbeit mit Visualizer wieder aufnehmen wollen, geben Sie Ihr Kennwort ein und klicken Sie **Entsperren** an.

Ändern des Visualizer-Kennworts

Durch regelmäßiges Ändern des Visualizer-Kennworts gewährleisten Sie die Sicherheit Ihres Visualizer-Benutzerkontos.

Vorbereitende Schritte

Sie müssen an Visualizer angemeldet sein, um Ihr Kennwort zu ändern.

Informationen zu diesem Vorgang

Visualizer-Kennwörter müssen nicht eine Mindestanzahl von Zeichen aufweisen. Sie können jede beliebige Kombination von Buchstaben (in Großbuchstaben oder in Kleinbuchstaben), Sonderzeichen und Zahlen verwenden. Beim Kennwort muss die Groß-/Kleinschreibung beachtet werden. Das heißt, wenn Sie sich anmelden, muss das von Ihnen eingegebene Kennwort exakt mit Ihrem Visualizer-Benutzerkontokennwort übereinstimmen. Wenn Ihr Kennwort beispielsweise `PASSw0rd` lautet, Sie aber versuchen sich mit `passw0rd` anzumelden, stimmen die Kennwörter nicht überein und das System zeigt eine Fehlernachricht an.

Vorgehensweise

1. Klicken Sie in Visualizer **Datei** > **Kennwort ändern** an.
2. Geben Sie in **Aktuelles Kennwort** das Kennwort ein, mit dem Sie sich an dieser Visualizer-Sitzung angemeldet haben. Wenn Ihnen ein Kennwort zugeordnet oder dieses zurückgesetzt wurde, entspricht dieses Kennwort dem Kennwort von Ihrem Systemadministrator.
3. Geben Sie in **Neues Kennwort** das neue Kennwort ein, das Sie als Visualizer-Kennwort verwenden wollen.
4. Geben Sie in **Neues Kennwort wiederholen** das Kennwort, das Sie eben in **Neues Kennwort** eingeben haben, nochmals ein.
5. Klicken Sie **Kennwort ändern** an.

Ergebnisse

- Sind die Einträge in **Neues Kennwort** und in **Neues Kennwort wiederholen** identisch, zeigt das System eine Nachricht an, die angibt, dass Ihr Kennwort geändert wurde. Klicken Sie **OK** an. Verwenden Sie Ihr neues Kennwort, wenn Sie sich das nächste Mal an Visualizer anmelden.
- Stimmen die Einträge nicht überein, zeigt das System eine Fehlernachricht an, die darauf hinweist, dass die neuen Kennwörter nicht übereinstimmen. Klicken Sie **OK** an. Ihr Kennwort wurde nicht geändert. Zum Ändern des Kennworts beginnen Sie nochmals ab Schritt 2.

Analysieren von Alerts in Visualizer

Die Auswertung von Alerts stellt eine der häufigsten Tasks dar, die von Visualizer-Benutzern ausgeführt wird, um zu entscheiden, welche Alerts geprüft und welche an andere Visualizer-Gruppen übertragen werden sollen.

Alerts werden im Fenster **Alertzusammenfassung** von Visualizer angezeigt. Dieses Fenster stellt den Ausgangspunkt für die Auswertung, Zuordnung oder Übertragung und Überprüfung von Alerts dar.

Alerts sind in Alertzusammenfassungen gruppiert. Alertzusammenfassungen enthalten alle Alerts eines Alerttyps mit den folgenden Merkmalen: Beschreibung, Alertwertigkeit, Status, Auflösungsregel, Beziehungsbewertung und Auflösungs-(ähnlichkeits)bewertung. Eine Alertzusammenfassung enthält in der Regel mehrere einzelne Alerts, von denen jeder geprüft und analysiert werden muss. Ein Teil der Prüfung umfasst die Zuordnung einer Disposition zum Alert, damit Ihnen und anderen Visualizer-Benutzern der Status der Analyse und Kommentare zu den Suchergebnissen angezeigt werden.

Beachten Sie, dass im Fenster **Alertzusammenfassung** lediglich Folgendes angezeigt wird:

- Alertzusammenfassungen für Ihre Visualizer-Analystengruppe, die nicht zugeordnete Alerts enthalten
- Alerts, die Sie bereits sich selbst zugeordnet haben

Ihnen werden keine Alerts angezeigt, die andere Analysten in Ihrer Visualizer-Analystengruppe sich selbst zugeordnet haben. Ferner werden Ihnen auch keine Alerts angezeigt, die anderen Visualizer-Analystengruppen zugeordnet sind.

Auswerten von Alertzusammenfassungen

Wie entscheiden Sie, welche Alerts Sie sich selbst für die Analyse zuordnen? Beginnen Sie mit der Prüfung der Alertzusammenfassungen im Fenster **Alertzusammenfassung**. Vergleichen Sie den Stellenwert der Informationen, aus denen die Alertzusammenfassung besteht, mit Ihren Analysezielen. Möglicherweise müssen Sie eine oder mehrere Alertangaben auswerten, bevor Sie eine Entscheidung treffen können.

Tipps zur Vergabe von Prioritäten für die Alertzusammenfassungen:

- **Alertwertigkeit:** Beginnen Sie mit dem Sortieren der Alertzusammenfassungen nach Wertigkeit. Klicken Sie die Spaltenüberschrift **Alertwertigkeit** an. Diese Informationen sind möglicherweise ausreichend für die Entscheidung, welche Alerts am kritischsten oder wichtigsten sind und daher eine Analyse erfordern. Wenn Ihr Unternehmen beispielsweise "C" für Alerts mit einer kritischen Wertigkeit verwendet, können Sie unverzüglich erkennen, welche Alerts kritisch sind, indem Sie ihre Wertigkeit prüfen.
- **Alertbeschreibung:** Die Wertigkeit allein ist jedoch möglicherweise nicht ausreichend. Die Alertbeschreibung kann Sie bei der Entscheidung unterstützen, welche Alerts in der Prioritätenliste eine höhere Priorität aufweisen, wenn mehrere Alertzusammenfassungen mit derselben Alertwertigkeit vorliegen. Es ist möglicherweise wichtiger, Alerts zu analysieren, die nach der Beschreibung "Passagier in No-Fly-Liste enthalten" gruppiert sind, als Alerts mit der Beschreibung "Passagier kennt Arbeitnehmer".
- **Ähnlichkeitsbewertung** und **Beziehungsbewertung:** Je höher die Bewertungen, desto wahrscheinlicher ist es, dass eine relevante Beziehung vorhanden ist, oder dass die Identität die Entität ist. Wenn im Beispiel "Passagier in No-Fly-Liste enthalten" sowohl die Ähnlichkeits- als auch die Beziehungsbewertung 100 beträgt, ist die Person auf der No-Fly-Liste mit dem Passagier identisch und Sie wollen möglicherweise sofort entsprechende Maßnahmen einleiten. Wenn die Ähnlichkeitsbewertung dagegen unter 70 und die Beziehungsbewertung unter 85 liegt, kann dieser Alert zwar noch wichtig sein, aber nicht mehr kritisch. Sie wollen möglicherweise weiterhin die am Alert beteiligten Entitäten analysieren, halten jedoch eine sofortige Maßnahme nicht für erforderlich.

Als Visualizer-Benutzer sind Sie mit den Zielen Ihres Unternehmens vertraut und können wahrscheinlich Ihre eigenen Faktoren hinzufügen, die bei der Vergabe von Prioritäten für Alerts verwendet werden sollen. Diese Tipps helfen Ihnen bei der Ausführung der ersten Schritte.

Zuordnen von Alerts

Wenn Sie auf Basis der Priorität entschieden haben, mit welchen Alerts Sie arbeiten wollen, können Sie diese Alerts sich selbst zuordnen. Durch das Zuordnen von Alerts kann Ihre Visualizer-Analystengruppe die Liste der eingehenden Alerts aufteilen und bearbeiten. Wenn Ihnen ein Alert zugeordnet ist, wird dieser nur in Ihrem Fenster **Alertzusammenfassung** angezeigt, wodurch verhindert wird, dass ein anderer Visualizer-Benutzer denselben Alert bearbeitet. Sie können unverzüglich sehen, welche Alerts Sie zurzeit alleine prüfen.

Wenn in Ihrem Fenster **Alertzusammenfassung** mindestens ein Alert angezeigt wird, der Ihrer Meinung nach zu einer anderen Visualizer-Analystengruppe gehören könnte, können Sie den bzw. die betreffenden Alerts übertragen. Beispiel: Sie arbeiten als Sachbearbeiter für Buchungen und werten die durch neue oder geänderte Buchungen generierten Alerts aus. Es wird ein Alert aufgelistet, der vom Sicherheitsdienst bearbeitet wird. Sie können diesen Alert der Sicherheitsgruppe zuordnen, da er in ihren Zuständigkeitsbereich fällt.

Prüfung und Disposition von Alerts ausführen

Wenn Sie sich selbst mindestens einen Alert zuordnen, können Sie mit dem Untersuchen und Analysieren dieser Alerts beginnen. Visualizer vereinfacht die Task im Prüffenster, in dem alle relevanten zugeordneten Informationen zum Alert in nur einem Fenster angezeigt werden. Im Prüffenster können Sie die folgenden Tasks im Rahmen Ihrer Analyse ausführen:

- Prüfen der Alertdetails
- Überprüfen der Entitätszusammenfassungen der zusammengehörigen Entitäten
- Anzeigen der zugeordneten Entitäts- oder Alertdiagramme, um die Gemeinsamkeiten der Entitäten oder Attribute anzuzeigen und zu untersuchen, die Teil des Alerts darstellen
- Hinzufügen von Kommentaren, die die Suchergebnisse Ihrer Analyse angeben
- Ändern des Status (bzw. der Statusdisposition) des Alerts während der Analyse

Attributalerts

Attributalerts sind Alerts, die von Attributalertgeneratoren erzeugt werden, welche eine permanente Systemabfrage erstellen, von der nach bestimmten Attributen oder Identitäten in der Entitätendatenbank gesucht wird. Sobald Attribute für Entitäten den Kriterien des Attributalertgenerators entsprechen, erzeugt das System einen Attributalert.

Visualizer-Benutzer erstellen ihre eigenen, persönlichen Attributalertgeneratoren. Wenn Sie nach einer bestimmten Identität oder Identitäten oder Entitäten, die einer bestimmten Gruppe von Attributen entsprechen, suchen, können Sie einen eigenen, persönlichen Attributalertgenerator erstellen, der bis zum angegebenen Ablaufdatum nach Übereinstimmungen sucht.

Beispiele für Entitätsattribute, für die Sie eventuell eine Benachrichtigung erhalten wollen:

- Name und eindeutige Nummer (z. B. eine Kreditkartennummer)
- Name und Telefonnummer
- Adresse
- Name und nicht eindeutige Nummer

Attributalertgeneratoren werden in Visualizer konfiguriert und können dort angezeigt werden. Die von Ihnen erstellten Attributalertgeneratoren sind nur für Sie verfügbar.

Beispiel für einen Adressattributalert

Sie überwachen die Adresse 675 Hickory Street Las Vegas, NV. Sie können einen Attributalertgenerator so konfigurieren, dass ein Attributalert erzeugt wird, wenn diese Adresse einem eingehenden Identitätsdatensatz zugeordnet wird, der der Entitätendatenbank hinzugefügt wird.

Ereignisalerts

Ein Ereignisalert tritt auf, wenn mindestens ein Ereignis festgelegte Kriterien über einen angegebenen Zeitraum erfüllt. Ereignisalerts basieren auf komplexen Ereignisgeschäftsregeln und weiteren, in einer Ereignisregeldatei (`cep.xml`) enthaltenen Konfigurationen. Diese Alerts können interessante Situationen aufzeigen, z. B. dass in der letzten Stunde zwei oder mehr Kauftransaktionen über mehr als 10.000 Euro an Orten, die 200 Kilometer voneinander entfernt sind, aufgetreten sind.

Rollenalerts

Ein Rollenalert gibt an, dass eine oder zwei über eine Beziehung verknüpfte Entitäten eine konfigurierte Rollenalertregel erfüllen oder übererfüllen. Rollenalerts basieren auf konfigurierten Rollen und Rollenalertregeln. Sie zeigen eine Warnung oder ein Problem (z. B. dass ein Kunde eine potenziell gefährliche Person kennt) oder einfach interessante Beziehungen (z. B. dass ein Kunde einen Mitarbeiter kennt) an.

Sie geben für Beziehungen an, dass sie *von Interesse* sind oder einen *Konflikt* darstellen, indem Sie Rollenalertregeln konfigurieren, die angeben, welche Rollen nicht in einer einzelnen Entität vorhanden sein sollen oder nicht zwischen einer oder mehreren Entität(en) verknüpft sein können. Sie können mit der Konfigurationskonsole Rollenalertfilter konfigurieren, die festlegen, ob das System neue Alerts generiert, wenn neue Informationen vorliegen (beispielsweise eine neue Identität oder ein neuer Datenquellencode).

Während der Entitätsauflösung wertet die Pipeline Beziehungen zwischen der eingehenden Identität und Entitäten in der Kandidatenliste aus. Nach der Feststellung einer Beziehung zwischen der eingehenden Identität und einer Kandidatenentität wertet das System aus, ob die zugeordneten Rollen einer konfigurierten Rollenalertregel entsprechen. Wenn das der Fall ist, generiert das System einen Rollenalert.

Ein Rollenalert stellt Entitätsdaten zum Zeitpunkt der Rollenalerterstellung fest. In der Anzeige **Rollenalert-Detail** werden die Entitätsdaten so gezeigt, wie sie bei der Erstellung des Rollenalerts existierten. Da sich Entitätsdaten im Laufe der Zeit ändern, enthält die Entitätszusammenfassung die letzten Entitätsdaten. Wenn Sie die aktuellen Daten für eine bestimmte Entität anzeigen wollen, rufen Sie die Entitätszusammenfassung auf.

Sie können in den Komponenten von Analyst's Toolkit (Cognos-Berichte, Identity Insight-Plug-in für i2 und Identity Insight Explorer) Rollenalerts anzeigen und mit ihnen arbeiten.

Anzeigen von Alerts

Bei der Anzeige von Alerts im Fenster **Alertzusammenfassung** können Sie entscheiden, welche Alerts analysiert und Ihnen selbst zugeordnet oder an eine andere Visualizer-Analystengruppe übertragen werden sollen. Dann können Sie beginnen, für die Alerts Untersuchungen und Dispositionen vorzunehmen, die Sie sich selbst zugeordnet haben.

Informationen zu diesem Vorgang

Zu den Alerts, die in Ihrem Fenster **Alertzusammenfassung** angezeigt werden, zählen folgende:

- Alerts, die Sie sich selbst zur Analyse zugeordnet haben.
- Nicht zugeordnete Alerts für Ihre Visualizer-Analystengruppe

- Attributalerts, die von einem Ihrer Attributalertgeneratoren generiert wurden

Die Zusammenfassungen nicht zugeordneter Alerts werden auf der Basis der Standardfilterwerte für die Alertanzeige des Fensters **Alertzusammenfassung** gefiltert, die auf der Registerkarte **Benutzervorgaben für das System** des Fensters **Benutzervorgaben für die Anzeige konfigurieren** konfiguriert werden. Sie können Werte für Alertanzeigefilter im Gruppenfeld **Filter anzeigen** ändern.

Vorgehensweise

1. Wählen Sie **Anzeigen** > **Alertzusammenfassung**.
2. Wählen Sie dann den Alerttyp, den Sie anzeigen wollen, oder **Alle Alerttypen anzeigen**.

Ergebnisse

Vom Fenster **Alertzusammenfassung** aus können Sie entscheiden, mit welchen Alerts Sie arbeiten wollen. Sie können sich selbst Alerts zuordnen oder Alerts an eine andere Visualizer-Analystengruppe übertragen. Sie können die Alerts, die Sie sich selbst zugeordnet haben, analysieren und Kommentare zu Ihrer Analyse hinzufügen.

Filtern der Alertanzeige im Fenster 'Alertzusammenfassung'

Wenn Sie Alerts im Fenster **Alertzusammenfassung** prüfen, können Sie filtern, welche Alertzusammenfassungen angezeigt werden, indem Sie die Werte im Gruppenfeld **Filter anzeigen** ändern. Die Anzeigefilter wirken sich nur auf Alertzusammenfassungen aus, die gegenwärtig den Status 'Nicht Zugeordnet' aufweisen.

Informationen zu diesem Vorgang

Die Standardwerte für diese Alertfilter werden auf der Registerkarte **Benutzervorgaben für das System** des Fensters **Benutzervorgaben für die Anzeige konfigurieren** konfiguriert. Wenn Sie die Alertanzeigefilter im Fenster **Alertzusammenfassung** ändern, überschreiben Sie diese Standardwerte vorübergehend. Wenn Sie das nächste Mal ein neues Fenster **Alertzusammenfassung** öffnen, werden die Filter wieder auf ihre Standardwerte zurückgesetzt.

Vorgehensweise

1. Öffnen Sie im Fenster **Alertzusammenfassung** das Gruppenfeldtwistie **Filter anzeigen**.
2. Nehmen Sie Ihre Änderungen an einem oder mehreren der Alertanzeigefilter vor.
3. Klicken Sie **Anwenden** an, um das Fenster **Alertzusammenfassung** zu aktualisieren und wenden Sie Ihre angegebenen Alertfilter an.

Zuordnen von Alerts zu sich selbst

Durch Zuordnen eines Alerts zu sich selbst übernehmen Sie das Eigentumsrecht zum Überprüfen, Untersuchen und Dispositionieren für diesen Alert. Nachdem Sie einen Alert sich selbst zugeordnet haben, wird dieser nur in Ihrem Fenster **Alertzusammenfassung** angezeigt, was es Ihnen erleichtert, Ihre Alerts zu identifizieren.

Vorgehensweise

1. Klicken Sie in Visualizer im Fenster **Alertzusammenfassung** in der Tabelle **Alertzusammenfassung** eine Zusammenfassung nicht zugeordneter Alerts an. Die Alertzusammenfassung enthält mindestens einen Alert. Wenn mehrere

Alerts aufgelistet werden, sind diese nach Alerttyp zusammengefasst und haben dieselben Werte für Beschreibung, Status, Auflösungsregel, Ähnlichkeitsbewertung und Beziehungsbewertung.

2. Klicken Sie in der Tabelle mit der Alertliste den an sich zu übertragenden Alert doppelt an.
3. Klicken Sie im Prüffenster **Status festlegen** an.
4. Führen Sie in **Status festlegen** Folgendes aus:
   a. Wählen Sie **Status festlegen**, in **Auszuführende Aktion auswählen** aus. Ein entsprechender Aktivitätscode wird in **Aktivitätscode auswählen** angezeigt.
   b. Erforderlich: Wählen Sie **Zugeordnet** in **Status auswählen** aus. Wenn Sie einen anderen Status auswählen, wird Ihnen der Alert nicht zugeordnet.
   c. Optional: Zum Zuordnen eines anderen Aktivitätscodes wählen Sie diesen in **Aktivitätscode auswählen** aus. Wird der Aktivitätscode nicht angezeigt, den Sie auswählen wollen, bitten Sie Ihren Systemadministrator, diesen Aktivitätscode zu konfigurieren.
   d. Geben Sie Kommentare oder Hinweise in das Textfeld **Kommentare** ein. Sie können z. B. Kommentare eingeben, die erklären, warum Sie den Status ändern, oder Hinweise über Ihre Analyse des Alerts hinzufügen.
   e. Klicken Sie **OK** an, um die Änderungen zu speichern.

Ergebnisse

Der Alert spiegelt jetzt den zugeordneten Status wider und wird, nachdem Sie die Anzeige aktualisiert haben, nur in Ihrem Fester **Alertzusammenfassung** angezeigt. Anderen Analysten in Ihrer Visualizer-Analystengruppe wird dieser Alert nicht mehr angezeigt, nachdem sie die Anzeige ihres Fensters **Alertzusammenfassung** aktualisiert haben.

Zuordnen von Alerts zu anderen Analystengruppen

Wenn Sie feststellen, dass ein Alert einer anderen Visualizer-Analystengruppe zugeordnet werden muss, können Sie diesen Alert übertragen. Sie können einen Alert nicht an einen bestimmten Visualizer-Benutzer übertragen, aber Sie können diesen Alert an die Visualizer-Analystengruppe übertragen, der der Benutzer angehört.

Vorgehensweise

1. Klicken Sie in Visualizer im Fenster **Alertzusammenfassung** in der Tabelle **Alertzusammenfassung** die Alertzusammenfassung an, mit der der Alert verknüpft ist.
2. Klicken Sie in der Tabelle mit der Alertliste den zu übertragenden Alert doppelt an.
3. Klicken Sie im Prüffenster **Status festlegen** an.
4. Führen Sie in **Status festlegen** Folgendes aus:
   a. Wählen Sie **Alert übertragen**, in **Auszuführende Aktion auswählen** aus.
   b. Wählen Sie in **Alert übertragen auf** die Visualizer-Analystengruppe aus, an die Sie den Alert übertragen wollen. Wird die Visualizer-Analystengruppe, die Sie auswählen wollen, nicht angezeigt, bitten Sie Ihren Systemadministrator, diese Analystengruppe zu konfigurieren. Ein entsprechender Aktivitätscode wird in **Aktivitätscode auswählen** angezeigt.
   c. Optional: Zum Zuordnen eines anderen Aktivitätscodes wählen Sie diesen in **Aktivitätscode auswählen** aus. Wird der Aktivitätsstatuscode nicht angezeigt, den Sie auswählen wollen, bitten Sie Ihren Systemadministrator, diesen Aktivitätscode zu konfigurieren.

d. Geben Sie Kommentare oder Hinweise in das Textfeld **Kommentare** ein. Sie können z. B. Kommentare eingeben, die erklären, warum Sie den Alert übertragen.
e. Klicken Sie **OK** an, um die Übertragung zu beenden.

Ergebnisse

Der Alert wird jetzt an die ausgewählte Visualizer-Analystengruppe übertragen und im Fenster **Alertzusammenfassung** der Analysten in der betreffenden Visualizer-Analystengruppe angezeigt. (Analysten in dieser Gruppe müssen möglicherweise vorher ihr Fenster **Alertzusammenfassung** aktualisieren). Dieser Alert wird nicht mehr im Fenster **Alertzusammenfassung** der Analysten in Ihrer Visualizer-Analystengruppe (einschließlich Ihrer selbst) angezeigt, nachdem die Anzeige dieses Fensters aktualisiert wurde.

Ändern des Status eines Alerts

Wenn Sie die Alerts analysieren, die Ihnen oder Ihrer Visualizer-Analystengruppe zugewiesen sind, können Sie mit Visualizer Ihre Untersuchungen, Ihre Kommentare und die Art der Disposition für den Alert verfolgen.

Informationen zu diesem Vorgang

Sie können den Alertstatus für Alerts, die Ihnen oder Ihrer Visualizer-Analystengruppe zugeordnet sind, jederzeit aktualisieren. Sie können diesen Alerts auch jederzeit Kommentare hinzufügen. Sie können jedoch vorhandene Kommentare nicht bearbeiten.

Vorgehensweise

1. Klicken Sie in Visualizer im Fenster **Alertzusammenfassung** in der Tabelle **Alertzusammenfassung** die Alertzusammenfassung an, die den zu aktualisierenden Alert enthält.
2. Klicken Sie in der Alertliste den Alert, dessen Status geändert werden soll, doppelt an.
3. Klicken Sie im Prüffenster **Status festlegen** an.
4. Führen Sie in **Status festlegen** Folgendes aus:
   a. Wählen Sie **Status festlegen** in **Auszuführende Aktion auswählen** aus. Ein entsprechender Aktivitätscode wird in **Aktivitätscode auswählen** angezeigt.
   b. Optional: Zum Zuordnen eines anderen Aktivitätscodes wählen Sie diesen in **Aktivitätscode auswählen** aus. Wird der Aktivitätsstatuscode nicht angezeigt, den Sie auswählen wollen, bitten Sie Ihren Systemadministrator, diesen Aktivitätscode zu konfigurieren.
   c. Geben Sie Kommentare oder Hinweise in **Kommentare** ein. Sie können z. B. Kommentare eingeben, die erklären, warum Sie den Status ändern, oder Hinweise über Ihre Analyse des Alerts hinzufügen.
   d. Klicken Sie **OK** an, um die Änderungen zu speichern.

Ergebnisse

Der Alert spiegelt jetzt den neuen Status im Fenster **Alertzusammenfassung** wider.

Der aktuellste Status oder die neueste Kommentaraktualisierung für einen Attributalert werden ganz oben im Abschnitt **Statuszusammenfassung** angezeigt.

Wenn die Statusänderung die Zuordnung des Attributalerts an Sie selbst beinhaltete, wird dieser Attributalert, nachdem Sie die Anzeige aktualisiert haben, nur in Ihrem Fenster **Alertzusammenfassung** angezeigt. Anderen Analysten in Ihrer Visualizer-Analystengruppe wird dieser Alert nicht mehr in ihrem Fenster **Alertzusammenfassung** angezeigt, nachdem sie die Anzeige aktualisiert haben.

Hilfethemen

Fenster 'Alertzusammenfassung':

In diesem Fenster können Sie nicht zugeordnete Alertzusammenfassungen für Ihre Visualizer-Analystengruppe oder Alerts anzeigen, die Sie sich selbst zugeordnet haben.

Blenden Sie mit den Twisties die Abschnitte der Anzeige ein oder aus, um den Fokus auf ein bestimmtes Detail zu setzen.

Alerts nach Typ anzeigen
Wählen Sie einen Alerttyp aus, der angezeigt werden soll, oder zeigen Sie alle Alerttypen an.

Auswahlgruppe 'Filter anzeigen'
Ändert die Standardfiltereinstellungen, die festlegen, welche Alertzusammenfassungen in Ihrem Fenster **Alertzusammenfassung** angezeigt werden. Diese Filter ändern nur die Anzeige der Alertzusammenfassungen, die zurzeit nicht zugeordnet sind, und es handelt sich dabei nur um eine temporäre Änderung. Wenn Sie das Fenster **Alertzusammenfassung** schließen und zu einem anderen Zeitpunkt erneut öffnen, werden diese Einstellungen auf die Standardfiltereinstellungen zurückgesetzt.

Als Standardeinstellungen gelten die Alertfiltereinstellungen, die für Ihre Workstation konfiguriert sind. (Sie können die Standardeinstellungen auf der Registerkarte **Benutzervorgaben für das System** im Fenster **Benutzervorgaben für die Anzeige konfigurieren** ändern.)

Tabelle 'Alertzusammenfassung'
Alerts, die folgende Elemente gemein haben, werden in Alertzusammenfassungen gruppiert: Alerttyp, Beschreibung, Wertigkeit, Status, Auflösungsregel, Ähnlichkeitsbewertung und Beziehungsbewertung. In der Spalte **Anzahl** wird angezeigt, wie viele einzelne Alerts in der Zusammenfassung gruppiert sind.

Sie können die Tabelle sortieren, indem Sie eine Spaltenüberschrift in der Tabelle anklicken. Beim ersten Anklicken werden die Spaltenwerte in aufsteigender Reihenfolge sortiert. Beim zweiten Anklicken werden die Spaltenwerte in aufsteigender Reihenfolge sortiert.

Standardmäßig ist die Tabelle nach Alerttyp sortiert.

Typ Alerttyp, zu dem die Alertzusammenfassung gehört.

Beschreibung
Beschreibung der Alerts in dieser Zusammenfassung.

Im Fall von Attributalerts besteht diese Beschreibung aus der Fallnummer. Im Fall von Ereignisalerts besteht diese Beschreibung aus der Ereignissituationsbeschreibung. Im Fall von Rollenalerts besteht diese Beschreibung aus der Beschreibung der Rollenalertregel.

Status Aktueller Aktivitätsstatus der Alerts in dieser Zusammenfassung.

Auflösungsregel
Name der Auflösungsregel, die verwendet wird, um Beziehungen zwischen den Entitäten innerhalb dieser Alertzusammenfassung erkennen.

Ähnlichkeitsbewertung
Bewertung (0 - 100), die anzeigt, mit welcher Wahrscheinlichkeit die zusammengehörigen Entitäten dieselbe Entität darstellen.

Beziehungsbewertung
Bewertung (0 - 100), die anzeigt, wie eng die Beziehungen der Entitäten im Alert untereinander sind.

Anzahl
Anzahl der einzelnen in dieser Alertzusammenfassung gruppierten Alerts, die die aktuell ausgewählten Kriterien für die Auswahlgruppe **Filter anzeigen** erfüllen.

Tabelle 'Alertliste'
Nach dem Auswählen einer Alertzusammenfassung aus der Tabelle **Alertzusammenfassung** werden die einzelnen Alerts, die zu dieser Zusammenfassung gehören, in diesem Abschnitt angezeigt. Die Anzahl der angezeigten Alerts (Zeilen) hängt von der Gesamtzahl der Alerts in der Zusammenfassung (in der Spalte **Anzahl** der Tabelle **Alertzusammenfassung** gefunden) und der Nummer im Feld **Maximale Anzahl Zeilen in Alertliste** der Auswahlgruppe **Filter anzeigen** ab. Eine Listenzahl in der Titelleiste der Tabelle **Alertliste** zeigt an, wie die Anzahl der aktuell angezeigten Alerts in die Gesamtzahl der Alerts für diese Zusammenfassung passt.

Sortieren Sie die Tabelle, indem Sie eine Spaltenüberschrift in der Tabelle anklicken. Beim ersten Anklicken werden die Spaltenwerte in aufsteigender Reihenfolge sortiert. Beim zweiten Anklicken werden die Spaltenwerte in aufsteigender Reihenfolge sortiert.

Die angezeigten Felder hängen vom ausgewählten Alertzusammenfassungstyp ab.

Anzeige 'Attributalert':

In dieser Anzeige können Sie den Analysestatus eines Attributalerts festlegen oder ändern und seine Details prüfen.

Blenden Sie mit den Twisties die Abschnitte der Anzeige ein oder aus, um den Fokus auf ein bestimmtes Detail zu setzen.

Statuszusammenfassung
Fasst den aktuellen Analysestatus und die Disposition des Alerts zusammen.

Alertzusammenfassung
Enthält die Beschreibung der Alertzusammenfassung sowie Generierungsdatum und -zeit des Alerts.

Abschnitt 'Abgleich mit Entität'
Enthält Details dazu, welche Attribute zwischen den Suchkriterien Ihres Attributalertgenerators und den vorhandenen Entitäten in der Entitätendatenbank übereinstimmten. Klicken Sie ein bestimmtes Attribut an, um die Übereinstimmungsinformationen aus den Identitäten der übereinstimmenden Entitäten hervorzuheben.

Attributalertgenerator - Details
Fasst die Kriterien für den Attributalertgenerator zusammen, der diesen Attributalert generiert hat. Klicken Sie zum Hervorheben aller Kriterien die Datenquelle an.

Abschnitt 'Entität'
Zeigt Informationen zur Entität an, die mit den Kriterien des Attributalertgenerators übereinstimmte. Klicken Sie zum Hervorheben der Daten, die aus einem Identitätsdatensatz aus dieser Datenquelle stammen, die Datenquelle an.

Schaltfläche 'Entitätszusammenfassung'
Klicken Sie diese Schaltfläche an, um die Entitätszusammenfassung für die übereinstimmende Entität anzuzeigen. Sie können auch weitere, der Entität zugeordnete Identitäten prüfen, um Ihre Analyse dieses Alerts voranzutreiben.

Anzeige 'Ereignisalert':

In der Anzeige **Ereignisalert** können Sie den Analysestatus eines Ereignisalerts festlegen oder ändern und seine Details prüfen. Ereignisalerts werden nur angezeigt, wenn der Ereignismanager für Ihr System aktiviert ist, die Aktivitätscodes für Ereignisalerts konfiguriert sind und mindestens ein Ereignisalert vorhanden ist.

Blenden Sie mit den Twisties die Abschnitte der Anzeige ein oder aus, um den Fokus auf ein bestimmtes Detail zu setzen.

Statuszusammenfassung
Fasst den aktuellen Analysestatus und die Disposition des Ereignisalerts zusammen.

Alertzusammenfassung
Enthält die Beschreibung des Ereignisalerts sowie das Datum und die Uhrzeit der Alertgenerierung.

Abschnitt 'Ereignisalert'
Enthält die Ereignisdetails, aus denen dieser Ereignisalert besteht.

Abschnitt 'Entität'
Bietet eine kurze Zusammenfassung für jede an diesem Ereignisalert beteiligte Entität.

Schaltfläche 'Bericht'
Klicken Sie diese Schaltfläche an, um einen Bericht zu den Ereignisalertdetails zu erstellen.

Anzeige 'Rollenalert':

In dieser Anzeige können Sie die Details eines Rollenalerts anzeigen und den Analysestatus des Rollenalerts festlegen oder ändern.

Blenden Sie durch Anklicken der Twisties die Abschnitte der Anzeige ein oder aus, um den Fokus auf ein bestimmtes Detail zu setzen.

Abgrenzungsgrade
Gibt die Anzahl der Abgrenzungsgrade zwischen den Entitäten in diesem Rollenalert an.

Statuszusammenfassung
Fasst den aktuellen Analysestatus und die Disposition des Alerts zusammen.

Alertzusammenfassung
Enthält eine Beschreibung der Alertzusammenfassung, den Alertwertigkeitscode für diesen Alert, die Auflösungsregel, die zum Abgleichen der Entitäten innerhalb des Alerts verwendet wird, die Auflösungsbewertung, die die Ähnlichkeit zwischen zwei Entitäten angibt, und die Beziehungsbewertung, die die Wahrscheinlichkeit angibt, mit der sich die zwei Entitäten kennen.

Registerkarte 'Übereinstimmende Details'
Enthält Details dazu, welche Attribute zwischen den zwei Entitäten übereinstimmten. Klicken Sie ein bestimmtes Attribut an, um die Übereinstimmungsinformationen aus den Identitäten der übereinstimmenden Entitäten hervorzuheben.

Enthält Details dazu, welche Attribute zwischen den Suchkriterien Ihres Attributalertgenerators und den vorhandenen Entitäten in der Entitätendatenbank übereinstimmten.

Schaltfläche 'Bericht'
Klicken Sie diese Schaltfläche an, um einen Bericht zu den Rollenalertdetails für diesen Rollenalert zu erstellen.

Schaltfläche 'Entitätszusammenfassung'
Klicken Sie diese Schaltfläche an, um die Entitätszusammenfassung für die ausgewählte Entität anzuzeigen. Sie können auch weitere, der Entität zugeordnete Identitäten prüfen, um Ihre Analyse dieses Alerts voranzutreiben.

Anzeige 'Entitätsereignisse':

In der Anzeige **Entitätsereignisse** können Sie die Ereignisse für eine Entität prüfen, die innerhalb eines bestimmten Datumsbereichs aufgetreten sind. Der erste Zugriff auf diese Anzeige erfolgt durch Anklicken von **Ereignisse anzeigen** in der Anzeige **Entitätszusammenfassung**.

Abschnitt 'Ereigniszusammenfassung'
Zeigt eine Zusammenfassung aller Ereignisse für diese Entität im angegebenen Datumsbereich an. In der Anzeige werden standardmäßig alle Ereignisse angezeigt, die der Entität ab dem Datum des ersten Ereignisses bis zum aktuellen Datum zugeordnet sind. Ändern Sie den Datumsbereich unter Verwendung des Ereignisdatumsfilters, um Ereignisse aufzurufen, die in einem anderen Datumsbereich liegen.

Auf dem Bildschirm angezeigter Ereignisdatumsfilter
Filtert die angezeigten Ereignisse anhand des angegebenen Datumsbereichs, wenn Sie **Sicht aktualisieren** anklicken.

Anfangsdatum
Geben Sie ein Datum ein, oder klicken Sie die Kalendersteuerung an, um das Anfangsdatum im Datumsbereich auszuwählen.

Wenn Sie ein Datum eingeben wollen, verwenden Sie eines der folgenden Datumsformate:

- `MM/tt/jjjj`, `MM-tt-jjjj`, `MM.tt.jjjj` oder `MMttjjjj`
- `jjjj/MM/tt`, `jjjj-MM-tt` oder `jjjj.MM.tt`
- `3. Januar 2008` oder `03. Januar 2008`
- `3. Januar 08` oder `03. Januar 08`
- `03. Jan. 2008` oder `3. Jan. 2008`
- `3. Jan. 08` oder `03. Jan. 08`

Der Standardwert für dieses Feld ist die erste Instanz des Ereignisdatums.

Enddatum
Geben Sie ein Datum ein, oder klicken Sie die Kalendersteuerung an, um das Enddatum im Datumsbereich auszuwählen.

Wenn Sie ein Datum eingeben wollen, verwenden Sie eines der folgenden Datumsformate:

- `MM/tt/jjjj`, `MM-tt-jjjj`, `MM.tt.jjjj` oder `MMttjjjj`
- `jjjj/MM/tt`, `jjjj-MM-tt` oder `jjjj.MM.tt`
- `3. Januar 2008` oder `03. Januar 2008`
- `3. Januar 08` oder `03. Januar 08`
- `03. Jan. 2008` oder `3. Jan. 2008`
- `3. Jan. 08` oder `03. Jan. 08`

Der Standardwert für dieses Feld ist das aktuelle Datum.

Schaltfläche 'Sicht aktualisieren'
Klicken Sie diese Schaltfläche an, um Ereignisse für diese Entität anzuzeigen, die innerhalb des angegebenen Datumsbereichs liegen. Diese Schaltfläche wird erst aktiviert, wenn Sie die Standarddatumsangaben in den Datumsfeldern ändern.

Schaltfläche 'Bericht'
Klicken Sie diese Schaltfläche an, um einen Bericht **Alle Ereignisse** für diese Entität zu generieren.

Bildschirmanzeige
In diesem Abschnitt der Anzeige sind die Ereignisse für diese Entität, die innerhalb des angegebenen Datumsbereichs liegen, nach Ereignistyp zusammengefasst.

Ereignistyp
Beschreibt den Ereignistyp.

Anzahl
Gibt die Gesamtzahl der Ereignisse für diese Entität nach Ereignistyp an, die innerhalb des angegebenen Datumsbereichs liegen. (Beträgt die Anzahl beispielsweise 4, sind vier Ereignisse eines Ereignistyps für diese Entität innerhalb des angegebenen Datumsbereichs aufgetreten.)

Wert Gibt die Gesamtzahl der Ereignisse für diese Entität nach Ereignistyp an, die innerhalb des angegebenen Datumsbereichs liegen. (Liegen z. B. vier Ereignisse vor, ist diese Zahl die Gesamtzahl des Werts für diese vier Ereignisse.)

Menge
Gibt die Gesamtzahl der Einheiten für die Ereignisse dieser Entität nach Ereignistyp an, die innerhalb des angegebenen Datumsbereichs liegen.

Maßeinheit
Beschreibt die Maßeinheit für den Ereigniswert. Die Maßeinheit wird abhängig vom Ereignistyp in der Konfigurationskonsole konfiguriert.

Gesamtanzahl
Gibt die Gesamtzahl aller Ereignisse für diese Entität an, die innerhalb des angegebenen Datumsbereichs liegen.

Gesamtwert
Gibt den Gesamtwert aller Ereignisse für diese Entität an, die innerhalb des angegebenen Datumsbereichs liegen.

Abschnitt 'Ereignisdetails'
Wählen Sie eine Ereigniszeile im Abschnitt 'Ereigniszusammenfassung' aus, um weitere Details zu den einzelnen Ereignissen aufzurufen, die in der Ereignistypzusammenfassung enthalten sind. Wenn Sie eine beliebige Ereigniszeile in diesem Abschnitt doppelt anklicken, enthält die aufgerufene Anzeige **Ereignisdetails** noch detailliertere Informationen zum ausgewählten Ereignis.

Datum
Gibt das Datum und die Uhrzeit des Ereignisses an.

Datenquelle - Beschreibung
Beschreibt die Datenquelle, die dem Ereignis zugeordnet ist.

Externe ID
Zeigt den eindeutigen Schlüssel an, der den eingehenden Datensatz in der ursprünglichen Datenquelle für dieses Ereignis angibt.

Ereignisreferenz
Bietet zusätzliche Informationen zum Ereignis in der ursprünglichen Datenquelle, wenn diese Informationen zum eingehenden Datensatz gehören.

Wert Gibt den Wert des Ereignisses an.

Menge
Gibt die Anzahl der Einheiten im Ereignis an.

Kurzinfo oder *benutzerdefinierte Bezeichnung*
Bietet zusätzliche Informationen zum Ereignis, z. B. Hinweise oder Kommentare, die zusätzlichen Kontext zur Ereignistransaktion bieten können.

Benutzer können im Rahmen der Konfiguration eines Ereignistyps in der Konfigurationskonsole eine benutzerdefinierte Bezeichnung für diese Spalte definieren. So wird Ihnen möglicherweise statt **Kurzinfo** eine aussagekräftigere benutzerdefinierte Bezeichnung angezeigt (beispielsweise **Hinweise zu telegrafischen Geldanweisungen**).

Suchen von Entitäten

Sie können mehrere Suchmethoden in Visualizer zum Suchen einer Entität in der Entitätendatenbank verwenden. Wenn Sie immer dann benachrichtigt werden wollen, wenn das System einen Datensatz mit einem bestimmten Namen, einer bestimmten Adresse, Nummer oder E-Mail-Adresse verarbeitet, erstellen Sie einen Attributalertgenerator, um Entitäten automatisch zu "suchen".

Suchen von Entitäten nach Attribut

Wenn Sie Visualizer verwenden und nach einer Entität in der Entitätendatenbank suchen wollen, können Sie die Entität durch Eingabe von Kriterien für die Attribute suchen, die der Entität zugeordnet sind. Sie geben die Attributkriterien an, wor-

aufhin Visualizer basierend auf diesen Kriterien eine Abfrage erstellt. Dieser Typ der Entitätsabfrage durchläuft keinen Entitätsauflösungsprozess, um Suchergebnisse zurückzugeben.

Vorgehensweise

1. Führen Sie einen der folgenden Schritte in Visualizer aus:
   a. Klicken Sie **Anzeigen** > **Suchen nach** > **Attribut** an.
   b. Klicken Sie in der Symbolleiste das Symbol für Suchen an.
   c. Klicken Sie in der Symbolleiste den Pfeil an und wählen Sie **Attribut** aus.
   d. Wählen Sie **Attribut** in der Dropdown-Liste **Suchen nach** des Fensters **Suchen nach** aus.
2. Geben Sie die Kriterien für jeden Attributtyp ein, den Sie bei der Suche nach Entitäten verwenden wollen.
   a. Klicken Sie **+** an, um eine Zeile zur Angabe von Kriterien für einen anderen Attributtyp hinzuzufügen.
   b. Klicken Sie **-** an, um die ausgewählten Abfragekriterieneinträge zu entfernen.
3. Optional: Klicken Sie **Zusammenfassung anzeigen** an, um eine Zusammenfassung der Abfrage **Suche nach Attributen** anzuzeigen. Die Zusammenfassung ist eine hilfreiche Möglichkeit sicherzustellen, dass die Abfrage die gewünschten Werte enthält. Ist dies nicht der Fall, schließen Sie die Zusammenfassung und korrigieren Sie die Abfragekriterien.

   Zwei Abfragekriterien desselben Attributtyps werden durch eine Klausel OR verbunden. Alle anderen Abfragekriterien werden durch die Klausel AND verbunden.

   Die Reihenfolge der Attributtypkriterien hat keinen Einfluss auf die Ergebnisse.
4. Klicken Sie **Suchen** an.

Ergebnisse

Entitäten, die die Abfragekriterien erfüllen, werden im Teilfenster **Ergebnisse** angezeigt.

Die für attributbasierte Abfragen angezeigten Ergebnisse sind standardmäßig auf die ersten 1.000 übereinstimmenden Entitäten beschränkt. Wenn es mehr als 1.000 Übereinstimmungen gibt, wird im Teilfenster **Ergebnisse** angezeigt, dass weitere Ergebnisse vorhanden sind. (Die Anzahl der angezeigten Ergebnisse kann von Ihrem Systemadministrator in der Konfigurationskonsole konfiguriert werden. Dazu muss dieser in den Systemparametern den Parameter MAX_ENTITIES_RETURNED festlegen.)

Anmerkung: Wenn Ihr System eine zusätzliche Adressbereinigungsanwendung verwendet, werden Adressen mit Sonderzeichen möglicherweise transliteriert. Das Suchergebnis für z. B. eine deutsche Adresse, die mindestens einen Umlaut in der Adresse enthält, liefert möglicherweise ein Ergebnis, das keine übereinstimmenden Umlaute enthält.

Nächste Schritte

Klicken Sie eine Entität an, um die Entitätszusammenfassung für die ausgewählte Entität anzuzeigen.

Suchen von Entitäten nach Datenquellenbenutzerkonto

Wenn Sie die Kontonummer (oder externe ID) einer Identität kennen und nach der Entität suchen wollen, die diese Identität enthält, verwenden Sie die auf Datenquellenbenutzerkonten basierte Suche in Visualizer. Darüber hinaus können Sie auch nach einer Entität suchen, die Sie über die Anzeige **Entität hinzufügen** hinzugefügt haben.

Vorbereitende Schritte

Sie müssen die Datenquellenbeschreibung und die externe ID der Identität (oder des Benutzerkontos) kennen. Wenn Sie eine Entität nach Namen suchen wollen, verwenden Sie die Methode **Attributbasierte Suche**.

Vorgehensweise

1. Führen Sie einen der folgenden Schritte in Visualizer aus:
   a. Klicken Sie **Anzeigen** > **Suchen nach** > **Datenquellenbenutzerkonto** an.
   b. Klicken Sie in der Symbolleiste den Pfeil an und wählen Sie **Datenquellenbenutzerkonto** aus.
   c. Wählen Sie **Datenquellenbenutzerkonto** in der Dropdown-Liste **Suchen nach** des Fensters **Suchen nach** aus.
2. Geben Sie in **Externe ID eingeben** die Kontonummer für die Identität ein. Über das Benutzerkonto ist die Identität in der ursprünglichen Datenquelle bekannt.
3. Wählen Sie in **Datenquelle** den Datenquellencode und die Beschreibung aus.
4. Klicken Sie **Suchen** an.

Ergebnisse

Wenn das System eine Entität findet, die eine Identität mit der angegebenen externen ID und den Datenquellenkriterien enthält, zeigt Visualizer die Entitätszusammenfassung für diese Entität an.

Suchen von Entitäten nach Entitäts-ID

Wenn Sie die Entitäts-ID-Nummer einer Entität kennen, verwenden Sie die auf Entitäts-IDs basierte Suche, um die Entität schnell zu finden und die Entitätszusammenfassung für diese Entität anzuzeigen.

Vorbereitende Schritte

Sie müssen die Entitäts-ID-Nummer der Entität kennen, nach der Sie suchen wollen. Wenn Sie eine Entität nach Namen suchen wollen, verwenden Sie stattdessen die Methode **Attributbasierte Suche**.

Vorgehensweise

1. Führen Sie einen der folgenden Schritte in Visualizer aus:
   a. Klicken Sie **Anzeigen** > **Suchen nach** > **Entitäts-ID** an.
   b. Klicken Sie in der Symbolleiste den Pfeil an und wählen Sie **Entitäts-ID** aus.
   c. Wählen Sie **Entitäts-ID** in der Dropdown-Liste **Suchen nach** des Fensters **Suchen nach** aus.
2. Geben Sie in **Entitäts-ID eingeben** die Entitäts-ID-Nummer für die zu suchende Entität ein.
3. Klicken Sie **Suchen** an.

Ergebnisse

Wenn die Entitäts-ID mit einer Entität in der Entitätendatenbank übereinstimmt, zeigt Visualizer die Entitätszusammenfassung für diese Entität.

Suchen von Entitäten nach Auflösung

Verwenden Sie die auflösungsbasierte Suche zum Erstellen einer Suchentität, die den Entitätsauflösungsprozess durchläuft, um festzustellen, ob in der Entitätendatenbank Identitäten vorhanden sind, die Kriterien der Abfrage erfüllen.

Vorbereitende Schritte

Die Funktion **Auflösungsbasierte Suche** erfordert eine aktive Pipeline, die dem Visualizer-Server, mit dem kommuniziert werden soll, zur Verfügung steht. Die Pipeline ist die Komponente, in der die Entitäts- und Beziehungsauflösung stattfindet.

Informationen zu diesem Vorgang

Damit Sie die Funktion **Auflösungsbasierte Suche** so effektiv wie möglich verwenden können, müssen Sie wissen, wie die Entitätsauflösung funktioniert und für Ihr System konfiguriert ist, da die Entitätsauflösung für die Suche nach den Ergebnissen verwendet wird. Wenn die Entitätsauflösung beispielsweise nicht für die Suche nach Übereinstimmungen nur nach Namen konfiguriert ist, gibt die auflösungsbasierte Suche bei Suchen nur nach einem Namenswert keine Ergebnisse zurück. Gleichermaßen werden, wenn nur eine Postleitzahl angegeben wird, keine Ergebnisse zurückgegeben, da die Entitätsauflösung keine Entitäten ausschließlich basierend auf der Postleitzahl auflöst.

Die auflösungsbasierte Suche verwendet die Mindestbewertungswerte, die auf der Registerkarte **Benutzervorgaben für das System** des Menüs **Datei** definiert sind.

Vorgehensweise

1. Führen Sie einen der folgenden Schritte in Visualizer aus:
   a. Klicken Sie **Anzeigen** > **Suchen nach** > **Auflösung** an.
   b. Klicken Sie in der Symbolleiste den Pfeil an und wählen Sie **Auflösung** aus.
   c. Wählen Sie **Auflösung** in der Dropdown-Liste **Suchen nach** des Fensters **Suchen nach** aus.
2. Geben Sie so viele Attribute ein, wie Ihnen über die Identität bekannt sind.
   - Wenn Sie im Abschnitt **Name** eine Eingabe machen, ist der **Nachname** erforderlich.
   - Wenn Sie in den Abschnitt **Adressliste** Informationen eingeben, ist eine Angabe in **Adresse** erforderlich.
   - Wenn Sie einen **Typ** im Abschnitt **Nummernliste** auswählen, müssen Sie einen Zahlenwert in das Feld **Wert** eingeben. (**Standort** ist optional.)
   - Wenn Sie einen **Typ** im Abschnitt **Merkmalliste** auswählen, müssen Sie einen Merkmalwert in das Feld **Wert** eingeben.
   - Wenn Sie einen **Typ** im Abschnitt **E-Mail-Liste** auswählen, müssen Sie einen Wert für die E-Mail-Adresse in das Feld **Adresse** eingeben.
3. Klicken Sie **Suche** an.

Suchen von Entitäten anhand von Attributalertgeneratoren

Wenn Sie eine Entität beobachten, können Sie Attributalertgeneratoren mit den gewünschten Kriterien für diese Entität erstellen. Wenn Identitätsdatensätze oder En-

titäten Attribute enthalten, die die Kriterien erfüllen, wird vom System ein Attributalert generiert. Jeder Visualizer-Benutzer erstellt und verwaltet persönliche Attributalertgeneratoren für einen bestimmten Datumsbereich.

Da Attributalertgeneratoren über die Pipeline übergeben werden, wird der Entitätsauflösungsprozess für diese Suchanforderungen auf dieselbe Weise ausgeführt wie für eingehende Entitätsdaten:

- Namen und Adressen werden standardisiert
- Teilsuchen oder Suchen nach grober Übereinstimmung und Vergleiche werden ausgeführt, sodass anwendbare Entitäten in den nachfolgenden Attributalerts festgestellt werden

Damit Sie Attributalertgeneratoren so effektiv wie möglich verwenden können, müssen Sie wissen, wie die Entitätsauflösung funktioniert und für Ihr System konfiguriert ist, da die Entitätsauflösung für die Suche nach Ihren Attributalertergebnissen verwendet wird. Wenn die Entitätsauflösung beispielsweise nicht für die Suche nach Übereinstimmungen lediglich anhand eines Namenswerts konfiguriert ist, gibt ein Attributalertgenerator, der nur für die Suche nach einem Namenswert konfiguriert ist, keine Ergebnisse zurück. Gleichermaßen gibt ein Attributalertgenerator, der nur die Postleitzahl angibt, keine Ergebnisse zurück, da die Entitätsauflösung keine Entitäten ausschließlich basierend auf der Postleitzahl auflöst.

Verwenden Sie beim Erstellen eines Attributalertgenerators die folgenden Richtlinien:

- Verwenden Sie die Dropdown-Liste **Mindestbewertung**, um die Attributalertergebnisse zu filtern. Der Standardwert für dieses Feld ist **Beliebige Beziehung**. Diese Auswahl führt zu den meisten Ergebnissen. Wählen Sie eine höhere Stufe aus, um weniger Ergebnisse zu erzielen. Diese Werte werden in den Visualizer-Systemvorgaben konfiguriert, die im Menü **Datei** zur Verfügung stehen.
- Für Namen: Geben Sie entweder eine Kombination aus Nachname und Vorname oder Nachname und zweitem Vornamen an. Attributalertgeneratoren, die nur einen Nachnamen, Vornamen oder zweiten Vornamen angeben, geben keine Ergebnisse zurück.
- Für Adressen: Sowohl die Adresse als auch die Postleitzahl sind erforderlich. Attributalertgeneratoren, die nur eine Stadt, einen Bundesstaat, eine Postleitzahl, eine Straße oder ein Land angeben, geben keine Ergebnisse zurück.

Erstellen von Attributalertgeneratoren:

Wenn jedes Mal ein Alert empfangen werden soll, wenn ein bestimmter Attributwert oder eine bestimmte Kombination von Attributwerten vom System verarbeitet wird, erstellen Sie einen Attributalertgenerator. Attributalertgeneratoren generieren Alerts, bis das angegebene Ablaufdatum erreicht ist.

Vorgehensweise

1. Führen Sie einen der folgenden Schritte in Visualizer aus:
   a. Wählen Sie **Anzeigen** > **Manager für Attributalertgenerator** aus.
   b. Klicken Sie in der Symbolleiste das Symbol für den Manager für Attributalertgeneratoren an.
2. Klicken Sie **Erstellen** im Fenster **Manager für Attributalertgenerator** an.
3. Verwenden Sie die Dropdown-Listen und Felder, um die genauen Kriterien für den neuen Attributalert einzugeben (einschließlich ein Ablaufdatum). Das Standardablaufdatum ist gemäß Einstellung sechs Monate ab dem heutigen Datum.

4. Klicken Sie **Erstellen** an.

Ergebnisse

Nun wird jedes Mal, wenn Daten, die den von Ihnen angegebenen Kriterien entsprechen, mithilfe der Entitätsauflösung verarbeitet werden, in Ihrem Fenster **Alertzusammenfassung** ein neuer Attributalert angezeigt. Wenn die gesuchten Informationen sich zurzeit in der Entitätendatenbank befinden, wird im Fenster **Alertzusammenfassung** ein neuer Attributalert angezeigt.

Bearbeiten von Attributalertgeneratoren:

Bearbeiten Sie einen aktiven Attributalertgenerator, wenn Sie die Fallnummer, den Kommentar oder das Ablaufdatum ändern wollen.

Informationen zu diesem Vorgang

Sie können die Attribute oder die Mindestauflösungsbewertung für diese Attribute nicht ändern. Wenn Sie dies jedoch trotzdem erreichen wollen, erstellen Sie einen Attributalertgenerator. Soll der neue Attributalertgenerator zudem einen vorhandenen ersetzen, führen Sie die folgenden Schritte aus, um den nicht mehr benötigten Attributalertgenerator verfallen zu lassen.

Vorgehensweise

1. Führen Sie einen der folgenden Schritte in Visualizer aus:
   a. Klicken Sie **Anzeigen** > **Manager für Attributalertgenerator** an.
   b. Klicken Sie in der Symbolleiste das Symbol für den Manager für Attributalertgeneratoren an.
2. Wählen Sie den zu bearbeitenden Attributalertgenerator aus und klicken Sie **Erstellen** an.
3. Nehmen Sie im Fenster **Attributalertgenerator - Informationen** Ihre Änderungen vor.
   - Sie können das Ablaufdatum ändern. Dabei besteht auch die Möglichkeit, das Datum auf ein zurückliegendes Datum zu setzen, um den Attributalertgenerator verfallen zu lassen.
   - Sie können auch die Fallnummer und Kommentare aktualisieren.
   - Nicht ändern können Sie den Ursachencode, die Attribute, die Sie für den Attributalertgenerator bei dessen Erstellung ausgewählt haben, oder die Mindestauflösungsbewertung.
4. Klicken Sie **Aktualisieren** an.

Ergebnisse

Das System protokolliert die Änderungen, die Sie an dem Attributalertgenerator vorgenommen haben. Zeigen Sie einen Bericht **Attributalertgenerator - Protokoll** an oder drucken Sie diesen aus, um alle Änderungen an Ihrem Attributalertgenerator einsehen zu können.

Hilfethemen:

Anzeige für die Suche nach Attributen:

In diesem Fenster können Sie eine Abfrage erstellen, um Entitäten in der Entitätendatenbank nach Attributen zu suchen, z. B. nach Namen, Adressen, Nummern,

Merkmalen usw. Bei diesem Abfragetyp wird nicht der Entitätsauflösungsprozess verwendet, um die Abfrageergebnisse zurückzugeben.

Attributtyp
Entitätsattributtyp, den Sie als Kriterium für die Abfrage verwenden wollen: Name, Adresse, Nummern, Merkmale, E-Mail-Adresse, Datenquelle oder Dateiladedatum. Wenn Sie einen Attributtyp auswählen, werden im Fenster die für diesen Typ relevanten Felder für Abfragekriterien angezeigt.

Die Abfrageanweisung, die Sie erstellen, hängt davon ab, welche Attributtypen Sie für die Abfrage ausgewählt haben:

- In einer einzelnen Abfrage erstellen die Kriterien für mehrere gleiche Attributtypen eine Abfrageanweisung des Typs "OR". Beispiel: "Bob Hayes" OR "Rob Hays".
- In einer einzelnen Abfrage erstellen die Kriterien für mehrere Attributtypen eine Abfrageanweisung des Typs "AND". Beispiel: "Bob Hayes" AND credit card number "5252-1010-5252-1010".

Wenn Sie in einem solchen Fall die folgenden zwei Namen und eine Kreditkarte eingegeben haben, sieht die Abfrageanweisung wie folgt aus: Bob Hayes" OR "Rob Hays AND credit card number "5252-1010-5252-1010".

Verwenden Sie die Schaltfläche **Zusammenfassung anzeigen**, um die vollständige Abfrageanweisung anzuzeigen.

Wertfelder
Geben Sie die spezifischen Werte des Attributtyps ein, die beim Suchen von Entitäten verwendet werden sollen. Jeder Attributtyp verfügt über eigene Wertfelder. Wenn Sie die Wertfelder leer lassen, sucht die Abfrage alle potenziellen Werte. Wenn Sie jedoch in alle Wertfelder Daten eingeben, wird die Abfrage schneller ausgeführt und liefert bessere Ergebnisse.

- Namenskriterien sind erforderlich.
- Wenn Sie Informationen in ein Adress- oder E-Mail-Kriterienfeld eingeben, sind alle Adressfelder erforderlich.
- Wenn Sie einen Nummern- oder Merkmaltyp auswählen, ist das Feld **Wert** erforderlich.

Schaltfläche +
Fügt den Kriterien eine neue Attributzeile hinzu.

Schaltfläche -
Entfernt die ausgewählte Attributzeile und den Kriterieneintrag.

Fenster 'Attributbasierte Suche - Ergebnisse'
Enthält die Ergebnisse der attributbasierten Abfrage auf der Basis der Kriterieneinträge. Im Anzeigebereich werden standardmäßig die ersten 1.000 Datensätze angezeigt, die die Abfragekriterien erfüllen. (Diese Option kann jedoch von Ihrem Systemadministrator festgelegt werden.)

Die Ergebnisse werden nach Entität angezeigt und stellen die neuesten Informationen zu jeder Entität dar. Wenn Sie eine Entität im Teilfenster **Ergebnisse** doppelt anklicken, öffnet Visualizer die Entitätszusammenfassung für diese Entität.

Entitäts-ID
Zeigt die ID der Entität an, die den Abfragekriterien entspricht.

Name (*anzahl*)
Zeigt den Namen der Entität an, die die Abfragekriterien erfüllt, sowie eine Zahl, die die Anzahl der dieser Entität zugeordneten

Namen angibt. Beispielsweise gibt 'Bob M. Smith (4)' an, dass der Entität 'Bob Smith' vier Namen zugeordnet sind.

Adresse (*anzahl*)
Zeigt die Adresse der Entität an, die die Abfragekriterien erfüllt, sowie eine Zahl, die die Anzahl der dieser Entität zugeordneten Adressen angibt. Beispielsweise gibt '1024 Daisy Lane, Akron, OH 43596 (24)' an, dass dieser Entität 24 Adressen zugeordnet sind.

Nummerntyp: *wert*
Zeigt die Nummerntypen und Nummernwerte der Entität an, die die Abfragekriterien erfüllt.

Merkmaltyp: *wert*
Zeigt die Merkmaltypen und Werte der Entität an, die die Abfragekriterien erfüllt.

Beziehungen
Zeigt die Anzahl der von der Entität unterhaltenen Beziehungen an, die die Abfragekriterien erfüllt.

Alerts Zeigt die Anzahl der Alerts an, die der Entität zugeordnet sind, die die Abfragekriterien erfüllt.

Anzeige für die Suche nach Datenquellenbenutzerkonto:

In diesem Fenster können Sie eine Entität aus der ursprünglichen Datenquelle nach Benutzerkontoinformationen suchen.

Externe ID eingeben
Geben Sie die Informationen zum Datenquellenbenutzerkonto ein, die der Entität in der in **Datenquelle** angegebenen Datenquelle zugeordnet ist.

Datenquelle
Wählen Sie die Datenquelle aus, die dem im Fenster **Externe-ID eingeben** angegebenen Benutzerkonto entspricht.

Anzeige für die Suche nach Entitäts-ID:

Über diese Suchmethode können Sie eine Entität in der Entitätendatenbank schnell nach Entitäts-ID suchen. Wenn die Abfrage die Entität in der Entitätendatenbank lokalisiert hat, zeigt Visualizer die Entitätszusammenfassung für diese Entität an.

Fenster für die auflösungsbasierte Suche:

Im Fenster für die auflösungsbasierte Suche können Sie eine Suchentität erstellen und diese mit den Identitäten in der Entitätendatenbank vergleichen.

Datenquellencode - Beschreibung
Wählen Sie einen Datenquellencode und eine Beschreibung aus, um sie den Identitäten zuzuordnen, die im auflösungsbasierten Suchprozess gefunden wurden.

Mindestauflösungsbewertung
Wählen Sie die Mindestauflösungsbewertung aus, die beim Vergleich von Identitäten mit den für die auflösungsbasierte Suchabfrage angegebenen Kriterien verwendet werden soll.

Die von Ihnen ausgewählte Bewertung bestimmt die Anzahl und den Typ der Ergebnisse, die diese Abfrage zurückgibt.

Abschnitt mit den Kriterien für die auflösungsbasierte Suche
Geben Sie die Attribute an, um die Suchentität zu erstellen, die mit Identitäten in der Entitätendatenbank verglichen werden soll. Das System gibt Identitäten auf Basis der von Ihnen angegebenen Mindestauflösungsbewertung zurück.

Namensliste
Geben Sie die Namenskriterien in die Felder der Namensliste ein, wenn Sie einen bestimmten Namen suchen. Wenn Sie in einem der Namensfelder eine Eingabe vornehmen, muss auch das Feld **Nachname** ausgefüllt werden.

Adressliste
Geben Sie die Adresskriterien in die Felder der Adressliste ein, wenn Sie eine bestimmte Adresse suchen. Wenn Sie in einem der Adressfelder eine Eingabe vornehmen, muss auch das Feld **Straße** ausgefüllt werden.

Nummernliste
Geben Sie die entsprechenden Nummernkriterien in die Felder der Nummernliste ein, beispielsweise eine Pass- oder Kreditkartennummer. Die Felder **Typ** und **Wert** sind erforderlich.

Merkmalliste
Geben Sie die entsprechenden Merkmalkriterien in die Merkmalfelder ein, beispielsweise Geschlecht oder Geburtsdatum. Die Felder **Typ** und **Wert** sind erforderlich.

E-Mail-Liste
Geben Sie die entsprechenden Kriterien für die E-Mail-Adresse in die Felder der E-Mail-Adressliste ein. Die Felder **Typ** und **Adresse** sind erforderlich.

Fenster 'Manager für Attributalertgenerator':

Über dieses Fenster können Sie die zurzeit aktiven Attributalertgeneratoren anzeigen und verwalten. Im Fenster **Manager für Attributalertgenerator** werden keine abgelaufenen Attributalertgeneratoren angezeigt.

Ablaufdatum
Zeigt das Datum an, an dem der Attributalertgenerator abläuft.

Erstellungsdatum
Zeigt das Datum an, an dem der Attributalertgenerator erstellt wurde.

Entitäts-ID
Entitäts-ID der Suchentität, die anhand der Kriterien für den Attributalertgenerator erstellt wurde.

Ursache
Ursachencode, der während des Erstellungsprozesses für den Attributalertgenerator zugeordnet wird.

Mindestauflösungsbewertung
Zeigt die Mindestauflösungsbewertung an, die Entitäten beim Vergleich der Attributalertkriterien mit vorhandenen Entitäten in der Entitätendatenbank aufweisen müssen, bevor ein Attributalert für diese Entität generiert wird.

Fallnummer
Zeigt die Fallnummer an, die während des Erstellungsprozesses für den Attributalertgenerator zugeordnet wird.

Schaltfläche 'Erstellen'
Zeigt das Fenster **Attributalertgenerator erstellen** an, in dem Sie einen Attributalertgenerator erstellen können.

Schaltfläche 'Bearbeiten'
Zeigt das Fenster **Attributalertgenerator - Informationen** an, in dem Sie den ausgewählten Attributalertgenerator bearbeiten können. (Wählen Sie den Attributalertgenerator aus und klicken Sie anschließend diese Schaltfläche an.)

Fenster 'Attributalertgenerator erstellen':

In diesem Fenster können Sie einen Attributalertgenerator erstellen, der angegebene Attributkriterien verwendet, um in der Entitätendatenbank permanent nach Entitäten mit übereinstimmenden Attributdaten zu suchen.

Datenquellencode - Beschreibung
Wählen Sie einen Datenquellencode und eine Beschreibung aus der Dropdown-Liste aus, um sie den von diesem Attributalertgenerator erstellten Attributalerts zuzuordnen. Die Standardauswahl ist in der Regel auf **Suchen** gesetzt.

Mindestauflösungsbewertung
Wählen Sie die Mindestauflösungsbewertung aus der Dropdown-Liste aus, die beim Vergleich von Identitäten mit den für den Attributalertgenerator angegebenen Kriterien verwendet werden soll.

Ursachencode
Wählen Sie einen Ursachencode aus der Dropdown-Liste aus, den Sie diesem Attributalertgenerator zuordnen wollen.

Fallnummer
Geben Sie eine optionale Fallnummer für Attributalerts an, die von diesem Attributalertgenerator erstellt wurden.

Kommentar
Geben Sie einen optionalen Kommentar für Attributalerts an, die von diesem Attributalertgenerator erstellt wurden.

Ablaufdatum
Wählen Sie das Datum aus, an dem dieser Attributalertgenerator abläuft, oder klicken Sie das Kalendersymbol an und wählen Sie mithilfe der Kalendersteuerung ein Datum aus. Das Ablaufdatum liegt standardmäßig sechs Monate nach dem aktuellen Datum. Da Attributalertgeneratoren stets im Hintergrund ausgeführt werden, ist es hilfreich, ein Ablaufdatum festzulegen.

Abschnitt mit den Attributkriterien
Geben Sie die Attribute an, die einen Attributalert immer dann generieren sollen, wenn das System einen Identitätsdatensatz mit den angegebenen Attributen verarbeitet.

Namensliste
Geben Sie die Namenskriterien in die Felder der Namensliste ein, wenn Sie einen bestimmten Namen suchen.

Adressliste
Geben Sie die Namenskriterien in die Felder der Adressliste ein, wenn Sie einen bestimmten Namen suchen.

Nummernliste
Geben Sie die Nummernkriterien in die Felder der Nummernliste ein, wenn Sie eine bestimmte Nummer suchen, beispielsweise eine Pass- oder Kreditkartennummer.

Merkmalliste
Geben Sie die Merkmalkriterien in die Felder der Merkmalliste ein, wenn Sie ein bestimmtes Merkmal suchen, beispielsweise das Geschlecht oder das Geburtsdatum.

E-Mail-Liste
Geben Sie die Kriterien für die E-Mail-Adresse in die Felder der E-Mail-Adressliste ein, wenn Sie eine bestimmte E-Mail-Adresse suchen.

Fenster 'Attributalertgenerator - Informationen':

In diesem Fenster können Sie einen vorhandenen Attributalertgenerator bearbeiten. Sie können nur die Fallnummer, das Ablaufdatum und die Kommentare ändern.

Ursachencode
(Nur Anzeige) Zeigt den für diesen Attributalertgenerator ausgewählten Ursachencode an.

Fallnummer
Zeigt die optionale alphanumerische Fallnummer an, die von dem Benutzer eingegeben wird, der den Attributalertgenerator erstellt hat.

Kommentar
Zeigt alle Kommentare an, die vom Benutzer eingegeben wurden, der den Attributalertgenerator erstellt hat.

Ablaufdatum
Zeigt das aktuelle Ablaufdatum für den Attributalertgenerator an.

Verwendete Namen
(Nur Anzeige) Wenn Namensinformationen als Kriterien für diesen Attributalertgenerator eingegeben wurden, werden in diesem Abschnitt alle Namensinformationen aufgeführt, die vom Benutzer eingegeben wurden, der den Attributalertgenerator erstellt hat.

Adresse
(Nur Anzeige) Wenn Adressinformationen als Kriterien für diesen Attributalertgenerator eingegeben wurden, werden in diesem Abschnitt alle Adressinformationen aufgeführt, die vom Benutzer eingegeben wurden, der den Attributalertgenerator erstellt hat.

Nummern
(Nur Anzeige) Wenn Nummerninformationen als Kriterien für diesen Attributalertgenerator eingegeben wurden, werden in diesem Abschnitt alle Nummerninformationen aufgeführt, die vom Benutzer eingegeben wurden, der den Attributalertgenerator erstellt hat.

Andere Attribute
(Nur Anzeige) Wenn Merkmalinformationen als Kriterien für diesen Attributalertgenerator eingegeben wurden, werden in diesem Abschnitt alle Merkmalinformationen aufgeführt, die vom Benutzer eingegeben wurden, der den Attributalertgenerator erstellt hat.

Schaltfläche 'Aktualisieren'
Klicken Sie diese Schaltfläche an, um Ihre Änderungen auszuführen.

Analysieren von Entitäten

Mit Visualizer können Sie Prüfungen und Analysen durchführen und Entitäten in der Entitätendatenbank grafisch darstellen.

Entitäten

Eine Entität ist eine Sammlung von mindestens einer Identität, die für dieselbe Person, dasselbe Unternehmen, denselben Bereich oder dasselbe Element stehen. Entitäten werden in der Entitätendatenbank gespeichert.

Obwohl Entitäten häufig mit Menschen assoziiert werden, können sie ebenso gut Gegenstände wie Unternehmen oder Fahrzeuge sein. Sie können die Daten Ihres Unternehmens sogar mithilfe der erweiterbaren Systemkonfiguration zuordnen und jede beliebige Art von Entität erstellen, die aufgelöst werden oder in Beziehung gesetzt werden soll.

Entitäten setzen sich häufig aus Identitäten zusammen, die aus mehreren verschiedenen Quellensystemen kommen. Die Entitätsauflösung ermittelt, welche Identitäten wirklich dieselbe Entität aufweisen, und erstellt eine zusammengesetzte Entität, die alle Identitäten enthält, die dieser zusammengesetzten Entität zugeordnet sind. Das System wahrt die Möglichkeit zur vollständigen Zurückführung der Datensätze auf die ursprüngliche Datenquelle und gibt die Quelle an, die jeder Identität in der zusammengesetzten Entität zugeordnet ist.

Sie konfigurieren das System derart, dass Entitäten so aufgelöst werden und in Beziehung zueinander gesetzt werden, dass sie die Ziele Ihres Unternehmens erfüllen.

Entitätszusammenfassungen

Eine Entitätszusammenfassung ist eine vereinheitlichte Sammlung aller Informationen in der Entitätendatenbank zu einer bestimmten Entität.

Entitäten sind in der Entitätendatenbank nach Entitäts-IDs organisiert. Jede Entitäts-ID hat ihre eigene Entitätszusammenfassung.

Sie können Entitätszusammenfassungen in Visualizer anzeigen. Entitätszusammenfassungen können die folgenden Arten von Informationen enthalten:

- Quellendokumentverweise
- Rollen
- Verwendete Namen
- Adressen
- Nummern
- Merkmale
- Offenlegungen
- Zusammengehörige Entitäten
- Rollenalertprotokoll
- Ereignisalertprotokoll
- E-Mail-Adressen

Anzeigen von Entitätszusammenfassungen

Wenn Sie alle Informationen zu einer bestimmten Entität in der Entitätendatenbank anzeigen wollen, können Sie hierzu die Entitätszusammenfassung verwenden.

Informationen zu diesem Vorgang

Sie können von jeder der folgenden Visualizer-Positionen auf eine Entitätszusammenfassung zugreifen:

- Jedes Alertdetailfenster
- Jedes Diagrammfenster
- Jedes Fenster **Suchen nach:**

Vorgehensweise

- Klicken Sie von einem Fenster **Rollenalert-Detail**, einem Fenster **Attributalertdetail** oder einem Fenster **Ereignisalert - Detail** die Option **Entitätszusammenfassung** an.
- Klicken Sie in einem Entitätsdiagramm das Symbol **Entität** für die Entitäts-ID-Informationen, die Sie anzeigen wollen, mit der rechten Maustaste an und wählen Sie **Entitätszusammenfassung**.
- Klicken Sie im Abschnitt **Ergebnisse** eines Fensters **Suchen nach:** die Zeile doppelt an, die die Entität enthält, deren Zusammenfassung Sie anzeigen lassen wollen.

Drucken einer Entitätszusammenfassung

Sie haben verschiedenen Möglichkeiten, einen Ausdruck oder eine PDF-Version einer Entitätszusammenfassung zu erstellen oder die Entitätszusammenfassungsinformationen in eine andere Anwendung, wie z. B. ein Textverarbeitungsprogramm oder ein Tabellenkalkulationsprogramm, zu kopieren.

Vorgehensweise

- Gehen Sie wie folgt vor, um eine Momentaufnahme des Fensters **Entitätszusammenfassung** zu drucken:
  1. Klicken Sie **Drucken** im Fenster **Entitätszusammenfassung** an.
  2. Geben Sie im Druckdialog Ihre Druckeinstellungen an.
  3. Klicken Sie **OK** an.
- Zum Ausgeben der Entitätszusammenfassung in eine PDF-Datei klicken Sie **Bericht** im Fenster **Entitätszusammenfassung** an.
- Gehen Sie wie folgt vor, um die Entitätszusammenfassungsinformationen zu kopieren (drucken) und in eine andere Anwendung einzufügen:
  1. Klicken Sie **Anzeige in Zwischenablage kopieren** im Menü **Bearbeiten** des Fensters **Entitätszusammenfassung** an.

     Anmerkung: Durch Drücken der Tastenkombination **Strg** + **C** werden nur einzelne Feldwerte kopiert.
  2. Fügen Sie den Inhalt der Zwischenablage in die Anwendung ein, die Sie verwenden wollen.
  3. Verwenden Sie die Druckfunktion der Anwendung, um die Entitätszusammenfassungsinformationen zu drucken.

Drucken des aktuellen Fensters

Mit dem Druckbefehl können sie in Visualizer jedes Fenster, einschließlich Diagrammen und Entitätszusammenfassungen, direkt über das Fenster drucken.

Vorgehensweise

1. Wählen Sie in Visualizer im zu druckenden Fenster die Option **Drucken** im Menü **Datei** aus.

2. Geben Sie im Dialog **Drucken** Ihre Druckeinstellungen an.
3. Klicken Sie **OK** an.

Anzeigen von Entitätsdiagrammen

Visualizer zeichnet sich insbesondere durch die Möglichkeit aus, Entitätsbeziehungen und Rollenalertinformationen grafisch darstellen zu können. Das Diagramm liefert eine visuelle Darstellung der Informationen zu der ausgewählten Entität.

Informationen zu diesem Vorgang

Sie können von jeder der folgenden Visualizer-Positionen auf ein Entitätsdiagramm zugreifen:

- Fenster **Entitätszusammenfassung**
- Fenster **Diagramm**
- Fenster **Ereignisalert - Detail**

Vorgehensweise

- Klicken Sie **Diagramm** im Fenster **Entitätszusammenfassung** an.
- Klicken Sie in einem Fenster **Diagramm** das Symbol **Entität** für die Entitäts-ID, deren Informationen Sie anzeigen wollen, mit der rechten Maustaste an und wählen Sie **Entitätsdiagramm anzeigen** aus. Wenn Sie die Entitätszusammenfassung einer Entität in einem Diagramm anzeigen wollen, klicken Sie die Entität mit der rechten Maustaste an und wählen **Entitätszusammenfassung** aus.
- Klicken Sie **Diagramm** in einem Fenster **Ereignisalert - Detail** an.
- Optional: Wenn Sie ändern wollen, wie Informationen in einem Diagramm angezeigt werden, klicken Sie einen leeren Bereich im Diagramm mit der rechten Maustaste an und gehen dann wie folgt vor:
  1. Wählen Sie eine andere Einstellung für **Diagrammlayout** aus, um die Anordnung und Darstellung der Informationen im Diagramm zu ändern.
  2. Wählen Sie eine andere Einstellung für **Zoomen** aus, um die aktuelle Zoomstufe zu ändern.

  Immer wenn Sie Diagrammeinstellungen ändern, werden die neuen Einstellungen als Standardeinstellungen für jedes weitere Diagramm verwendet, das Sie während der aktuellen Visualizer-Sitzung anzeigen.

Anzeigen von Rollenalertdiagrammen

Wenn Sie eine grafische Darstellung der Beziehungen zwischen den Entitäten anzeigen wollen, die in einem Rollenalert erkannt wurden, können Sie ein Rollenalertdiagramm aufrufen.

Vorgehensweise

1. Klicken Sie in Visualizer im Fenster **Alertzusammenfassung** den Rollenalert doppelt an.
2. Klicken Sie **Diagramm** in der Anzeige **Rollenalert-Detail** an.
3. Optional: Wenn Sie ändern wollen, wie Informationen in einem Diagramm angezeigt werden, klicken Sie einen leeren Bereich im Diagramm mit der rechten Maustaste an und gehen dann wie folgt vor:
   a. Wählen Sie eine andere Einstellung für **Diagrammlayout** aus, um die Anordnung und Darstellung der Informationen im Diagramm zu ändern.
   b. Wählen Sie eine andere Einstellung für **Zoomen** aus, um die aktuelle Zoomstufe zu ändern.

Immer wenn Sie Diagrammeinstellungen ändern, werden die neuen Einstellungen als Standardeinstellungen für jedes weitere Diagramm verwendet, das Sie während der aktuellen Visualizer-Sitzung anzeigen.

4. Optional: Wenn Sie die Entitätszusammenfassung einer Entität in einem Diagramm anzeigen wollen, klicken Sie die Entität mit der rechten Maustaste an und wählen **Entitätszusammenfassung** aus.

Anpassen von Diagrammsymbolen

Alle Diagramme in Visualizer verwenden vordefinierte Symbole zur Darstellung von Entitäten und der Attributtypen wie Adressen und Zahlen. Sie können die Symbole, die in Visualizer-Diagrammen angezeigt werden, anpassen oder auch ein für einen neuen Attributtyp zu verwendendes Symbol angeben.

Vorbereitende Schritte

Beachten Sie vor dem Anpassen von Visualizer-Diagrammsymbolen folgende Einschränkungen:

- Benutzerdefinierte Symbole befinden sich auf dem Anwendungsserver. Nur Benutzer, die Verwaltungsberechtigungen für den Anwendungsserver besitzen, können benutzerdefinierte Diagrammsymbole hinzufügen oder ändern. Alle auf diesem Anwendungsserver basierenden Visualizer-Clients verwenden dieselbe Symbolgruppe; das heißt, die von Ihnen vorgenommene Änderung hat Auswirkung darauf, welche Symbole in Visualizer-Diagrammen für jeden dieser Clients angezeigt werden.
- Speichern Sie benutzerdefinierte Symbole in einen separaten Symbolordner auf dem Anwendungsserver. Bei der Installation einer neuen Datei *.EAR für den Visualizer werden alle benutzerdefinierten Diagrammsymbole entfernt. Nach Installieren einer neuen Visualizer-Datei *.EAR können Sie die benutzerdefinierten Diagrammsymbole aus dem Symbolordner in den Symbolordner des angegebenen Anwendungsservers kopieren.
- Symbole müssen im .GIF-Format vorliegen. Empfohlen wird eine Bildgröße von 24 x 24 Pixel.
- Die Namen der Symbole müssen ihrem jeweiligen Attributtyp entsprechen (ausschließlich in Kleinbuchstaben). Wenn Sie zum Beispiel einen neuen Attributtyp mit dem Namen 'Evidence Photo' hinzufügen, muss die Datei den Namen 'Evidence Photo.gif' erhalten, damit Visualizer das benutzerdefinierte Beweisfoto erkennt. Wie in diesem Beispiel zu sehen ist, enthält sowohl der Name des Attributtyps als auch der Name der Symboldatei ein Leerzeichen.

Informationen zu diesem Vorgang

Standardsymbolbilddateien von Visualizer werden auf dem Anwendungsserver gespeichert, und zwar in der Regel in einem Ordner mit dem Namen `images`.

Vorgehensweise

1. Stoppen Sie den Anwendungsserver.
2. Navigieren Sie auf dem Anwendungsserver zum Standarddiagrammsymbolordner von Visualizer. In der Regel befindet sich dieser Ordner im Verzeichnis *`Installationspfad für IBM Infosphere Identity Insight-Anwendungsserver`*`/was_apps/ibm-is-ii-visualizer.ear/eas-visualizer-client.war/images`.
3. Erforderlich: Erstellen Sie für Ihre benutzerdefinierten Diagrammsymbolbilddateien einen Ordner mit dem Namen `graph` unter dem Standarddiagrammsymbolordner von Visualizer (Ordner `/images`).

Anmerkung: Der Ordner muss den Namen graph erhalten.

4. Speichern, kopieren oder versetzen Sie jede Symbolbilddatei in den neuen Ordner.

Beispiel

Wenn Sie einen Attributtyp mit dem Namen FINGERPRINT_FILE erstellt haben und wollen, dass dieser Attributtyp in den Visualizer-Diagrammen durch ein benutzerdefiniertes Diagrammsymbol dargestellt wird, führen Sie die folgenden Schritte aus:

1. Erstellen Sie für die Darstellung des Attributtyps FINGERPRINT_FILE eine geeignete .GIF-Bilddatei (24 x 24 Pixel) oder stellen Sie eine entsprechende Bilddatei bereit. Stellen Sie sicher, dass der Name der Bilddatei dem Namen des Attributtyps entspricht und nur Kleinbuchstaben enthält (wie zum Beispiel der folgende Dateiname: fingerprint_file.gif
2. Navigieren Sie auf dem IBM InfoSphere Identity Insight-Anwendungsserver zum Ordner images. Im vorliegenden Beispiel befindet sich der Bildordner im Verzeichnis IBM-II_install/ was_apps/ibm-is-ii-visualizer.ear/eas-visualizer-client.war/images.
3. Erstellen Sie unter dem Bildordner einen Ordner mit dem Namen graph. Der Dateipfad lautet somit wie folgt: IBM-II_install/ was_apps/ibm-is-ii-visualizer.ear/eas-visualizer-client.war/images/graph
4. Kopieren Sie das Bildsymbol fingerprint_file.gif in den Ordner graph.

Nächste Schritte

Führen Sie einen Neustart des Anwendungsservers aus.

Hilfethemen

Anzeige 'Entitätszusammenfassung':

In dieser Anzeige können Sie alle bekannten Informationen zu einer Entität im Detail prüfen, einschließlich der Attribute der Identitäten, die der Entität zugeordnet sind, aller zusammengehöriger Entitäten sowie der Protokolle aller der Entität zugeordneten Alerts.

Blenden Sie mit den Twisties die Abschnitte der Anzeige ein oder aus, um den Fokus auf ein bestimmtes Detail zu setzen.

Datenquelle - Informationen
: Zeigt die Datenquellen mit den Identitätsdatensätzen an, die in diese Entität aufgelöst wurden. Klicken Sie eine Datenquelle an, um die Attribute hervorzuheben, die den Identitätsdatensatz bilden, der von dieser Datenquelle verarbeitet wurde. Informationen zu Datenquellen helfen Ihnen dabei, die Identitätsdatensätze zu ihrer ursprünglichen Quelle zurückzuverfolgen.

  Wenn Entitäten mehrere Identitäten haben, ist die Hervorhebung möglicherweise hilfreich, um eine Identität von der anderen sowie von der ursprünglichen Datenquelle, aus der diese Identität stammt, unterscheiden zu können.

Rollen
: Zeigt die Rollen an, die den Identitäten zugeordnet sind, die in diese Entität aufgelöst wurden.

Namen
Zeigt die Namen an, die von den Identitäten verwendet werden, die in diese Entität aufgelöst wurden.

Adressen
Zeigt die bekannten Adressen an, die von den Identitäten verwendet werden, die in diese Entität aufgelöst wurden, einschließlich des Datumsbereichs, innerhalb dessen jede Adresse für die Identität gültig war (wenn diese Information verfügbar ist).

Nummern
Zeigt die bekannten Nummern an, die von den Identitäten verwendet werden, die in diese Entität aufgelöst wurden, einschließlich des Datumsbereichs, innerhalb dessen jede Nummer für die Identität gültig war (wenn diese Information verfügbar ist).

Merkmale
Zeigt die bekannten Merkmale an, die von den Identitäten verwendet werden, die in diese Entität aufgelöst wurden, einschließlich des Datumsbereichs, innerhalb dessen jedes Merkmal für die Identität gültig war (wenn diese Information verfügbar ist).

E-Mail-Adressen
Zeigt die bekannten E-Mail-Adressen an, die von den Identitäten verwendet werden, die in diese Entität aufgelöst wurden, einschließlich des Datumsbereichs, innerhalb dessen jede E-Mail-Adresse für die Identität gültig war (wenn diese Information verfügbar ist).

Offenlegungen
Zeigt offengelegte Beziehungen an, die von einem Analysten oder autorisierten Visualizer-Benutzer explizit hinzugefügt wurden, um zwei Identitäten zu verknüpfen. Offenlegungen erstellen eine Beziehung mit 100% Relevanz zwischen zwei Identitäten.

Zusammengehörige Entitäten
Führt Basisinformationen zu anderen Entitäten auf, die zu dieser Entität gehören. Wählen Sie eine zusammengehörige Entität aus, um die Informationen hervorzuheben, mit denen die Beziehung erstellt wurde.

Rollenalertprotokoll
Führt Basisinformationen zu den Rollenalerts auf, die dieser Entität zugeordnet sind.

Ereignisalertprotokoll
Zeigt Informationen zu den Ereignisalerts an, die dieser Entität zugeordnet sind.

Schaltfläche 'Drucken'
Öffnet den Druckdialog, damit Sie die Entitätszusammenfassung drucken können.

Schaltfläche 'Bericht'
Generiert einen Entitätszusammenfassungsbericht, der alle Informationen aus der Entitätszusammenfassung enthält.

Anzeige 'Entitätsbeziehungsdiagramm':

In dieser Anzeige können Sie eine grafische Darstellung von Beziehungsdetails für die ausgewählte Entität aufrufen, einschließlich der Entitätsattribute, zusammengehöriger Entitäten und Entitätsereignissen.

Diagrammbereich (Erstellungsbereich)

Der Hauptteil des Diagramms wird als Erstellungsbereich bezeichnet. Er enthält die grafische Darstellung der Beziehungen und zeigt an, welche Attribute die Entitäten miteinander verknüpfen.

Klicken Sie die Objekte (Knoten) im Diagramm an, um ihre Position zu ändern. Wenn ein Hyperlinkattribut vorhanden ist, klicken Sie bei gedrückter Taste **Strg**, um dem Link zu folgen.

Kontextmenüoptionen

Diagrammlayout
Ändert das aktuelle Layout und die Position der Diagrammknoten. Jedes Objekt im Diagramm wird als ein Knoten aufgefasst.

Experimentieren Sie mit den Einstellungen für das Diagrammlayout, bis Sie die für Sie optimalen Einstellungen gefunden haben. Sie können diese Einstellungen bei der Prüfung der Entitätsbeziehungen in diesem Diagramm ganz nach Ihren persönlichen Präferenzen oder Anforderungen festlegen.

Anneal
Wählen Sie diese Einstellung aus, um Knoten gleichmäßig zu verteilen. Durch die Einstellung **Anneal** werden Diagrammkantenlängen vereinheitlicht und Linienschnittpunkte minimiert. Außerdem verhindert diese Einstellung, dass Knoten den Kanten des Diagramms zu nahe kommen.

Hierarchisch
Wählen Sie diese Einstellung aus, um Knoten entsprechend der Hierarchie anzuzeigen. Die Einstellung **Hierarchisch** eignet sich am besten für gerichtete Diagramme, die einen Gesamtfluss haben. Dies bedeutet, dass sie mindestens einen Startpunkt, mindestens einen Endpunkt und einen Gesamtfluss zwischen diesen Punkten haben.

Organisch
Wählen Sie diese Einstellung aus, um Diagrammscheitelpunkte gleichmäßig zu verteilen. Die Einstellung **Organisch** vereinheitlicht Kantenlängen und spiegelt die Diagrammsymmetrie wider, lässt jedoch die Anzeige zusammengehöriger Entitäten nicht zu.

Selbstorganisierend
Wählen Sie diese Einstellung aus, um einheitlich angeordnete Cluster verknüpfter Diagrammknoten zu erstellen.

Zufällig
Wählen Sie diese Einstellung aus, um Diagrammknoten zufällig zu verteilen.

Geneigt
Wählen Sie diese Einstellung aus, um die Anordnung der Diagrammknoten des zuvor zugewiesenen Diagrammlayouts zu verschieben oder zu neigen.

Kreis Wählen Sie diese Einstellung aus, um Diagrammknoten in einem Kreis mit gleichmäßigen Abständen zwischen den benachbarten Diagrammknoten anzuordnen.

Zoomen
Wählen Sie diese Einstellung aus, um die Anzeigegröße des Erstellungsbereichs unter Beachtung der aktuellen Fenstergröße zu ändern.

75 % Zeigt das Diagramm mit 75 % seiner ursprünglichen Größe an.

50 % Zeigt das Diagramm mit 50 % seiner ursprünglichen Größe an.

Alle Attribute anzeigen
Zeigt alle Attribute an, die dieser Entität zugeordnet sind.

Attribut ausblenden
Blendet das ausgewählte Attribut aus.

Zusammengehörige Entitäten anzeigen
Zeigt alle anderen Entitäten, die mit dieser Entität in Beziehung stehen, sowie eine grafische Darstellung der Art der Beziehung an. Diese Option ist nicht verfügbar, wenn die aktuelle Einstellung für das Diagrammlayout **Organisch** lautet.

Entitätszusammenfassung
Öffnet das Fenster **Entitätszusammenfassung** und zeigt eine detaillierte Zusammenfassung aller Informationen an, die zu dieser Entität bekannt sind.

Entitätsereignisse
Öffnet die Anzeige **Entitätsereignisse** und zeigt Informationen zu den Ereignisse an, die der Entität zugeordnet sind. Diese Option ist nur verfügbar, wenn die ausgewählte Entität zugeordnete Ereignisse aufweist.

Entitätsdiagramm anzeigen
Öffnet das Fenster **Entitätsdiagramm** und zeigt eine grafische Darstellung der Informationen nur zu dieser Entität an.

Optionen für die Diagrammanpassung

Zoomschiebeleiste
Verschieben Sie den Zoomanzeiger, um die Größe des Erstellungsbereichs zu ändern.

Layoutvorgabe
Wählen Sie eine Vorgabe für Layoutgrenzen aus, um die Größe des Erstellungsbereichs festzulegen.

Eigenschaftentabelle

Wählen Sie einen Knoten im Diagramm aus. In dieser Tabelle werden daraufhin die Eigenschaften des ausgewählten Knoten (Attribute oder Entitäten) angezeigt.

Anzeige 'Rollenalertdiagramm':

In dieser Anzeige können Sie eine grafische Darstellung von Rollenalertdetails für die ausgewählte Entität aufrufen, einschließlich der Entitätsattribute, zusammengehöriger Entitäten und Entitätsereignissen.

Diagrammbereich (Erstellungsbereich)

Der Hauptteil des Diagramms wird als Erstellungsbereich bezeichnet. Er enthält die grafische Darstellung der Details des Rollenalerts.

Klicken Sie die Objekte (Knoten) im Diagramm an, um ihre Position zu ändern. Wenn ein Hyperlinkattribut vorhanden ist, klicken Sie bei gedrückter Taste **Strg**, um dem Link zu folgen.

Kontextmenüoptionen

Über das Kontextmenü können Sie die grafische Anzeige steuern und es enthält Optionen, mit denen Sie zu den Fenstern für zusammengehörige Entitäten navigieren können.

Diagrammlayout
Ändert das aktuelle Layout und die Position der Diagrammknoten. Jedes Objekt im Diagramm wird als ein Knoten aufgefasst.

Experimentieren Sie mit den Einstellungen für das Diagrammlayout, bis Sie die für Sie optimalen Einstellungen gefunden haben. Sie können diese Einstellungen bei der Prüfung der Rollenalerts in diesem Diagramm ganz nach Ihren persönlichen Präferenzen oder Anforderungen festlegen.

Anneal
Wählen Sie diese Einstellung aus, um Knoten gleichmäßig zu verteilen. Durch die Einstellung **Anneal** werden Diagrammkantenlängen vereinheitlicht und Linienschnittpunkte minimiert. Außerdem verhindert diese Einstellung, dass Knoten den Kanten des Diagramms zu nahe kommen.

Hierarchisch
Wählen Sie diese Einstellung aus, um Knoten entsprechend der Hierarchie anzuzeigen. Die Einstellung **Hierarchisch** eignet sich am besten für gerichtete Diagramme, die einen Gesamtfluss haben. Dies bedeutet, dass sie mindestens einen Startpunkt, mindestens einen Endpunkt und einen Gesamtfluss zwischen diesen Punkten haben.

Organisch
Wählen Sie diese Einstellung aus, um Diagrammscheitelpunkte gleichmäßig zu verteilen. Die Einstellung **Organisch** vereinheitlicht Kantenlängen und spiegelt die Diagrammsymmetrie wider, lässt jedoch die Anzeige zusammengehöriger Entitäten nicht zu.

Selbstorganisierend
Wählen Sie diese Einstellung aus, um einheitlich angeordnete Cluster verknüpfter Diagrammknoten zu erstellen.

Zufällig
Wählen Sie diese Einstellung aus, um Diagrammknoten zufällig zu verteilen.

Geneigt
Wählen Sie diese Einstellung aus, um die Anordnung der Diagrammknoten des zuvor zugewiesenen Diagrammlayouts zu verschieben oder zu neigen.

Kreis Wählen Sie diese Einstellung aus, um Diagrammknoten in einem Kreis mit gleichmäßigen Abständen zwischen den benachbarten Diagrammknoten anzuordnen.

Zoomen
Wählen Sie diese Einstellung aus, um die Anzeigegröße des Erstellungsbereichs unter Beachtung der aktuellen Fenstergröße zu ändern.

75 % Zeigt das Diagramm mit 75 % seiner ursprünglichen Größe an.

50 % Zeigt das Diagramm mit 50 % seiner ursprünglichen Größe an.

Alle Attribute anzeigen
Zeigt alle Attribute an, die dieser Entität zugeordnet sind.

Attribut ausblenden
Blendet das ausgewählte Attribut aus.

Zusammengehörige Entitäten anzeigen
Zeigt alle anderen Entitäten, die mit dieser Entität in Beziehung stehen, sowie eine grafische Darstellung der Art der Beziehung an. Diese Option ist nicht verfügbar, wenn die aktuelle Einstellung für das Diagrammlayout **Organisch** lautet.

Entitätszusammenfassung
Öffnet das Fenster **Entitätszusammenfassung** und zeigt eine detaillierte Zusammenfassung aller Informationen an, die zu dieser Entität bekannt sind.

Entitätsereignisse
Öffnet die Anzeige **Entitätsereignisse** und zeigt Informationen zu den Ereignisse an, die der Entität zugeordnet sind. Diese Option ist nur verfügbar, wenn die ausgewählte Entität zugeordnete Ereignisse aufweist.

Entitätsdiagramm anzeigen
Öffnet das Fenster **Entitätsdiagramm** und zeigt eine grafische Darstellung der Informationen nur zu dieser Entität an.

Optionen für die Diagrammanpassung

Zoomschiebeleiste
Verschieben Sie den Zoomanzeiger, um die Größe des Erstellungsbereichs zu ändern.

Layoutvorgabe
Wählen Sie eine Vorgabe für Layoutgrenzen aus, um die Größe des Erstellungsbereichs festzulegen.

Eigenschaftentabelle

Wählen Sie einen Knoten im Diagramm aus. In dieser Tabelle werden daraufhin die Eigenschaften des ausgewählten Knoten (Attribute oder Entitäten) angezeigt.

Hinzufügen von Daten über Visualizer

Entitätsdaten werden in der Regel von Systembedienern mithilfe einer UMF-Datendatei im Stapelbetrieb oder über Echtzeitverarbeitung in die Pipelines geladen. Visualizer-Benutzer können jedoch Visualizer verwenden, um eine einzelne Entität manuell hinzuzufügen, eine Beziehung zwischen zwei Entitäten (durch Identität) offenzulegen, eine UMF-Datendatei zu laden und zu verarbeiten oder eine UMF-Datendatei vor dem Laden zu prüfen.

Vorbereitende Schritte

Das Hinzufügen von Daten erfordert generell eine verfügbare, aktive Pipeline, damit die Daten verarbeitet werden können. Visualizer-Benutzer müssen jedoch nicht ihre eigene Pipeline starten oder ausführen. Beim Hinzufügen von Daten durch Visualizer, sendet Visualizer die Daten automatisch über eine angegebene Visualizer-Pipeline.

Hinzufügen einer einzelnen Entität

Sie können der Entitätendatenbank eine einzelne Entität hinzufügen, ohne einen UMF-Datensatz manuell zu erstellen. Sie können eine Entität nur mit der Namensinformation erstellen; es ist allerdings empfehlenswert, so viele bekannte Informationen zur Entität (bekannte Adressen, Zahlen, Merkmale oder E-Mail-Adressen) wie möglich einzugeben, um eine optimale Entitäts- und Beziehungsauflösung zu gewährleisten.

Vorgehensweise

1. Führen Sie einen der folgenden Schritte in Visualizer aus:
   a. Klicken Sie **Anzeigen** > **Hinzufügen** > **Entität** an.
   b. Klicken Sie in der Symbolleiste das Symbol für Hinzufügen an und wählen Sie **Entität** aus.
   c. Klicken Sie in der Symbolleiste den Pfeil an und wählen Sie **Entität** aus.
   d. Wählen Sie **Entität** in der Dropdown-Liste **Hinzufügen** des Fensters **Hinzufügen** aus.
2. Verwenden Sie die Dropdown-Listen und Felder, um die Informationen zur Entität einzugeben. Bei der Dateneingabe werden Sie durch Hervorhebung der erforderlichen Felder in Gelb durch die Anzeige geführt. Basierend auf Ihren anderen Auswahlen in dieser Anzeige werden Felder gelb hervorgehoben, in die Sie Daten eingeben müssen.
   - Feld **Verweis**: In dieses Feld müssen Sie Informationen eingeben. Die Referenzinformationen sind eine Kennung für die Identität. Geben Sie zum Beispiel die Nummer des Datenquellenbenutzerkontos (z. B. ein Bankkonto) ein.
   - Namensfelder: Wenn Sie einen Teil des Namens (Vorname, zweiter Vorname oder Generation) eingeben, ist der Nachname erforderlich.
   - Adressfelder: In das Feld **Adresse** können Sie Informationen hinzufügen, ohne den Ort, den Bundesstaat, die Postleitzahl oder das Land eingeben zu müssen. Bei der Eingabe eines anderen Teils der Adresse ist eine Eingabe von Informationen in das Feld **Adresse** jedoch erforderlich.
   - Zahlen-, Merkmals- oder E-Mail-Felder: Wenn Sie in eines dieser Attribute Informationen eingeben wollen, müssen Sie für das Attribut einen Typ auswählen und einen Wert eingeben.

   Achtung: Alle von Ihnen in dieser Anzeige eingegebenen Informationen werden Bestandteil der Entität, die Sie hinzufügen. Sie geben keine Beziehungen mit anderen Entitäten oder gemeinsam genutzte Merkmale oder Zahlen an. Geben Sie nur Informationen an, die sich auf die Entität beziehen, die Sie hinzufügen, wie Aliasnamen oder andere zur Entität gehörigen Namen und Adressen, Zahlen, Merkmale sowie E-Mail-Adressen, die der Entität zugeordnet sind.
3. Klicken Sie **Übergeben** an.

Ergebnisse

Visualizer erstellt einen UMF-Identitätsdatensatz, der sämtliche Informationen enthält, die Sie für diese Entität eingegeben haben, und sendet den Datensatz an eine Pipeline, wo sie zur Entitäts- und Beziehungsauflösung verarbeitet und der Entitätendatenbank hinzugefügt wird.

Laden von Daten aus einer Datei

Über die Funktion **Laden von Datei** in Visualizer können Sie Daten für mehrere, in einer UMF-Datei definierten Identitäten laden. Mit **Laden von Datei** werden nur Datensätze vom Typ `<UMF_ENTITY>` geladen. Wenn Sie eine UMF-Datei auswählen,

öffnet das System die Datei und lädt die Daten in die Pipeline. Anschließend verarbeitet die Pipeline die Identitäten in der Datei. Dabei werden die Identitäten der Entitätendatenbank hinzugefügt und Entitäten sowie identifizierte Beziehungen aufgelöst. Alerts werden auf der Grundlage der konfigurierten Regeln generiert.

Informationen zu diesem Vorgang

Die Entitäten- und Beziehungsauflösung findet in der Pipelinekomponente statt. Wenn UMF-Dateien über Visualizer geladen und verarbeitet werden sollen, muss eine Pipeline aktiv sein und dem Visualizer-Server für die Kommunikation zur Verfügung stehen.

Vor dem Laden einer Datei ist es empfehlenswert, für die Datei eine UMF-Prüfung durchzuführen, um sicherzustellen, dass die Datei keine Fehler enthält.

Vorgehensweise

1. Führen Sie eine der folgenden Aktionen in Visualizer aus:
   a. Klicken Sie **Anzeigen** > **UMF** > **Laden von Datei** an.
   b. Klicken Sie in der Symbolleiste das Symbol für UMF an.
   c. Wählen Sie im Fenster **UMF** aus dem Dropdown-Feld **UMF** die Option **Laden von Datei** aus.
2. Klicken Sie **Laden von Datei...** an, um die zu ladende UMF-Datei auszuwählen, und klicken Sie dann **Öffnen** an. Das System lädt die ausgewählte Datei in die Pipeline und diese beginnt die Daten in der Datei zu verarbeiten. Die Dateifortschrittsleiste zeigt die während der Verarbeitung abgelaufene Zeit, die Anzahl der verarbeiteten Datensätze und den Status des Dateiladevorgangs an.
   a. Zum Stoppen des Dateilade- und Dateiverarbeitungsvorgangs, klicken Sie die Schaltfläche für das Symbol für Stopp an.
   b. Zum Anhalten des Dateilade- und Dateiverarbeitungsvorgangs, klicken Sie die Schaltfläche für das Symbol für Anhalten an.
   c. Zum Fortsetzen eines angehaltenen Dateilade- und Dateiverarbeitungsvorgangs, klicken Sie die Schaltfläche für das Symbol für Weiter an.

   Beim Laden der Daten in der Datei verarbeitet eine Pipeline die Daten mittels Entität- und Beziehungsauflösung. Tritt ein Fehler auf, wenden Sie sich an Ihren Systemadministrator. Bei dem Fehler handelt es sich höchstwahrscheinlich um einen Pipelinefehler.

   Neue Identitäten werden der Datenbank zusammen mit aufgelösten Entitäten und Beziehungen hinzugefügt. Alerts, die in Zusammenhang mit den Daten stehen, generiert das System auf der Grundlage der konfigurierten Systemregeln.
3. Optional: Wenn das Laden und Verarbeiten der Datei abgeschlossen ist, klicken Sie **Ergebnisse anzeigen** an, um den Dialog **Ergebnisse des Ladens von Datei** anzuzeigen. Dieser enthält die folgenden Informationen:
   - Die Anzahl der an die Pipeline gesendeten Datensätze.
   - Die Anzahl der in der Entitätendatenbank erstellten neuen Entitäten. Diese Angabe basiert auf den Daten in der Datei, die Sie geladen haben.
   - Die Anzahl der UMF-Ausnahmebedingungen, die in der Pipeline beim Verarbeiten der Daten in dieser Datei aufgetreten sind. (Diese Zahl kann auf Fehler in der UMF-Datei oder auf Syntaxprobleme hinweisen, die ein vollständiges Verarbeiten der Daten durch die Pipeline verhindern.)

Nächste Schritte

Weist der Dialog **Ergebnisse des Ladens von Datei** darauf hin, dass in der von Ihnen geladenen Datei UMF-Ausnahmebedingungen aufgetreten sind, prüfen Sie die Datei mithilfe der UMF-Dateiprüfungsfunktion. Diese hilft Ihnen die Fehler in der Datei zu finden, damit Sie sie beheben können. Nachdem Sie die Fehler behoben haben, laden Sie die Daten erneut, in der die Fehler vorhanden waren, damit die Pipeline diese Daten vollständig verarbeiten kann.

Prüfen einer UMF-Datei vor dem Laden der Daten

Wenn Sie planen, mit Visualizer Datensätze in kleinen UMF-Dateien zu laden und zu verarbeiten, ist es empfehlenswert, die Daten in der Datei zuvor zu prüfen.

Informationen zu diesem Vorgang

Der Prüfprozess prüft, ob die Daten die Mindestanforderungen für die Verarbeitung der Entitäts- und Beziehungsauflösung erfüllen. Darüber hinaus stellt der Prüfprozess hilfreiche Informationen zu Bereichen der Datei zur Verfügung, die vor dem Laden und Verarbeiten der Daten geprüft werden müssen. Je höher die Qualität der in das System aufgenommenen Daten ist, desto besser sind die Ergebnisse.

Vorgehensweise

1. Führen Sie eine der folgenden Aktionen in Visualizer aus:
   - Klicken Sie **Anzeigen** > **UMF** > **UMF-Dateiprüfung** an.
   - Klicken Sie in der Symbolleiste den Pfeil rechts neben dem Symbol an und klicken Sie **UMF-Dateiprüfung** an.
   - Wählen Sie **UMF-Dateiprüfung** in der Liste **UMF** im Fenster **UMF** aus.
2. Klicken Sie **Datei prüfen...** an.
3. Wählen Sie die zu prüfende UMF-Datei aus.

   Anmerkung: Wenn Sie bereits mindestens eine UMF-Datei geprüft haben und das Fenster **UMF** anschließend geöffnet geblieben ist, enthalten die beiden Felder **Zu prüfende Datei** und **Fehler-/Warnungsdatei** die Werte aus der letzten UMF-Dateiprüfung.
4. Optional: Wenn Sie den Verzeichnispfad oder Dateinamen der Prüfprozessprotokolldatei im Fenster **UMF-Prüfungskonfiguration** ändern wollen, wählen Sie eine der folgenden Aktionen:
   - Wählen Sie das zu verwendende Verzeichnis und den zu verwendenden Dateinamen aus, klicken Sie **Durchsuchen...** und anschließend **Öffnen** an.
   - Geben Sie den vollständigen Pfad und Dateinamen der Gültigkeitsfehler- und Warnungsprotokolldatei ein. Sie können entweder den Namen einer vorhandenen Protokolldatei oder den Namen einer neuen Protokolldatei eingeben.

   Anmerkung: Wenn Sie mehr als eine UMF-Datei prüfen und dabei das Fenster **UMF** geöffnet halten, werden Sie bemerken, dass für den Protokolldateiwert im Fenster **UMF-Prüfungskonfiguration** standardmäßig der Pfad und Dateiname der letzten Prüffehler- und Prüfwarnungsprotokolldatei angezeigt wird. Durch Schließen des Fensters **UMF** löschen Sie den Inhalt der Pfad- und Protokolldateifelder.
5. Klicken Sie **UMF-Datei prüfen** an, um den Prüfprozess zu starten. Während der Prüfprozess aktiv ist, werden Prüfstatistikdaten angezeigt, einschließlich dynamische Informationen wie Prozentsatz der Fertigstellung des Vorgangs, die

abgelaufene Zeit, die Anzahl der verarbeiteten Datensätze und der Status des Prozesses. Sie können den Prüfprozess jederzeit anhalten oder stoppen.

6. Optional: Wenn Sie **UMF-Datei prüfen** anklicken, wenn bereits eine Prüfprotokolldatei an dem Standort und mit dem Namen vorhanden ist, den Sie in Schritt 4 eingegeben haben, zeigt das System eine diesbezügliche Informationsnachricht. In der Nachricht ist der Name und Standort der Datei angegeben. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie **Ja** an, um dieselbe Prüffehler-/Prüfwarnungsprotokolldatei zu verwenden. Bei dieser Auswahl wird die vorherige Protokolldatei überschrieben.
   - Klicken Sie **Nein** an, um eine andere Prüffehler-/Prüfwarnungsprotokolldatei zu erstellen oder zu verwenden. Das System kehrt zum Fenster **UMF-Prüfungskonfiguration** zurück, sodass Sie den Pfad und Dateinamen der Prüffehler-/Prüfwarnungsprotokolldatei manuell ändern können.
7. Wenn der Prüfprozess abgeschlossen ist, klicken Sie **Ergebnisse anzeigen** an, wenn Sie eine Zusammenfassung der Ergebnisse anzeigen wollen.

Nächste Schritte

Verwenden Sie die Informationen im Fenster **Anzeige der UMF-Prüfergebnisse**, um die Ergebnisse und Informationen in der Fehler- und Warnungsprotokolldatei anzuzeigen.

Offenlegen von Beziehungen zwischen Identitäten

Wenn Sie feststellen, dass Daten vorhanden sind, die zwei Identitäten (oder Benutzerkonten) miteinander verbinden, können Sie angeben, dass diese Verbindung die Beziehung offenlegt. Dies erfolgt über Visualizer.

Vorgehensweise

1. Führen Sie einen der folgenden Schritte in Visualizer aus:
   a. Klicken Sie **Anzeigen** > **Hinzufügen** > **Offenlegung** an.
   b. Klicken Sie in der Symbolleiste den Pfeil rechts neben dem Symbol für Hinzufügen an und wählen Sie **Offenlegung** aus.
   c. Wählen Sie **Offenlegung** in der Dropdown-Liste **Hinzufügen** des Fensters **Hinzufügen** aus.
2. Erforderlich: Geben Sie in den Feldern **Entitäts-ID** die Entitäts-ID-Nummern der Entitäten ein, die die Identitäten enthalten, die in Beziehung zueinander gesetzt werden sollen.
3. Erforderlich: Klicken Sie **Suchfunktion** für jede Entitäts-ID an, um die ihr zugeordneten Identitäten abzurufen. Überprüfen Sie die Liste der abgerufenen Identitäten, um sicherzustellen, dass Sie die gewünschte Entitäts-ID eingegeben haben.
4. Wählen Sie für jede Entität das Optionsfeld der Identität (oder des Datenquellenbenutzerkontos) aus, für die (bzw. für das) Sie eine Beziehung offenlegen.
5. Geben Sie in **Offengelegte Beziehung - Beschreibung** eine Beschreibung der Beziehung zwischen den Identitäten ein.
6. Klicken Sie **Erstellen** an. Ein Bestätigungsfenster wird mit der Nachricht angezeigt, dass die offengelegte Beziehung erfolgreich erstellt wurde.

Hilfethemen

Fenster 'Entität erstellen':

In diesem Fenster können Sie der Entitätendatenbank eine einzelne neue Identität über Visualizer hinzufügen. Alle Informationen, die Sie in dieser Anzeige eingeben, werden zu Attributen der neu erstellten Identität. (Sie erstellen jeweils eine Identität.) Nachdem Sie die für die Identität eingegebenen Daten übergeben haben, verarbeitet das System diese über die Pipeline für die Entitäts- und Beziehungsauflösung. Während dieses Vorgangs kann die Identität weiteren vorhandenen Entitäten zugeordnet werden.

Datenquellencode - Beschreibung

Wählen Sie die Datenquelle aus, die der Identität zugeordnet werden soll, die Sie gerade hinzufügen. Die Datenquelle muss in Ihrem System vorhanden sein. (Sie können an dieser Stelle keine neue Datenquelle hinzufügen. Wenn Sie den Datenquellencode und die Beschreibung, die Sie verwenden wollen, nicht finden können, setzen Sie sich mit Ihrem Systemadministrator in Verbindung, damit dieser die Datenquelle für Sie erstellt.)

Für das Hinzufügen einer Identität sind der Datenquellencode und die Beschreibung erforderlich.

Verweis

Geben Sie eine Kennung für dieses Datenquellenbenutzerkonto ein, mit der das Konto der Identität zugeordnet wird, die Sie gerade eingeben. (Als Referenznummern gelten beispielsweise Fallnummern, Kontonummern und Kundenkartennummern.)

Für das Hinzufügen einer Identität ist ein Verweis erforderlich.

Namensliste

Geben Sie die Namen ein, die der einzelnen Identität zugeordnet werden sollen, die Sie gerade hinzufügen. Für das Hinzufügen einer Identität sind Namensinformationen (zumindest Vor- und Nachname) erforderlich. Sie können mehrere Namen für die Identität angeben, die Sie gerade hinzufügen. Geben Sie dazu jeden Namen der Identität in eine separate Zeile ein. Wenn Sie beispielsweise sowohl den Eigennamen der Identität als auch mindestens einen Aliasnamen ("Andere Bezeichnung") kennen, können Sie all diese Namen in dieser Anzeige eingeben.

Anmerkung: Stellen Sie sicher, dass Sie nur einen Namen pro Zeile eingeben.

Alle in dieser Liste von Ihnen eingegebenen Namen werden der neu erstellten Identität als Attribute dieser Identität automatisch zugeordnet. Wenn Sie z. B. "Robert Hays" und "Bob J. Hayes, Jr." eingeben, werden beide Namen der neu erstellten Identität zugeordnet.

Adressliste

Geben Sie mindestens eine Adresse ein, die der Identität zugeordnet werden soll, die Sie gerade hinzufügen. Wenn Sie beispielsweise die aktuelle und die vorherige Adresse für die Identität kennen, geben Sie die beiden vollständigen Adressen in jeweils eine Zeile ein. Alle von Ihnen in diesem Listenabschnitt eingegebenen Adressen werden automatisch der Identität zugeordnet, die Sie gerade hinzufügen.

Für das Hinzufügen einer Identität sind keine Adressen erforderlich. Wenn keine Adressen für diese Identität bekannt sind, können Sie diesen Listenabschnitt leer lassen.

Adresse

Diese Angabe entspricht in der Regel den in den Zeilen **Adresse 1** und **Adresse 2** eingegebenen Informationen. Beispiel: 555 Main Street Building 17 Suite 102-B

Wenn Sie Daten in eines der Adressfelder eingeben, müssen Sie auch Daten in das Feld **Adresse** eingeben.

Anfangsdatum

Geben Sie das Datum ein, an dem diese Adressinformation für diese Identität gültig wurde (falls bekannt). Wenn die Adresse dieser Identität beispielsweise ab dem 15. März 1999 gültig war, geben Sie dieses Datum ein.

Sie können ein Anfangsdatum ohne ein Enddatum angeben.

Enddatum

Geben Sie das Datum ein, an dem diese Adressinformation für diese Identität ungültig wurde (falls bekannt). Wenn die Adresse dieser Identität beispielsweise ab dem 1. Juni 2001 nicht mehr gültig war, geben Sie dieses Datum ein.

Sie können ein Enddatum ohne ein Anfangsdatum angeben.

Nummernliste

Geben Sie mindestens eine Nummer an, die der Identität zugeordnet ist, die Sie gerade hinzufügen. Wenn Sie z. B. die Daten einer Kreditkarte kennen, die von der Identität verwendet wird, einer Führerscheinnummer, einer Identifikationsnummer, einer Passnummer und einer Telefonnummer, geben Sie diese Nummern jeweils in eine separate Zeile ein. Alle von Ihnen in diesem Listenabschnitt eingegebenen Nummern werden automatisch der Identität zugeordnet, die Sie gerade hinzufügen.

Für das Hinzufügen einer Identität sind keine Nummern erforderlich. Sie können diesen Listenabschnitt daher leer lassen. Wenn Sie jedoch Nummerndaten eingeben, müssen die beiden Felder **Nummerntyp** und **Wert** ausgefüllt werden.

Nummerntyp

Wählen Sie den Nummerntyp aus der Dropdown-Liste der verfügbaren Nummerntypen aus. Diese Nummerntypen müssen in Ihrem System vorhanden sein. (Sie können an dieser Stelle keinen neuen Nummerntyp hinzufügen. Wenn Sie den Nummerntyp, den Sie verwenden wollen, nicht finden können, setzen Sie sich mit Ihrem Systemadministrator in Verbindung, damit dieser den Nummerntyp für Sie erstellt.)

Wenn Sie der Identität, die Sie gerade hinzufügen, eine Nummer zuordnen wollen, müssen Sie einen Nummerntyp auswählen.

Wert Geben Sie den Nummernwert für den ausgewählten Nummerntyp ein. Geben Sie beispielsweise die Passnummer hier ein, wenn Sie dieser Identität einen Pass zuordnen.

Wenn Sie der Identität, die Sie gerade hinzufügen, eine Nummer zuordnen wollen, müssen Sie einen Nummernwert eingeben, der dem Nummerntyp entspricht.

Standort

Geben Sie den Standort ein, der dieser Nummer zugeordnet ist, falls dieser bekannt oder vorhanden ist. Geben Sie hier beispielsweise den Namen des Landes ein, in dem der Pass ausgestellt wur-

de, wenn Sie dieser Identität einen Pass zuordnen. Geben Sie im Fall eines Führerscheins den Namen des Landes ein, in dem er ausgestellt wurde.

Anfangsdatum
Geben Sie das Datum ein, an dem diese Nummer für diese Identität gültig wurde (falls bekannt). Sie können ein Anfangsdatum ohne ein Enddatum angeben.

Enddatum
Geben Sie das Datum ein, an dem diese Nummer für diese Identität ungültig wurde (falls bekannt). Beispiel: Ablaufdatum eines Führerscheins, eines Passes oder einer Kreditkarte.

Sie können ein Enddatum ohne ein Anfangsdatum angeben.

Merkmalliste
Geben Sie mindestens ein Merkmal an, das zur Identität gehört, die Sie gerade hinzufügen, oder dieser zugeordnet ist. Wenn Ihr System z. B. Merkmale wie Geburtsdatum, Familienstand, Augenfarbe oder Größe erfasst, können Sie jedes bekannte Merkmal in jeweils eine Zeile dieser Liste eingeben. Alle von Ihnen in diesem Listenabschnitt eingegebenen Merkmale werden automatisch der Identität zugeordnet, die Sie gerade hinzufügen.

Für das Hinzufügen einer Identität sind keine Merkmale erforderlich. Sie können diesen Listenabschnitt daher leer lassen. Wenn Sie jedoch Merkmaldaten eingeben, müssen alle Merkmalfelder ausgefüllt werden.

Typ Wählen Sie den Merkmaltyp aus der Dropdown-Liste der verfügbaren Typen aus. Der Merkmaltyp muss in Ihrem System vorhanden sein. (Sie können an dieser Stelle keinen neuen Typ hinzufügen. Wenn Sie den Merkmaltyp, den Sie verwenden wollen, nicht finden können, setzen Sie sich mit Ihrem Systemadministrator in Verbindung, damit dieser den Merkmaltyp für Sie erstellt.)

Wenn Sie der Identität, die Sie gerade hinzufügen, ein Merkmal zuordnen wollen, müssen Sie einen Merkmaltyp auswählen.

Wert Geben Sie den Wert des Merkmals ein. Wenn Sie der Identität, die Sie gerade hinzufügen, ein Merkmal zuordnen wollen, müssen Sie einen Merkmalwert eingeben, der dem Merkmaltyp entspricht.

Anfangsdatum
Geben Sie das Datum ein, an dem dieses Merkmal für diese Identität gültig wurde (falls bekannt). Sie können ein Anfangsdatum ohne ein Enddatum angeben.

Enddatum
Geben Sie das Datum ein, an dem dieses Merkmal für diese Identität ungültig wurde (falls bekannt). Sie können ein Enddatum ohne ein Anfangsdatum angeben.

E-Mail-Liste
Geben Sie mindestens eine E-Mail-Adresse an, die zur Identität gehört, die Sie gerade hinzufügen, oder dieser zugeordnet ist. Geben Sie jede bekannte E-Mail-Adresse in diese Liste ein, jeweils eine E-Mail-Adresse pro Zeile. Alle von Ihnen in diesem Listenabschnitt eingegebenen E-Mail-Adressen werden automatisch der Identität zugeordnet, die Sie gerade hinzufügen.

Für das Hinzufügen einer Identität sind keine E-Mail-Adressen erforderlich. Sie können diesen Listenabschnitt daher leer lassen. Wenn Sie jedoch E-Mail-Daten eingeben, müssen die beiden Felder **Typ** und **Adresse** ausgefüllt werden.

Typ Wählen Sie den E-Mail-Adresstyp aus der Dropdown-Liste der verfügbaren Typen aus. Der E-Mail-Adresstyp muss in Ihrem System vorhanden sein. (Sie können an dieser Stelle keinen neuen Typ hinzufügen. Wenn Sie den E-Mail-Adresstyp, den Sie verwenden wollen, nicht finden können, setzen Sie sich mit Ihrem Systemadministrator in Verbindung, damit dieser den E-Mail-Adresstyp für Sie erstellt.)

Wenn Sie der Identität, die Sie gerade hinzufügen, eine E-Mail-Adresse zuordnen wollen, müssen Sie einen Typ auswählen.

Wert Geben Sie die vollständige E-Mail-Adresse ein. Wenn Sie der Identität, die Sie gerade hinzufügen, eine E-Mail-Adresse zuordnen wollen, müssen Sie einen E-Mail-Adresswert eingeben, der dem E-Mail-Adresstyp entspricht.

Anfangsdatum
Geben Sie das Datum ein, an dem diese E-Mail-Adressinformation für diese Identität gültig wurde (falls bekannt). Wenn Sie beispielsweise das Datum kennen, an dem dieser E-Mail-Account geöffnet wurde, können Sie dieses Datum hier eingeben.

Sie können ein Anfangsdatum ohne ein Enddatum angeben.

Enddatum
Geben Sie das Datum ein, an dem diese E-Mail-Adressinformation für diese Identität ungültig wurde (falls bekannt). Wenn Sie beispielsweise das Datum kennen, an dem dieser E-Mail-Account geschlossen wurde, können Sie dieses Datum hier eingeben.

Sie können ein Enddatum ohne ein Anfangsdatum angeben.

Schaltfläche 'Übergeben'
Klicken Sie **Übergeben** an, um die Identität über die Entitäts- und Beziehungsauflösung zu verarbeiten und der Entitätendatenbank hinzuzufügen, wenn Sie alle bekannten und relevanten Informationen zur Identität, die Sie hinzufügen wollen, eingegeben haben.

Schaltfläche 'Zurücksetzen'
Klicken Sie die Schaltfläche **Zurücksetzen** an, um alle in das Fenster eingegebenen Informationen zu löschen, ohne diese zu übergeben. Die Identität wird nicht über die Entitäts- und Beziehungsauflösung verarbeitet und auch nicht der Entitätendatenbank hinzugefügt.

Fenster 'Offenlegung hinzufügen':

In diesem Fenster können Sie eine Beziehung zwischen zwei vorhandenen Identitäten offenlegen. Durch die Offenlegung der Beziehung erstellen Sie eine Verknüpfung sowohl zwischen den Identitäten als auch zwischen den Entitäten, die diese Identitäten enthalten. Die Offenlegung einer Beziehung zeigt, dass die Verknüpfung zwischen diesen zwei Identitäten durch die Entitäts- und Beziehungsauflösung noch nicht festgestellt wurde und dass Sie die zwei Identitäten aus einem bestimmten Grund manuell verknüpfen wollen.

Entitäts-ID
Geben Sie die Entitäts-ID-Nummer der Identitäten ein, die Sie zueinander in Beziehung setzen wollen, wobei Sie jeweils eine Nummer in jedes Feld **Entitäts-ID** eingeben.

Suchfunktion
Klicken Sie, um die Identitätsinformationen zu der von Ihnen eingegebenen Entitäts-ID anzuzeigen. Führen Sie diesen Schritt für beide Entitäts-ID-Nummern aus. Durch das Prüfen der angezeigten Informationen können Sie sicherstellen, dass die Entitäts-IDs den Identitäten entsprechen, die Sie zueinander in Beziehung setzen wollen. Sie können auch die Entitäts-ID für eine oder beide Identitäten vor deren Verknüpfung korrigieren.

Optionsfelder (neben jeder Identität, die einer Entitäts-ID zugeordnet ist)
Wählen Sie eine einzelne Identität für beide Entitäts-IDs aus. Diese IDs stellen die beiden Identitäten dar, die Sie zueinander in Beziehung setzen wollen.

Anmerkung: Ihnen wird möglicherweise nur eine Identität pro Entität angezeigt. Dies bedeutet, dass die Entität zurzeit nur eine Identität im System aufweist.

Offengelegte Beziehung - Beschreibung
Geben Sie eine Beschreibung dazu ein, wie zwei ausgewählte Identitäten verknüpft werden. Diese Beschreibung stellt anderen Visualizer-Benutzern beim Anzeigen dieser Beziehung hilfreiche Informationen bereit. Sie erläutert diesen Benutzern, wie und aus welchem Grund diese zwei Identitäten verknüpft werden.

Erstellen
Klicken Sie **Erstellen** an, um die Beziehung zwischen den zwei ausgewählten Identitäten offenzulegen. Das System sendet die Informationen zu beiden Identitäten zur Verarbeitung über die Pipeline und aktualisiert anschließend die Daten beider Identitäten sowie auch alle diesen Identitäten zugeordneten Entitäten.

Fenster zum Laden der UMF-Datei:

In diesem Fenster können Sie über Visualizer Daten aus einer UMF-Datei in eine Entitätendatenbank laden.

Statusleiste für das Laden der Datei
Wenn Sie eine UMF-Datei ausgewählt haben, die Sie öffnen und laden wollen, klicken Sie die Schaltfläche **Datei laden...** an. Diese Statusleiste zeigt daraufhin den Fortschritt der Verarbeitung der Daten in der Datei an. Das System zeigt Statistikdaten an, einschließlich des Prozentsatzes der abgeschlossenen Verarbeitung, der seit Beginn der Dateiverarbeitung abgelaufenen Zeit sowie des Status der Systemverarbeitung.

Schaltfläche (Weiter)
Wenn Sie den Lade- und Verarbeitungsprozess für die Datei mithilfe der Schaltfläche **(Anhalten)** angehalten haben, klicken Sie diese Schaltfläche an, um die noch nicht verarbeiteten Datensätze in der Datei zu laden und zu verarbeiten. Das System fährt mit dem nächsten Datensatz in der ausgewählten Datei fort.

Schaltfläche (Anhalten)
Klicken Sie diese Schaltfläche an, wenn Sie den Lade- und Verarbeitungsprozess für die Datei vorübergehend anhalten wollen. Die Datei bleibt im Speicher und das System protokolliert, welche Datensätze bereits verarbei-

tet wurden. Die Datensätze in der Datei, die noch nicht verarbeitet wurden, befinden sich erst dann in der Entitätendatenbank, wenn Sie mit dem Laden der Datei fortfahren.

Diese Schaltfläche ist nur aktiv, solange das System die Datei lädt.

Schaltfläche (Stopp)
Klicken Sie diese Schaltfläche an, wenn Sie den Lade- und Verarbeitungsprozess für die Datei stoppen wollen. Die Datei wird daraufhin aus dem Speicher gelöscht. Die Datensätze in der Datei, die noch nicht verarbeitet wurden, sind nicht in der Entitätendatenbank vorhanden. Wenn Sie mit dem Laden von Datensätzen in dieser Datei fortfahren wollen, müssen Sie die Datei erneut laden. Während des erneuten Ladens der Datei werden alle Datensätze, die bereits verarbeitet worden sind, erneut verarbeitet.

Diese Schaltfläche ist nur aktiv, solange das System die Datei lädt.

Schaltfläche 'Ergebnisse anzeigen'
Klicken Sie diese Schaltfläche an, um den Dialog **Ergebnisse des Ladens von Datei** aufzurufen, der folgende Informationen enthält:

- Die Anzahl der an die Pipeline gesendeten Datensätze.
- Die Anzahl der in der Entitätendatenbank erstellten neuen Entitäten. Diese Angabe basiert auf den Daten in der Datei, die Sie geladen haben.
- Die Anzahl der UMF-Ausnahmebedingungen, die in der Pipeline beim Verarbeiten der Daten in dieser Datei aufgetreten sind. (Diese Zahl kann Fehler in der UMF-Datei oder Probleme in der Syntax angeben, die die Pipeline an der vollständigen Verarbeitung der Daten hindern. Bitten Sie Ihren Systemadministrator, die UMF-Ausnahmebedingungen zu korrigieren. Ihr Systemadministrator kann ein Protokoll mit den UMF-Ausnahmebedingungen prüfen, um nähere Informationen zu erhalten.)
- Die Anzahl der erstellten Rollenalerts basierend auf den Daten in der von Ihnen geladenen Datei.

Schaltfläche 'Datei laden...'
Klicken Sie diese Schaltfläche an, um die Datei in die Pipeline zu laden und beginnen Sie mit der Verarbeitung der Datensätze in der Datei für die Entitäts- und Beziehungsauflösung.

Fenster 'UMF-Dateiprüfung':

In diesem Fenster können Sie Daten in einer UMF-Datei prüfen, die Sie laden und über die Entitäts- und Beziehungsauflösung verarbeiten wollen. Wenn Sie die Daten zunächst prüfen, können Sie potenzielle Fehler korrigieren oder Warnungen beheben, bevor Sie die Datei laden und verarbeiten.

Schaltfläche 'Prüfen'
Zeigt das Fenster **UMF-Prüfungskonfiguration** an, in dem Sie die zu prüfende UMF-Datei auswählen, den Pfad und Dateinamen der Fehler- und Warnungsprotokolldatei festlegen und den UMF-Prüfprozess initiieren können.

Wenn Sie das Fenster **UMF-Prüfungskonfiguration** geöffnet lassen und eine andere UMF-Datei prüfen, werden die Pfad- und Protokolldateifelder mit den Speicherpositionen der zuletzt geprüften UMF-Datei sowie der Speicherposition der letzten Fehler- und Warnungsprotokolldatei gefüllt, wenn Sie die Schaltfläche **Prüfen** anklicken. Sie können entweder dieselbe Datei erneut prüfen oder eine neue UMF-Datei für die Prüfung auswählen.

Wenn Sie das Fenster **UMF-Prüfungskonfiguration** schließen, werden die Inhalte der Pfad- und Protokolldateifelder gelöscht.

Ausführen von Berichten über Visualizer

In Visualizer können Sie Berichte anzeigen und drucken, die Zusammenfassungen von Statistikdaten nach Datenquelle anzeigen, sowie Berichte, die Sie bei der Anzeige und Verwaltung von Alerts und offengelegten Beziehungen unterstützen.

Anzeigen und Drucken von Berichten in Visualizer

Verwenden Sie die Berichte in Visualizer, um Statistikdaten und Qualitätszusammenfassungen von Datenquellendateien anzuzeigen, Unterstützung bei der Verwaltung Ihrer zugeordneten Alerts zu erhalten und um Informationen zu offengelegten Beziehungen, Ereignisalerts oder zu Ereignissen zu überprüfen. Sie können die Berichte online anzeigen oder als Dokument ausdrucken.

Informationen zu diesem Vorgang

Auf die meisten Visualizer-Berichte können Sie über das Menü **Anzeigen** oder über die Symbolleiste zugreifen. Einige Berichte dagegen lassen sich nur über eine bestimmte Anzeige anzeigen und drucken, so zum Beispiel der Bericht **Entitätszusammenfassung**oder der **Ereignisalert - Detailbericht**.

Berichte werden in dem von Ihnen ausgewählten Web-Browser mithilfe von Adobe Acrobat Reader angezeigt. Zum Anzeigen und Drucken von Visualizer-Berichten muss Adobe Acrobat Reader Version 7.0 oder höher auf Ihrer Workstation installiert sein.

Anmerkung: Vom System generierte Datumsangaben und Zeitmarken, die über einen Visualizer-Client in Berichte gedruckt werden, werden an die jeweilige Zeitzone des Visualizer-Anwendungsservers angepasst. Beim Aufruf auf dem Bildschirm werden die Datumsangaben an die Zeitzone des Visualizer-Clients entsprechend angepasst korrekt auf dem Bildschirm angezeigt. Beispiel: Ein Visualizer-Client, der sich in der Zeitzone EST (Eastern Standard Time) befindet, ist mit einem Visualizer-Anwendungsserver verbunden, der sich in der Zeitzone PST (Pacific Standard Time) befindet. Beim Visualizer-Client wird auf dem Bildschirm ein systemgeneriertes Datum und die Zeitmarke 20:00 Uhr angezeigt, auf einem über ihn gedruckten Bericht ist jedoch die Zeitangabe 17:00 Uhr vermerkt.

Vorgehensweise

- Gehen Sie zum Anzeigen eines Berichts vom Typ 'Attributalertgenerator - Protokoll', 'Attributalertgenerator', 'Attributalert', 'Datenquelle - Ergebnisbericht', 'Offengelegte Beziehung', 'Laden - Ergebnisbericht' oder 'Rollenalertstatus' wie folgt vor:
  1. Klicken Sie **Anzeigen** > **Berichte** an und wählen Sie dann den Bericht aus, den Sie anzeigen oder drucken wollen.
  2. Geben Sie die Berichtskriterien ein.
  3. Klicken Sie **Bericht ausführen** an, um den ausgewählten Bericht zu generieren.
- Wenn Sie einen Entitätszusammenfassungsbericht anzeigen wollen, klicken Sie **Bericht** in der Anzeige **Entitätszusammenfassung** an.
- Wenn Sie einen Rollenalert-Detailbericht anzeigen wollen, klicken Sie **Bericht** in der Anzeige **Rollenalert-ID** an.
- Wenn Sie einen Ereignisalert-Detailbericht anzeigen wollen, klicken Sie **Bericht** in der Anzeige **Ereignisalert-ID** an.

- Wenn Sie einen Bericht zu allen Ereignissen anzeigen wollen, klicken Sie **Bericht** in der Anzeige **Entitätsereignisse** an.

Ergebnisse

Das System generiert den ausgewählten Bericht auf der Basis aller angegebenen Kriterien und zeigt den Bericht in einem separaten Fenster an. Wenn Sie den Bericht drucken wollen, klicken Sie die Schaltfläche für das Druckersymbol an oder verwenden Sie die Druckfunktion Ihres Web-Browsers.

Bericht 'Attributalertgenerator - Protokoll':

Im Bericht 'Attributalertgenerator - Protokoll' werden Änderungen aufgeführt, die an Attributalertgeneratoren vorgenommen wurden, beispielsweise Änderungen bei Ablaufdatumsangaben, Fallnummern, Kommentaren oder Status. Der Bericht ist nach Suchentitäts-ID sortiert.

Suchentität
Zeigt die Entitäts-ID (und den Namen, sofern dieser bereitgestellt wurde) aus den Suchkriterien für den Attributalertgenerator an.

Erstellungsdatum und -zeit
Zeigt das Datum und die Zeit an, an dem bzw. zu der dieser Attributalertgenerator erstellt wurde.

Statusprotokollabschnitt
Dieser Abschnitt des Berichts zeigt jede Aktualisierung des Attributalertgenerators, beginnend mit der jüngsten Aktualisierung.

Kommentar
Zeigt Kommentare an, die vom Benutzer eingegeben wurden, der diese Aktualisierung vorgenommen hat.

Aktualisierungsdatum und -zeit
Zeigt das Datum und die Zeit an, an dem bzw. zu der dieser Attributalertgenerator zuletzt modifiziert wurde. Wenn dieser Attributalertgenerator nicht modifiziert wurde, sind Datum und Zeit mit den Angaben für **Erstellungsdatum und -zeit** identisch.

Ablaufdatum und -zeit
Zeigt das Datum und die Zeit, an dem bzw. zu der dieser Attributalertgenerator abläuft, oder zeigt das Datum, an dem dieser Attributalertgenerator zum letzten Mal Attributalerts generiert.

Status Gibt an, ob der Attributalertgenerator aktiv oder abgelaufen ist.

Benutzer
Zeigt den Namen des Benutzers an, der diese Aktualisierung vorgenommen hat.

Analysegruppe
Zeigt die Visualizer-Analysegruppe an, zu der der Benutzer gehört, der diesen Attributalertgenerator zuletzt modifiziert hat.

Mindestauflösungsbewertung
Gibt die Mindestauflösungsbewertung und Beschreibung der Mindestbewertung an, die als Teil der Kriterien für den Attributalertgenerator ausgewählt wurde. Dieser Schwellenwert für die Bewertung gibt an, wie exakt die Attribute übereinstimmen müssen, damit ein Alert für diesen Attributalertgenerator generiert wird. "Ist Entität" ist daher die bestmögliche Übereinstimmung, "Beliebi-

ge Beziehung" die geringste Übereinstimmung. Sie können den Schwellenwert für jede dieser Bewertungen in der Anzeige **Benutzervorgaben für das System** des Fensters **Benutzervorgaben für die Anzeige konfigurieren** festlegen.

Ursachencode
Zeigt den vom Benutzer ausgewählten Code an, der die Ursache für den Attributalertgenerator angibt.

Fallnummer
Zeigt die optionale alphanumerische Fallnummer an, die von dem Benutzer eingegeben wird, der den Attributalertgenerator erstellt hat.

Bericht zu Attributalertgeneratoren:

Mit dem Bericht zu den Attributalertgeneratoren können Sie Attributalertgeneratoren verwalten. In diesem Bericht sehen Sie eine kurze Zusammenfassung aller Attributalertgeneratoren im System. Hierzu gehören das Datum und die Zeit der einzelnen Attributalertgeneratorerstellungen, das Ablaufdatum und die Ablaufzeit, der Status sowie das Datum und die Zeit der letzten Aktualisierung eines Attributalertgenerators. Der Bericht ist nach Suchentitäts-ID sortiert.

Suchentität
Gibt die ID der Suchentität an, die vom Attributalertgenerator erstellt wurde.

Erstellungsdatum und -zeit
Gibt das Datum und die Zeit an, an dem bzw. zu der dieser Attributalertgenerator erstellt wurde.

Kommentar
Zeigt den Kommentar an, den der Benutzer als Teil des Attributalertgenerators hinzugefügt hat.

Aktualisierungsdatum und -zeit
Gibt das Datum und die Zeit an, an dem bzw. zu der dieser Attributalertgenerator zuletzt modifiziert wurde. Wenn dieser Attributalertgenerator nicht modifiziert wurde, sind Datum und Zeit mit den Angaben für **Erstellungsdatum und -zeit** identisch.

Ablaufdatum und -zeit
Gibt das Datum und die Zeit an, an dem bzw. zu der dieser Attributalertgenerator abläuft.

Status Aktueller Status dieses Attributalertgenerators zum Zeitpunkt der letzten Aktualisierung dieses Attributalertgenerators.

Benutzer
Gibt den Benutzer an, der diesen Attributalertgenerator zuletzt modifiziert hat. Wurde der Attributalertgenerator noch nie modifiziert, ist dies der Benutzer, der den ursprünglichen Attributalertgenerator erstellt hat.

Analysegruppe
Gibt den Namen der Analysegruppe an, zu der der Benutzer gehört, der diesen Attributalertgenerator zuletzt modifiziert hat.

Mindestauflösungsbewertung
Zeigt die Auswahl in der Dropdown-Liste **Mindestauflösungsbewertung** an, wenn der Attributalertgenerator erstellt wurde. Dieser Schwellenwert für die Bewertung legt fest, wie exakt die Attribute übereinstimmen müssen, damit ein Alert für diesen Attributalertgenerator generiert wird.

Die Schwellenwerte für diese Bewertungen definieren Sie auf der Registerkarte **Benutzervorgaben für das System** im Dialog **Benutzervorgaben für die Anzeige konfigurieren**, der über das Menü **Datei** aufgerufen wird.

Ursachencode
Ein vom Benutzer ausgewählter Code, der die Ursache für den Attributalertgenerator angibt.

Fallnummer
Optionale alphanumerische Fallnummer, die von dem Benutzer eingegeben wird, der den Attributalertgenerator erstellt hat.

Bericht 'Attributalert':

Mit dem Bericht **Attributalert** können Sie einzelne Attributalerts verwalten. In diesem Bericht sehen Sie eine Auflistung aller Entitäten, die den Attributalertgeneratorkriterien entsprachen, sowie den Status und die jüngste Aktivität bezüglich des Alerts.

Der Bericht ist nach Suchentitäts-ID aufsteigend sortiert. Gibt es mehrere übereinstimmende Entitäten pro Suchentität, werden die übereinstimmenden Entitäten aufsteigend nach Entitäts-ID sortiert.

Suchentität
Zeigt die Entitäts-ID an, die von der Attributalertsuche erstellt wurde.

Übereinstimmende Entität
Zeigt die ID und den Namen der Entität an, die der Suchentität gemäß den Attributalertgeneratorkriterien entsprach. Hat ein Attributalert mehrere übereinstimmende Entitäten, werden sie in alphanumerischer Anordnung nach Entitäts-ID angezeigt. `Entitäts-ID 37` wird beispielsweise vor `Entitäts-ID 1003` angezeigt.

Attributalertinformationen
In diesem Abschnitt des Berichts werden allgemeine Informationen zu den Alertergebnissen angezeigt.

Attributalert - Status
Zeigt den aktuellen Status dieses Attributalerts an.

Datum und Zeit des Suchergebnisses
Zeigt das Datum und die Zeit an, an dem bzw. zu der dieser Attributalert erstellt wurde.

Attributsuche - Status
Zeigt den aktuellen Status des Attributalertgenerators an, der diesen Attributalert generiert hat.

Mindestauflösungsbewertung
Gibt die Mindestauflösungsbewertung und Beschreibung der Mindestbewertung an, die als Teil der Attributalertgeneratorkriterien ausgewählt wurde. Dieser Schwellenwert für die Bewertung gibt an, wie exakt die Attribute übereinstimmen müssen, damit ein Attributalert generiert wird.

Informationen zum Attributalertstatus
In diesem Abschnitt des Berichts sehen Sie den Verlauf jeder Statusangabe für diesen Alert. Die Statusinformationen werden in der Reihenfolge der Aktualisierungen angezeigt, sodass die letzte Statusaktualisierung zuerst angezeigt wird.

Statusdatum und -zeit
Zeigt das Datum und die Zeit an, an dem bzw. zu der die Aktualisierung des Attributalerts stattfand.

Benutzer
Zeigt den Namen des Benutzers an, der den Alert aktualisiert hat.

Aktivitätscode
Zeigt den benutzerdefinierten Code an, der eine Aktion angibt, die bei diesem Attributalert von einem Benutzer ausgeführt wird. Wenn Benutzer Alerts aktualisieren, wählen Sie einen Aktivitätscode aus. Es gibt beispielsweise die Aktivitätscodes **Offen**, **Zugeordnet**, **Angehalten** und **Geschlossen**. Aktivitätscodes werden in der Konfigurationskonsole konfiguriert.

Status Zeigt den Dispositionsstatus für diese am am Statusdatum und zur Statuszeit geänderte Alertaktualisierung an. Dispositionsstatusangaben werden in der Reihenfolge der Aktualisierungen angezeigt, sodass die letzte Statusaktualisierung zuletzt aufgelistet wird.

Kommentar
Zeigt die Kommentare an, die von dem Benutzer eingegeben wurde, der diese Aktualisierung an dem Alert vorgenommen hat.

Übereinstimmende Informationen
Dieser Abschnitt zeigt, welche Attribute gemäß Datentyp und Wert zwischen der Suchentität und der übereinstimmenden Entität übereinstimmten.

Datentyp
Zeigt den Namen des Attributs an, das bei der Suchentität und der übereinstimmenden Entität übereinstimmte. Die beiden Werte dieses übereinstimmenden Attributs werden in den Spalten 'Übereinstimmungswert' und 'Suchkriterien' angezeigt.

Suchkriterien

Zeigt den zur Suchentität gehörigen Datenwert an, der mit dem entsprechenden, in der Spalte 'Übereinstimmende Entität' angezeigten Wert übereinstimmte.

Übereinstimmungswert
Zeigt den aktuellen, zur übereinstimmenden Entität gehörigen Datenwert an, der demselben Datentyp und Datenwert der Suchentität entspricht.

Genauigkeitsbeschreibung
Zeigt den Text an, der die Genauigkeitsstufe beschreibt, mit der die Suchkriterien und der Übereinstimmungswert übereinstimmten. Genauigkeitsstufen werden während der Entitätsauflösungskonfiguration nach Attribut konfiguriert.

Genauigkeit / Max. Genauigkeit
Die erste Zahl ist die vom System generierte Genauigkeitsbewertung, die anzeigt, wie exakt der Wert in **Suchkriterien** mit dem Wert in **Übereinstimmungswert** übereinstimmt. Die zweite Zahl ist die maximale Genauigkeitsbewertung, die erreicht werden kann.

Durch einen Vergleich der beiden Zahlen können Sie die Übereinstimmungsgenauigkeit zwischen der Suchentität und der übereinstimmenden Entität eingehender ermitteln. Mithilfe dieser Bewer-

tungen können Sie auch feststellen, ob die Suchkriterien für den Attributalert angepasst werden müssen.

Bewertungsanpassung
Zeigt die diesem Attribut zugeordnete Zahl an, die erhöht oder reduziert wird, um die Auflösungsbewertung während der Entitätsauflösung anzupassen. Diese Zahl wird als Teil der gesamten Entitätsauflösungskonfiguration konfiguriert.

Datenquelle - Ergebnisbericht:

Der Ergebnisbericht für Datenquellen enthält eine kurze statistische Zusammenfassung nach der Datenquelle der Datensätze, die zur Verarbeitung in das System geladen wurden. Dieser Bericht zeigt die Gesamtzahl der verarbeiteten Datensätze nach Lade-ID. Für diese Gesamtanzahl der geladenen Datensätze zeigt der Bericht, wie viele dieser Datensätze neue Identitäten oder neue Entitäten darstellten, und der Prozentsatz der jeweiligen Datensätze (neue Identitäten bzw. neu erstellte Entitäten) wird berechnet.

Statistik nach Ladevorgang innerhalb einer Datenquelle

Ladedatum
Zeigt das Datum an, an dem diese Datenquellendatei geladen wurde.

Lade-ID
Zeigt die vom System zugeordnete Lade-ID-Nummer an.

Datenquelle
Zeigt den Datenquellencode und die Datenquellenbeschreibung (getrennt durch einen Strich) der geladenen Datenquellendatei an.

Geladene UMF-Datensätze
Gibt die Gesamtanzahl der geladenen Identitätsdatensätze in dieser Datenquellendatei an.

Neue Identitäten
Gibt die Gesamtanzahl der in der geladenen Datendatei erkannten neuen Identitäten an. (Diese Zahl weist auf eine Identität hin, die das System noch nicht verarbeitet hat.)

Neue Identität %
Gibt den Prozentsatz der Gesamtanzahl geladener Datensätze an (neue Identitäten geteilt durch geladene UMF-Datensätze), die neue Identitäten darstellen.

Neue Entitäten
Gibt die Gesamtanzahl der neuen Entitäten an, die aus diesem Datenladevorgang erstellt wurden.

Neue Entitäten %
Gibt den Prozentsatz der Gesamtanzahl geladener Datensätze an (neue Entitäten geteilt durch geladene Datensätze), die neue Entitäten darstellen.

Statistikdiagramme nach Datenquelle

Geladene Datensätze nach Datenquelle
Zeigt ein Balkendiagramm an, in dem die Anzahl der von jeder Datenquelle in das System geladenen Datensätze gemäß den anderen angegebenen Berichtskriterien grafisch dargestellt wird. Sie sehen, welche Datenquellen

die meisten Datensätze oder die wenigsten Datensätze beigesteuert haben, und Sie können dieses Ergebnis mit Ihren geschätzten Ladezahlen vergleichen.

- Die vertikale Achse zeigt die Datenquellen nach Datenquellencode an.
- Die horizontale Achse zeigt die Anzahl der geladenen Datensätze.

Werden für eine bestimmte Datenquelle weniger Datensätze als erwartet geladen, können Sie die Datendateien für diese Datenquelle überprüfen. (Sie könnten auch einen Ladeergebnisbericht ausführen, um die Datenqualität der Dateien anzuzeigen, die für diese Datenquelle geladen wurden. Die Datenqualität wirkt sich unmittelbar auf die Anzahl der geladenen Datensätze aus.)

Neue Entitäten nach Datenquelle
Zeigt ein Balkendiagramm an, in dem grafisch dargestellt wird, welche Datenquellen die größte Anzahl neuer Entitäten gemäß den anderen angegebenen Berichtskriterien geliefert haben.

- Die vertikale Achse zeigt die Datenquellen nach Datenquellencode an.
- Die horizontale Achse zeigt die Anzahl der neu erstellten Entitäten.

Bericht 'Offengelegte Beziehungen':

Mit diesem Bericht können Sie offengelegte Beziehungen anzeigen und verwalten, die zwischen Identitäten erstellt wurden. Offengelegte Beziehungen sind Beziehungen, die entweder von Visualizer-Benutzern über die Anzeige **Offenlegung hinzufügen** manuell oder durch Einschließen des Tagpaars für offen gelegte Beziehungen (<DR> und </DR>) bei eingehenden Identitätsdatensätzen erstellt wurden.

Der Bericht ist nach Beziehungs-ID sortiert.

Beziehungs-ID
Zeigt die vom System generierte Nummer an, die jeder offengelegten Beziehung während ihrer Erstellung zugeordnet wird.

Erstellungsdatum und -zeit
Zeigt Erstellungsdatum und -zeit der offengelegten Beziehung an.

Beziehungsbeschreibung
Zeigt Text an, der den Grund beschreibt, warum die offengelegte Beziehung erstellt wurde. Dieser Text wird von dem Benutzer eingegeben, der die offengelegte Beziehung erstellt.

Aktualisierungsdatum und -zeit
Zeigt Datum und Zeit der letzten Aktualisierung dieser offengelegten Beziehung an.

Status Zeigt den Status dieser offengelegten Beziehung an.

Löschdatum
Zeigt Datum und Zeit der manuellen Löschung der offengelegten Beziehung an. In diesem Feld wird nur dann ein Datum und eine Zeit angezeigt, wenn ein Benutzer festgestellt hat, dass die Beziehung ungültig ist, und die offengelegte Beziehung gelöscht hat.

Datenquelle
Zeigt einen Datenquellencode und eine Beschreibung für beide Entitäten an (jeweils eine in separaten Zeilen), die jetzt durch diese offengelegte Beziehung verknüpft sind. Der Datenquellencode verweist auf die ursprüngliche Quellendatei.

Externe ID
Zeigt eine externe ID für beide Entitäten an (jeweils eine in separaten Zeilen), die jetzt durch diese offengelegte Beziehung verknüpft sind. Die externe ID verweist häufig auf eine Kontonummer in der ursprünglichen Quellendatei, die ausschließlich zu der Entität gehört.

Ereignisalert - Detailbericht:

Der Detailbericht für Ereignisalerts enthält vollständige Details zu einem bestimmten Ereignisalert sowie den an dem Alert beteiligten Entitäten. Dieser Bericht ist nützlich, wenn Sie einen Hardcopy-Bericht der Registerkarte **Ereignisalert** des Prüffensters benötigen.

Alert-ID
Zeigt die Beschreibung und Alert-ID für einen bestimmten Ereignisalert an. Die Alert-ID wird vor der Beschreibung in der Kopfzeile des Berichts angezeigt.

Ereignisalertinformationen
Dieser Abschnitt zeigt allgemeine Informationen zum Ereignisalert an wie eine Beschreibung der Ereignisalertregel, die diesen Alert ausgelöst hat, und den Status des Ereignisalerts.

Datum und Zeit des Alerts
Gibt das Datum und die Uhrzeit der Ereignisalertgenerierung an.

Regel-ID
Zeigt eine interne Zahl an, die von System generiert wurde, als die Ereignisalertregel ursprünglich konfiguriert wurde. Diese ID ist mit der Ereignisalertregel verknüpft, die diesen Ereignisalert auslöste.

Regelbeschreibung
Zeigt Text an, der die Ereignisalertregel beschreibt und von dem Benutzer definiert wurde, der die Ereignisalertregel konfiguriert hat.

Status Zeigt den aktuellen Status dieses Ereignisalerts an.

Ereignisdetails
Dieser Abschnitt bietet weitere Informationen zu den Ereignisalertdaten.

Datum und Zeit
Gibt das Datum und die Zeit der Ereignisalertgenerierung an.

Datenquelle
Zeigt für jedes Ereignis den Datenquellencode und die Beschreibung an, von denen die Ereignisdaten zur Verfügung gestellt wurden. Diese Informationen geben die ursprüngliche Quellendatei an.

Externe ID
Zeigt für jedes Ereignis die externe ID an, die dem Datenquellencode zugeordnet ist, der die Ereignisdaten zur Verfügung gestellt hat. Diese Informationen geben häufig eine Kontonummer für die Entität in der ursprünglichen Quellendatei an.

Ereignisreferenz
Zeigt für jedes Ereignis den eindeutigen Code an, der vom Prozessor für komplexe Ereignisse während der Ausführung des Ereignisprozessors erstellt wurde.

Menge
Gibt für jedes Ereignis die Nummer an, die die in dieses Ereignis

einbezogene Menge darstellt. 1 bedeutet z. B. eine Geldüberweisung des Werts in der Spalte **Wert**.

Wert Zeigt für jedes Ereignis den Gesamtwert an.

Entitätsinformationen
Für die an diesem Ereignis beteiligte Entität bietet dieser Abschnitt die Liste von Attributtypen und ihre zugeordneten Werte, die an dem Ereignis beteiligt waren.

Alertdispositionen
Dieser Abschnitt bietet eine Zusammenfassung der Status für den Ereignisalert.

Aktivitätscode
Zeigt den Ereignisaktivitätscode an, der von dem Benutzer ausgewählt wurde, der den Status dieses Ereignisalerts änderte.

Status Zeigt den Status (**Aktiv** oder **Inaktiv**) an, der mit dem Ereignisaktivitätscode verknüpft ist.

Statuskommentare
Zeigt Analystenkommentare an, die zu dieser Statusaktualisierung eingegeben wurden.

Benutzer
Zeigt die Benutzer-ID des Benutzers an, der den Status dieses Ereignisalerts änderte.

Datum und Zeit
Gibt das Datum und die Zeit der Statusänderung an.

Abschnitt 'Rollenereignisalertprotokoll'
In diesem Abschnitt werden alle Rollenalerts aufgelistet, an denen die für diesen Ereignisalert verantwortliche Entität beteiligt ist.

Abschnitt 'Ereignisalertprotokoll'
Dieser Abschnitt des Berichts listet das komplette Protokoll für die am Hauptereignisalert beteiligte Entität auf. Diesem Abschnitt können Sie die Anzahl von Ereignisalerts, an denen diese Entität beteiligt ist, entnehmen.

Alertdatum und -zeit
Gibt das Datum und die Zeit der Ereignisalertgenerierung an.

Alert-ID
Zeigt die ID für diesen Ereignisalert an.

Beschreibung
Zeigt Text für die Beschreibung der Verarbeitungsregel für komplexe Ereignisse an, die diesen Ereignisalert auslöste.

Aktivitätscode
Zeigt einen benutzerdefinierten Code an, der eine Aktion angibt, die bei diesem Alert von einem Benutzer ausgeführt wird. Aktivitätscodes werden in der Konfigurationskonsole konfiguriert und in einer Dropdown-Liste in Visualizer ausgewählt, wenn ein Alert aktualisiert wird. Es gibt beispielsweise die Aktivitätscodes **Zugeordnet**, **Geschlossen** und **Anstehend**.

Status Zeigt den Status für diese Alertaktualisierung, geändert am Statusdatum und zur Statuszeit. Statusangaben werden in der Reihenfolge der Aktualisierungen angezeigt, sodass die letzte Statusaktualisierung zuletzt aufgelistet wird.

Bericht zu allen Ereignissen:

Mit dem Bericht zu allen Ereignissen können Sie alle Ereignisse anzeigen, die mit einer einzelnen Entität verknüpft sind, unabhängig davon, ob sie einen Ereignisalert erzeugt haben. Dieser Bericht ist nützlich, wenn Sie einen Hardcopy-Bericht der Anzeige **Entitätsereignisse** des Prüffensters benötigen. Die im Bericht angezeigten Ereignisse hängen vom Ereignistyp und dem Datumsbereich, die in der Anzeige ausgewählt wurden, ab.

Wenn Sie keinen Ereignistyp ausgewählt haben, zeigt der Bericht Ereignisse aller Typen für die angegebene Entität innerhalb des definierten Datumsbereichs an. Wenn Sie einen Ereignistyp ausgewählt haben, werden nur die Ereignisse dieses Typs im definierten Datumsbereich angezeigt.

Basisberichtsinformationen
In diesem Abschnitt sind die Headerbasisberichtsinformationen wie der Datumsbereich für den Bericht und weitere Angaben über die mit diesen Ereignissen verknüpfte Entität zu finden.

Bericht – Datumsangaben: ‚Von' und ‚Bis'
Gibt das Start- und Enddatum für den Bericht an. Es werden nur Ereignisse, die im angegebenen Datumsbereich für diese Entität eintraten, in den Bericht aufgenommen.

Zugehörige Entität
Gibt die Entitäts-ID der Entität an, die mit diesen Ereignissen verknüpft ist.

Aktueller Name
Gibt den aktuellsten Namen für die Entität in der Entitätendatenbank an.

Aktuelle Adresse
Gibt die aktuellste Adresse für die Entität in der Entitätendatenbank an.

Ereignisinformationen
In diesem Abschnitt werden die Details der mit dieser Entität verknüpften Ereignisse nach Ereignistyp angegeben.

Ereignistyp
Beschreibt den Ereignistyp. Diese Beschreibung wird mit dem Ereignistyp in der Konfigurationskonsole konfiguriert.

Ereignis-ID
Zeigt die vom System generierte Zahl, die dieses Ereignis kennzeichnet, an.

Erstellungsdatum und -zeit
Zeigt das Datum und die Uhrzeit des Ereignisses an.

Datenquelle
Zeigt den Datenquellencode und die Datenquellenbeschreibung an, die mit dem Ereignis verknüpft sind.

Externe ID
Zeigt den eindeutigen Schlüssel an, der den eingehenden Identitätsdatensatz in der Originaldatenquelle für dieses Ereignis identifiziert.

Ereignisreferenz
Zeigt zusätzliche Informationen zum Ereignis an, in der Regel den Namen des Standorts, an dem das Ereignis stattfand.

Standort
Zeigt die Adressinformationen für den Standort an, an dem das Ereignis stattfand.

Wert Zeigt den Wert an, der mit diesem Ereignis verknüpft ist.

Menge
Zeigt die Anzahl von Einheiten an, die mit dem Ereignis verknüpft sind.

Maßeinheit
Zeigt die Maßeinheit an, die mit dem Ereigniswert verknüpft ist. Die Maßeinheit wird abhängig vom Ereignistyp in der Konfigurationskonsole konfiguriert. Die Maßeinheit hilft Ihnen, den Wert zu verstehen. Wenn z. B. die Maßeinheit US-Dollar ist und der Ereigniswert 5000 beträgt, wissen Sie, dass bei diesem Ereignis 5000 US-Dollar beteiligt waren.

Kurzinfo oder *benutzerdefinierte Bezeichnung*
Zeigt zusätzliche Informationen über das Ereignis wie Anmerkungen oder Kommentare an, die mehr Kontext für die Ereignistransaktion liefern können.

Benutzer können im Rahmen der Konfiguration eines Ereignistyps in der Konfigurationskonsole eine benutzerdefinierte Bezeichnung für diese Spalte definieren. Anstelle von **Kurzinfo** wird möglicherweise eine aussagekräftigere benutzerdefinierte Kennzeichnung angezeigt (beispielsweise **Hinweise zu telegrafischen Geldanweisungen**.

Zusätzliche Kurzinfo oder *benutzerdefinierte Bezeichnung*
Zeigt, falls verfügbar, weitere Informationen über das Ereignis an.

Benutzer können im Rahmen der Konfiguration eines Ereignistyps in der Konfigurationskonsole eine benutzerdefinierte Bezeichnung für diese Spalte definieren. Statt **Zusätzliche Kurzinfo** sehen Sie möglicherweise eine aussagekräftigere benutzerdefinierte Bezeichnung wie **Mitarbeiterkommentare**.

Laden - Ergebnisbericht:

Der Ladeergebnisbericht fasst Statistiken und Qualitätsmerkmale nach Datenquelle zusammen. Er enthält Informationen zu den Datenquellendateien. Mit diesem Bericht können Sie Statistikdaten zur Ladeleistung, die Anzahl der von diesem Ladevorgang erstellten Entitäten und Alerts, allgemeine Informationen zur Datenqualität der geladenen Daten, eine Zusammenfassung der Aktionen bezüglich der UMF-Datensätze nach Ladevorgang und alle von dem Ladevorgang generierten UMF-Ausnahmenbedingungen ermitteln. Der Bericht ist nach Lade-ID sortiert.

Der Bericht unterteilt die Statistikdaten für jeden Ladevorgang in verschiedene Abschnitte:

- Ladezusammenfassung
- Rollenalertzusammenfassung
- Beziehungszusammenfassung
- Qualitätszusammenfassung

- UMF-Dokumentzusammenfassung
- Zusammenfassung der Ausnahmebedingung

Ladezusammenfassung

Mit diesem Abschnitt können Sie feststellen, wie lange die Verarbeitung einer bestimmten Datei gedauert hat, und er gibt Ihnen eine allgemeine Vorstellung von der Brauchbarkeit dieser Datenquellendatei für die Entitätsauflösung und Erkennung von Beziehungen insgesamt.

Startdatum und -zeit
Gibt das Anfangsdatum und die Anfangszeit des Datenladevorgangs an.

Abschlussdatum und -zeit
Gibt das Enddatum und die Endzeit des Datenquellendateiladevorgangs an.

Anzahl UMF-Datensätze
Gibt die Gesamtanzahl der Datensätze an, die im Zeitraum zwischen **Startdatum und -zeit** und **Abschlussdatum und -zeit** aus dieser Datenquellendatei geladen wurden.

Die Differenz zwischen **Abschlussdatum und -zeit** und **Startdatum und -zeit** gibt die Minuten an, die zum Laden dieser Datenquellendatei benötigt wurden. Dieser Wert kann Ihnen eine Vorstellung von der Systemleistung geben. Außerdem kann er anzeigen, dass eine große Datenquellendatei zur schnelleren Verarbeitung in kleinere Dateien aufgeteilt werden muss.

Neue Identitäten
Gibt die Gesamtanzahl neuer Identitäten an, die im Zeitraum zwischen **Startdatum und -zeit** und **Abschlussdatum und -zeit** geladen wurden.

Neue Identität %
Gibt den Prozentsatz der Gesamtanzahl der Identitäten in diesem Datenladevorgang an, die (für die Entitätendatenbank) neue Identitäten sind.

Neue Entitäten
Gibt die Gesamtanzahl der Entitäten an, die im Zeitraum zwischen **Startdatum und -zeit** und **Abschlussdatum und -zeit** neu erstellt wurden.

Neue Entitäten %
Gibt den Prozentsatz der Gesamtzahl der Entitäten an, die als Ergebnis dieses Datenquellenladevorgangs neu erstellte Entitäten sind.

Die Anzahl der neuen Identitäten und der neuen Entitäten kann Ihnen eine allgemeine Vorstellung von der Brauchbarkeit dieser Datenquelle für die Entitätsauflösung und Erkennung von Beziehungen insgesamt geben. Bleiben diese Werte über einen Zeitraum hinweg niedrig, könnte dies bedeuten, dass diese Datenquelle für die Ziele Ihres Unternehmens in Bezug auf die Entitätsauflösung nicht geeignet ist.

Rollenalertzusammenfassung

In diesem Abschnitt sehen Sie die Auflösungsregeln und die Auflösungsbewertungen, die den erkannten Beziehungen gemein sind, die zu Rollenalerts führten. Jede Zeile stellt die Anzahl der generierten Rollenalerts auf der Basis der aufgelisteten Kriterien dar.

Auflösungsregel
Zeigt den Namen der Auflösungsregel an, die verwendet wird, um die Identität und die Entität während der Entitätsauflösung und der Beziehungserkennung auszuwerten.

Alertbeschreibung
Zeigt den Namen der Rollenalertregel an, die den Rollenalert auslöste.

Wertigkeit
Zeigt einen benutzerdefinierten Anzeiger zur Messung der Priorität oder Bedeutung dieses Rollenalerts an.

Auflösungsbewertung
Zeigt eine Beziehungsbewertung (0 - 100) für die Auflösungsregel an, die der Identität und der Entität in diesem Rollenalert zugeordnet wird. Diese Bewertung zeigt den Grad der Ähnlichkeit zwischen der Identität und der Entität an. Eine Bewertung von 100 bedeutet, dass der Identitätsdatensatz in die Entität aufgelöst wurde.

Alertanzahl
Gibt die Gesamtanzahl der Rollenalerts an, die gemäß der Beschreibung der Rollenalertregel, der Auflösungsregel und der Auflösungsbewertung generiert wurden.

Beziehungszusammenfassung

In diesem Abschnitt sehen Sie die Attribute, die den erkannten Beziehungen gemein sind, die keinen Rollenalert generierten. Jede Zeile stellt die Anzahl der erkannten Beziehungen auf der Basis der aufgelisteten Kriterien dar.

Auflösungsregel
Zeigt den Namen der Auflösungsregel an, die verwendet wird, um die eingehenden Identitätsdatensätze und die vorhandenen Entitäten während der Entitätsauflösung und der Beziehungserkennung auszuwerten.

Auflösungsbewertung
Zeigt eine Auflösungsbewertung (0 - 100) für die Auflösungsregel an, die der Identität und der Entität während der Entitätsauflösung zugeordnet wird. Diese Bewertung zeigt den Grad der Ähnlichkeit zwischen der Identität und der Entität an. Eine Bewertung von 100 bedeutet, dass der Identitätsdatensatz in die Entität aufgelöst wurde.

Beziehungsbewertung
Zeigt eine Beziehungsbewertung (0 - 100) für die Auflösungsregel an, die der Identität und der Entität während der Beziehungsauflösung zugeordnet wird. Diese Bewertung zeigt den Grad der Beziehung zwischen der Identität und der Entität an.

Je höher die Beziehungsbewertung, umso enger ist die Beziehung zwischen der Identität und der Entität (auf der Basis der übereinstimmenden Attribute).

Beziehungsanzahl
Gibt die Gesamtanzahl der Beziehungen an, die auf der Basis der Auflösungsregel, der Auflösungsbewertung und der Beziehungsbewertung erkannt werden.

Qualitätszusammenfassung

Mit den Informationen in diesem Abschnitt können Sie die Qualität der Daten in jeder Datenquellendatei bewerten. Der Abschnitt zeigt die Qualität nach Attributtyp innerhalb eines UMF-Segments und UMF-Dokumenttyps an. Anhand der Qualitätszusammenfassung und der Zusammenfassung der UMF-Ausnahmebedingungen können Sie erkennen, bei welchen Datenquellendateien Qualitätsprobleme oder UMF-Fehler vorliegen, die behoben werden müssen. Normalerweise können Sie diese Probleme durch ETL oder DQM/Datenquellenkonfiguration vor Verarbeitung der Datenquellendatei lösen.

In einigen Fällen kann dieser Abschnitt zeigen, dass die Qualität einer Datenquelle so schlecht ist, dass Sie diese Datenquelle nicht für die Entitätsauflösung verwenden wollen.

Dokumenttyp
Zeigt den Namen des UMF-Dokumenttyps an, der den in **Datentyp** aufgeführten Datentyp enthält. In der Regel lautet dieser Wert UMF_ENTITY.

Tabellenname
Zeigt den Namen der Datenbanktabelle an, in der die Daten aus UMF-Segmenten mit ähnlichem Namen gespeichert werden. Daten aus dem Segment NUMBER werden beispielsweise in der Tabelle NUMS gespeichert.

Datentyp
Gibt den Datentyp an, wie in den UMF-Tags für den Attributtyp der eingehenden Datensätze aufgelistet. Dieser Typ entspricht einem in **Tabellenname** aufgeführten UMF-Segment. Lautet der Tabellenname beispielsweise *ADDRESS* und der aufgeführte Datentyp *H*, werten die Qualitätsinformationen den Adresstyp *Home* aus.

Wenn Sie einen Datentyp nicht erkennen, kann dies bedeuten, dass die Datenquellendatei der entsprechenden Kombination aus UMF-Dokumenten, -Segmenten und -Tags nicht ordnungsgemäß zugeordnet ist. Überprüfen Sie den Abschnitt mit der Zusammenfassung der Ausnahmebedingungen, um festzustellen, ob Segmentausnahmebedingungen durch übereinstimmende UMF-Segmente und -Tags verursacht wurden. Wird das Problem durch ein ungültiges UMF verursacht, stimmen die Zahlen für **Zähler für schlechte Qualität** im Abschnitt mit der Qualitätszusammenfassung und für **Anzahl Segmentausnahmebedingungen** im Abschnitt mit den UMF-Ausnahmebedingungen häufig überein.

Datensatzanzahl
Gibt die Gesamtzahl der eingehenden Identitätsdatensätze für den Dokumenttyp, den Tabellennamen und den Datentyp an.

Generische Anzahl
Gibt die Gesamtzahl der eingehenden Identitätsdatensätze mit dem angegebenen Dokumenttyp, Tabellennamen und Datentyp an, die Werte enthalten, die als generisch betrachtet werden.

Zähler für schlechte Qualität
Gibt die Gesamtzahl der eingehenden Identitätsdatensätze mit dem angegebenen Dokumenttyp, Tabellennamen und Datentyp an, deren Qualität als schlecht betrachtet wird. Dieser Wert kann auf einen Datenerfassungs- oder ETL-Umsetzungsfehler in der Datenquellendatei hinweisen.

Verwendbar %
Gibt den Prozentsatz der eingehenden Identitätsdatensätze mit dem angegebenen Dokumenttyp, Tabellennamen (dieses UMF-Segments) und Daten-

typ an, die für die Entitätsauflösung und das Erkennen von Beziehungen verwendet werden können. ('Datensatzanzahl' minus 'Generische Anzahl' minus 'Zähler für schlechte Qualität') geteilt durch 'Datensatzanzahl' ist gleich 'Verwendbar %'.

Identität (%)
Gibt den Prozentsatz der eingehenden Identitätsdatensätze an, die den Dokumenttyp, Tabellennamen und Datentyp enthielten.

Attributzusammenfassung

In diesem Abschnitt sehen Sie die Attribute in der Datenquellendatei, die bei der Erkennung von Beziehungen und der Generierung von Rollenalerts beteiligt waren. Jedes Attribut ist einem bestimmten UMF-Segment zugeordnet und dieser Abschnitt zeigt die Anzahl der erkannten Beziehungen und der generierten Rollenalerts auf der Basis der Daten im eingehenden UMF-Segment.

Segmentname
Zeigt den Namen des UMF-Segments an, das unmittelbar einem Attribut zugeordnet ist.

Datentyp
Zeigt den Attributtyp (oder Datentyp) innerhalb des UMF-Segments, der der Genauigkeitsbeschreibung entspricht. Der Bericht könnte einen bestimmten Attributtyp oder *ALL* auflisten. *ALL* steht für alle Attributtypen im UMF-Segment.

Genauigkeitsbeschreibung
Beschreibt den Übereinstimmungsschwellenwert zwischen einem Attribut aus einer eingehenden Identität und einem Attribut aus einer vorhandenen Entität.

Rollenalerts
Gibt die Gesamtanzahl der Rollenalerts an, die gemäß diesem UMF-Segment, Datentyp und dieser Genauigkeitsbeschreibung generiert wurden.

Beziehungen
Gibt die Gesamtanzahl der Beziehungen an, die gemäß diesem UMF-Segment, Datentyp und dieser Genauigkeitsbeschreibung erkannt wurden.

UMF-Dokumentzusammenfassung

Sie können in diesem Abschnitt die Gesamtanzahl der eingehenden Datensätze in einer Datenquellendatei prüfen. Als Basis dient die Aktion, die für den Datensatz ausgeführt werden soll. Sie können diese Zahlen mit der Datensatzanzahl im Abschnitt mit der Ladezusammenfassung abgleichen.

Dokumenttyp
Zeigt den Namen des UMF-Eingangsdokumenttyps an. In der Regel lautet dieser Wert UMF_ENTITY.

Aktion
Gibt den Typ der Aktion für den eingehenden Identitätsdatensatz an. Nachfolgend finden Sie eine Liste der am häufigsten verwendeten Aktionen:

- *A* für Hinzufügen (Add)
- *C* für Ändern (Change)
- *D* für Löschen (Delete)

Als Teil des ETL-Prozesses verwenden Identitätsdatensätze in der Regel UMF-Tagging, um anzuzeigen, wie bei dem jeweiligen eingehenden Datensatz während der Systemverarbeitung verfahren werden soll.

Anzahl UMF-Datensätze
Gibt die Gesamtanzahl der für jeden Aktionstyp innerhalb des Dokumenttyps verarbeiteten Datensätze an.

Prozent
Gibt den Prozentsatz der Gesamtanzahl geladener Datensätze an, die die Datensatzanzahl darstellt. (Die Summe darf 100 % nicht überschreiten.)

Zusammenfassung der Ausnahmebedingung

Diese Informationen helfen beim Identifizieren von fehlerhaften Identitätsdatensätzen, z. B. Datensätzen mit UMF-Fehlern. Die Ausnahmebedingung beschreibt den Fehler und der Tabellenname und das Element zeigen, welches Segment und welcher Datensatz fehlerhaft sind. Die Anzahl zeigt, wie viele der Datensätze in der Datei diesen UMF-Fehler enthielten.

Dokumenttyp
Zeigt den Namen des UMF-Eingangsdokumenttyps an. In der Regel lautet dieser Wert UMF_ENTITY.

Aktion
Gibt den Typ der Aktion für den eingehenden Identitätsdatensatz an:

- *A* für Hinzufügen (Add)
- *C* für Ändern (Change)
- *D* für Löschen (Delete)

Als Teil des ETL-Prozesses verwenden Identitätsdatensätze in der Regel UMF-Tagging, um anzuzeigen, wie bei dem jeweiligen eingehenden Datensatz während der Systemverarbeitung verfahren werden soll.

Segment
Zeigt den Namen des UMF-Segments an, in dem die Ausnahmebedingung aufgetreten ist.

UMF-Tag
Zeigt den Wert des UMF-Tags an, der die UMF-Ausnahmebedingung verursacht hat.

Ausnahmebedingung
Zeigt die Nachrichten-ID oder einen anderen Ausnahmecode an, die bzw. der den Typ der aufgetretenen UMF-Ausnahmebedingung angibt und Informationen zur Behebung der Ausnahmebedingung liefert. Diese Informationen befinden sich auch in der Tabelle UMF_EXCEPT.

Anzahl Segmentausnahmebedingungen
Gibt die Gesamtanzahl der UMF-Ausnahmebedingungen dieses Typs an.

Überprüfen Sie den Zähler für schlechte Qualität im Abschnitt mit der Qualitätszusammenfassung, um festzustellen, ob ein entsprechender Datentyp mit schlechter oder unbrauchbarer Qualität gemeldet ist. Wird das Problem durch UMF-Fehler verursacht, stimmen die Zahlen bei **Zähler für schlechte Qualität** im Abschnitt mit der Qualitätszusammenfassung und bei **Anzahl Segmentausnahmebedingungen** im Abschnitt mit den UMF-Ausnahmebedingungen für dasselbe UMF-Segment und dieselben UMF-Tags häufig überein.

Rollenalert - Detailbericht:

Der Bericht für Rollenalert-Details enthält vollständige Details zu einem bestimmten Rollenalert sowie den an dem Alert beteiligten Entitäten auf jedem Abgrenzungsgrad. Dieser Bericht ist nützlich, wenn Sie Ihre Analyse der an jedem Rollenalert beteiligten Entitäten ausweiten wollen.

Für jeden Abgrenzungsgrad zeigt der Bericht Informationen zu den beiden Entitäten an, die an dem Alert beteiligt sind, sodass Sie sie vergleichen und gegenüberstellen können. Zudem zeigt der Bericht andere Alerts, die den einzelnen Entitäten zugeordnet sind, sodass Sie einen vollständigen Überblick über jede Entität und die zugehörigen Rollenalerts erhalten. Die Details zu einem Rollenalert sind normalerweise mehrere Seiten lang.

Alert-ID
Beschreibung und Alert-ID für einen bestimmten Rollenalert. Die Alert-ID wird vor der Beschreibung in der Kopfzeile des Berichts angezeigt.

Rollenalertinformationen
Dieser Abschnitt zeigt allgemeine Informationen für den Rollenalert an, wie eine Beschreibung der Rollenalertregel, die diesen Alert ausgelöst hat, und den Status des Rollenalerts.

Alertdatum und -zeit
Datum und Zeit der Generierung dieses Rollenalerts.

Regel-ID
Bei der Erstkonfiguration der Rollenalertregel vom System generierte interne Nummer. Diese ID ist der Rollenalertregel zugeordnet, die diesen Rollenalert auslöste.

Regelbeschreibung
Text, der die Rollenalertregel beschreibt und von dem Benutzer definiert wird, der die Rollenalertregel konfiguriert.

Wertigkeit
Benutzerdefinierter Code, der die Priorität oder Bedeutung dieses Alerts anzeigt.

Status Aktuelle Disposition dieses Rollenalerts.

Übereinstimmungswahrscheinlichkeit der Beziehung
Diese Bewertung zeigt an, wie eng die Beziehung der beiden im Abschnitt **Übereinstimmende Details: Grad *n*** aufgelisteten Entitäten ist. Je höher die Bewertung ist, umso enger ist die Beziehung. Eine Bewertung von 100 gibt an, dass die eingehende Entität und die abgeglichene Entität dieselbe Entität sind.

Die Bewertung für die Übereinstimmungswahrscheinlichkeit der Beziehung wird vom System während des Entitätsauflösungsprozesses generiert.

Auflösungsbewertung
Diese Bewertung zeigt an, wie groß die Übereinstimmung der beiden Entitäten ist. Je höher die Bewertung ist, umso größer ist die Übereinstimmung. Eine Bewertung von 100 gibt an, dass die eingehende Entität und die abgeglichene Entität dieselbe Entität sind.

Die Auflösungsbewertung wird vom System während des Entitätsauflösungsprozesses generiert.

Übereinstimmungswahrscheinlichkeit für Auflösung
Als Teil der Entitätsauflösung konfigurierte Basisauflösungsbewertung, die die Mindestbewertung angibt, mit der die eingehende Entität und die übereinstimmende Entität zu einer Entität aufgelöst werden sollen. Die Auflösungsbewertung und die Bewertung der Übereinstimmungswahrscheinlichkeit der Auflösung sind häufig identisch.

Abschnitt 'Übereinstimmende Details: Grad *n*'
Dieser Abschnitt enthält übereinstimmende Details für Entitäten, die an dem Alert beteiligt sind, und Identitätsinformationen für die jeweiligen Entitäten. Die beiden Entitäten werden als Entität *x* (Eingehende Identität) und Entität *y* (Übereinstimmende Identität) dargestellt.

Der Bericht enthält für jede Entität und jeden Attributdatentyp die übereinstimmenden Datenwerte sowie die Datenquelle und die externe ID, die den Datenwerten der Entitäten zugeordnet sind. Zudem zeigt der Bericht die Genauigkeitsbeschreibungen und Bewertungen für die übereinstimmenden Attribute. Lautet eins der übereinstimmenden Attribute Name, kann der Bericht auch die Informationen darüber enthalten, wie die Namen bei der Entitätsauflösung bewertet wurden (abhängig von den für die Entitätsauflösung konfigurierten Namensbewertungsoptionen).

Datentyp
Name des übereinstimmenden Attributs.

Wert Der übereinstimmende Datenwert.

Datenquelle
Für jede Entität der Datenquellencode und die Beschreibung, die das übereinstimmende Attribut und den übereinstimmenden Datenwert zur Verfügung gestellt haben. Diese Informationen geben die ursprüngliche Quellendatei an.

Externe ID
Für jede Entität die externe ID, die dem Datenquellencode zugeordnet ist, der das übereinstimmende Attribut und den übereinstimmenden Datenwert zur Verfügung gestellt hat. Diese Informationen geben häufig eine Kontonummer für die Entität in der ursprünglichen Quellendatei an.

Genauigkeitsbeschreibung
Text, der die Genauigkeitsstufe beschreibt, auf der die Entitäten übereinstimmten.

Genauigkeitsstufen werden während der Entitätsauflösungskonfiguration nach Attribut konfiguriert.

Genauigkeit / Max. Genauigkeit
Die erste Zahl ist die vom System generierte Genauigkeitsbewertung, die angibt, wie exakt **Entität** *x* (Eingehende Identität) mit **Entität** *y* (Übereinstimmende Identität) übereinstimmt. Die zweite Zahl ist die maximale Genauigkeitsbewertung, die erreicht werden kann.

Durch einen Vergleich der beiden Zahlen können Sie die Übereinstimmungsgenauigkeit zwischen den Entitäten eingehender ermitteln. Mithilfe dieser Bewertungen können Sie auch feststellen, ob die Alertsuchkriterien angepasst werden müssen.

Bewertungsanpassung
Die Auflösungsbewertung wurde mit dieser Zahl angepasst. Diese Zahl wird während der Entitätsauflösungskonfiguration konfiguriert.

Namensbewertung - Details
Hat eines der übereinstimmenden Attribute den Datentyp Name, kann der Bericht auch Informationen darüber enthalten, wie die Namensübereinstimmungen im Entitätsauflösungsprozess bewertet wurden. Damit dieser Abschnitt des Berichts angezeigt wird, muss mindestens eine der folgenden Namensoptionen während der Entitätsauflösung konfiguriert sein:

- Name Manager
- Namensvergleichsoperator 2

Vollständiger Name
Bewertung (0-100), die anzeigt, wie groß die Übereinstimmung zwischen den vollständigen Namen beider Entitäten war. Diese Bewertung ist als Teil der Entitätsauflösung konfiguriert.

Familienname
Bewertung (0-100), die anzeigt, wie groß die Übereinstimmung zwischen den Familiennamen beider Entitäten war. Diese Bewertung ist als Teil der Entitätsauflösung konfiguriert.

Vorname
Bewertung (0-100), die anzeigt, wie groß die Übereinstimmung zwischen den Vornamen beider Entitäten war. Diese Bewertung ist als Teil der Entitätsauflösung konfiguriert.

Entität *x* und *y* Abschnitt 'Identitätsinformationen'
Dieser Abschnitt des Berichts enthält spezielle Informationen zu den einzelnen Identitäten.

Datentyp
Merkmalname. (Beispiel: Name.)

Wert Merkmalwert. (Beispiel: SMITH, BRUCE.)

Abschnitt 'Andere Alerts für Entität *x* und *y*'
Dieser Abschnitt des Berichts zeigt den Verlauf aller anderen Rollenalerts und Beziehungen, die der eingehenden Entität (Entität *x*) und der übereinstimmenden Entität (Entität *y*) zugeordnet sind. Er enthält darüber hinaus das Ereignisalertprotokoll aller Ereignisalerts, die der eingehenden Entität (Entität *x*) und der übereinstimmenden Entität (Entität *y*) zugeordnet sind. Diese Informationen können Ihnen ein umfassenderes Bild der einzelnen Entitäten sowie der zugehörigen Alerts und Beziehungen zu anderen Entitäten zur Verfügung stellen, was bei Ihrer Analyse hilfreich sein kann.

Rollenalertprotokoll
Enthält die Informationen des Rollenalertprotokolls **Entitätszusammenfassung**.

Datum und Zeit des Alerts
Datum und Zeit der Generierung des Rollenalerts.

Alert-ID
Beschreibung und Alert-ID für diesen Rollenalert.

Beschreibung
Text, der die Rollenalertregel beschreibt, die diesen Alert ausgelöst hat.

Entitäts-ID
ID-Nummer für die Entität in dieser Zeile, die mit der Entität übereinstimmte, die nach Nummer in **Andere Alerts für Entität *n*** aufgelistet war.

Name Name der anderen Entität, die mit der Entität übereinstimmte, die nach Nummer in **Andere Alerts für Entität *n*** aufgelistet war.

Beziehungen
Anzahl von Beziehungen, die der zusammengehörigen Entität zugeordnet wurden.

Beziehungsbewertung
Diese Bewertung zeigt an, wie eng die Beziehung der beiden Entitäten ist. Je höher die Bewertung ist, umso enger ist die Beziehung. Eine Bewertung von 100 gibt an, dass die eingehende Entität und die abgeglichene Entität dieselbe Entität sind.

Diese Bewertung wird vom System während des Entitätsauflösungsprozesses generiert.

Aktivitätscode
Benutzerdefinierter Code, der eine Aktion angibt, die bei diesem Alert von einem Benutzer ausgeführt wird. Aktivitätscodes werden in der Konfigurationskonsole konfiguriert und in einer Dropdown-Liste in Visualizer ausgewählt, wenn ein Alert aktualisiert wird. Es gibt beispielsweise die Aktivitätscodes **Offen**, **Zugeordnet**, **Angehalten** und **Geschlossen**.

Status Dispositionsstatus für diese Alertaktualisierung, geändert am Statusdatum und zur Statuszeit. Statusangaben werden in der Reihenfolge der Aktualisierungen angezeigt, sodass die letzte Statusaktualisierung zuletzt aufgelistet wird.

Ereignisalertprotokoll
Enthält die Informationen des Ereignisalertprotokolls **Entitätszusammenfassung**.

Alertdatum und -zeit
Datum und Zeit der Ereignisgenerierung.

Alert-ID
Eindeutige, vom System generierte Kennung für den Ereignisalert.

Beschreibung
Beschreibung des Ereignisalerts, von der Ereigniskonfiguration in der Konfigurationskonsole.

Rollenalertstatus - Bericht:

Im Rollenalertstatusbericht wird der Status aller Rollenalerts für eine bestimmte Zeit zusammengefasst. Mit diesem Bericht können Sie Rollenalerts anzeigen und verwalten.

Der Bericht ist nach Rollenalert-ID und Alertdatum und -zeit sortiert.

Alert-ID - Beschreibung
Zeigt die vom System generierte Rollenalert-ID und die Beschreibung des Rollenalerts an, die von der zugeordneten Rollenalertregel abgerufen wurde.

Datum und Zeit des Alerts
Gibt Datum und Zeit der Erstellung des Rollenalerts an.

Übereinstimmende Entitätsinformationen
Dieser Abschnitt zeigt den Dispositionsverlauf des Alerts beginnend mit der jüngsten Statusaktualisierung.

Entität 1 und Entität 2
Zeigt die Entitäts-IDs und normalerweise die vollständigen Namen der beiden Entitäten an, die gemäß den Kriterien für diesen Rollenalert (nach Alert-ID-Beschreibung) übereinstimmten.

Aktivitätscode
Zeigt einen benutzerdefinierten Code an, der eine Aktion angibt, die bei diesem Alert von einem Benutzer ausgeführt wird. Aktivitätscodes werden in der Konfigurationskonsole konfiguriert und in einer Dropdown-Liste in Visualizer ausgewählt, wenn ein Alert aktualisiert wird. Es gibt beispielsweise die Aktivitätscodes **Offen**, **Zugeordnet**, **Angehalten** und **Geschlossen**.

Status Zeigt den Dispositionsstatus für diese am am Statusdatum und zur Statuszeit geänderte Alertaktualisierung an. Statusangaben werden in der Reihenfolge der Aktualisierungen angezeigt, sodass die letzte Statusaktualisierung zuletzt aufgelistet wird.

Statusdatum und -zeit
Gibt Datum und Zeit des Auftretens des Alertstatus an.

Benutzer
Zeigt den Namen des Benutzers an, der den Alert mit diesem Alertstatus aktualisiert hat.

Hilfethemen

Fenster 'Kriterien' des Berichts 'Attributalertgenerator - Protokoll':

Über dieses Visualizer-Fenster können Sie die Kriterien für die Anzeige des Berichts 'Attributalertgenerator - Protokoll' angeben. Mit diesem Bericht können Sie Änderungen anzeigen und prüfen, die an Attributalertgeneratoren vorgenommen wurden, beispielsweise Änderungen bei Ablaufdatumsangaben, Fallnummern, Kommentaren oder Status. Wenn Sie die Ergebnisse eines Attributalertgenerators anzeigen wollen, rufen Sie den Bericht zu den Attributalertgeneratoren auf.

Anfangsdatum
Geben Sie das erste Datum in dem Datumsbereich an, für den Daten im ausgewählten Bericht angezeigt werden sollen. Verwenden Sie das Format `MM/TT/JJ`. `01/01/01` beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Standardmäßig wird für **Anfangsdatum** das Tagesdatum verwendet.

Enddatum
Geben Sie das letzte Datum in dem Datumsbereich an, für den Daten im ausgewählten Bericht angezeigt werden sollen. Verwenden Sie das Format

MM/TT/JJ. 01/01/01 beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Standardmäßig wird für **Enddatum** das Tagesdatum verwendet.

Wenn Sie die Daten eines einzelnen Tages sehen wollen, geben Sie in den Feldern **Anfangsdatum** und **Enddatum** dasselbe Datum an.

Dropdown-Liste 'Status'
Wählen Sie einen bestimmten Status aus oder wählen Sie **Alle** aus, um zu allen Status aller Attributalertgeneratoren einen Bericht zu erstellen. Wenn Sie beispielsweise nur die Änderungen anzeigen wollen, die an zurzeit geöffneten Attributalertgeneratoren innerhalb des angegebenen Datumsbereichs vorgenommen wurden, wählen Sie **Öffnen** aus der Dropdown-Liste aus.

Der Standardstatus in der Dropdown-Liste **Status** ist **Alle**, d. h., es werden aktive und abgelaufene Attributalertgeneratoren angezeigt.

Dropdown-Liste 'Benutzer'
Wählen Sie eine Option aus, um Ihre eigenen oder die von einem anderen Benutzer Ihrer Visualizer-Benutzergruppe erstellten Attributalertgeneratoren anzuzeigen.

Die Standardoption ist Eigene Suchen.

Schaltfläche 'Bericht ausführen'
Klicken Sie diese Schaltfläche an, um den Bericht zu generieren.

Fenster 'Kriterien' des Berichts zu den Attributalertgeneratoren:

Über dieses Fenster können Sie die Kriterien für die Anzeige des Berichts zu den Attributalertgeneratoren in Visualizer angeben. Der Bericht zu den Attributalertgeneratoren kann zum Verwalten Ihrer Attributalertgeneratoren oder der von Analysten in Ihrer Visualizer-Benutzergruppe verwendet werden. Wenn Sie hingegen die Änderung des Protokolls für Attributalertgeneratoren anzeigen wollen, verwenden Sie stattdessen den Bericht zum Protokoll für die Attributalertgeneratoren.

Anfangsdatum
Geben Sie das erste Datum im Datumsbereich an. Verwenden Sie das Format MM/TT/JJ. 01/01/01 beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Standardmäßig wird für **Anfangsdatum** das Tagesdatum verwendet.

Enddatum
Geben Sie das letzte Datum im Datumsbereich an. Verwenden Sie das Format MM/TT/JJ. 01/01/01 beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Standardmäßig wird für **Enddatum** das Tagesdatum verwendet.

Wenn Sie die Daten eines einzelnen Tages sehen wollen, geben Sie in den Feldern **Anfangsdatum** und **Enddatum** dasselbe Datum an.

Dropdown-Liste 'Status'
Wählen Sie einen bestimmten Status aus oder wählen Sie **Alle** aus, um zu allen Status aller Attributalertgeneratoren einen Bericht zu erstellen. Wenn Sie beispielsweise nur zurzeit aktive Attributalertgeneratoren innerhalb des angegebenen Datumsbereichs anzeigen wollen, wählen Sie **Öffnen** aus.

Der Standardstatus ist **Alle**, d. h., der Bericht zeigt sowohl die abgelaufenen als auch die aktiven Attributalertgeneratoren an.

Dropdown-Liste 'Benutzer'
Treffen Sie eine Auswahl:

- Wählen Sie **Eigene Suchen** aus (Standardauswahl), wenn Sie nur die von Ihnen erstellten Attributalertgeneratoren anzeigen wollen.
- Wählen Sie **Eigene Gruppe** aus, wenn Sie alle Attributalertgeneratoren anzeigen wollen, die von den Benutzern in Ihrer Visualizer-Benutzergruppe erstellt wurden.

Schaltfläche 'Bericht ausführen'
Klicken Sie diese Schaltfläche an, um den Bericht zu generieren.

Fenster 'Kriterien' des Berichts zu den Attributalerts:

Über dieses Visualizer-Fenster können Sie die Kriterien für die Anzeige des Berichts zu den Attributalerts angeben, der Sie bei der Anzeige und Verwaltung Ihrer Attributalerts unterstützen kann.

Anfangsdatum
Geben Sie das erste Datum in dem Datumsbereich an, für den Daten im ausgewählten Bericht angezeigt werden sollen. Verwenden Sie das Format `MM/TT/JJ`. `01/01/01` beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Standardmäßig wird für **Anfangsdatum** das Tagesdatum verwendet.

Enddatum
Geben Sie das letzte Datum in dem Datumsbereich an, für den Daten im ausgewählten Bericht angezeigt werden sollen. Verwenden Sie das Format `MM/TT/JJ`. `01/01/01` beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Standardmäßig wird für **Enddatum** das Tagesdatum verwendet.

Wenn Sie die Daten eines einzelnen Tages sehen wollen, geben Sie in den Feldern **Anfangsdatum** und **Enddatum** dasselbe Datum an.

Dropdown-Liste 'Status'
Wählen Sie einen bestimmten Status aus, oder wählen Sie **Alle** aus, um zu allen Status aller Attributalerts einen Bericht zu erstellen. Wenn Sie beispielsweise nur die Änderungen anzeigen wollen, die an zurzeit geöffneten Attributalerts innerhalb des angegebenen Datumsbereichs vorgenommen wurden, wählen Sie **Öffnen** aus der Dropdown-Liste aus.

Der Standardstatus in der Dropdown-Liste **Status** ist **Alle**, d. h., es werden aktive und abgelaufene Attributalertgeneratoren angezeigt.

Dropdown-Liste 'Benutzer'
Wählen Sie einen Visualizer-Benutzer nach Benutzernamen aus, oder wählen Sie **Alle** aus, um einen Bericht zu den Attributalerts für alle Visualizer-Benutzer zu erstellen.

In der Dropdown-Liste wird Ihr Benutzername als Standardbenutzer angezeigt.

Schaltfläche 'Bericht ausführen'
Klicken Sie diese Schaltfläche an, um den Bericht zu generieren.

Fenster 'Kriterien' des Berichts 'Datenquelle - Zusammenfassung':

Über dieses Fenster können Sie die Kriterien für die Anzeige des Berichts **Datenquelle - Zusammenfassung** in Visualizer angeben. Im Bericht **Datenquelle - Zu-**

sammenfassung werden Daten angezeigt, die nach Datenquelle in das System geladen wurden. Datenquellen geben Aufschluss darüber, woher die Identitätsdaten stammen.

Dropdown-Liste 'Datenquelle'
Wählen Sie eine bestimmte Datenquelle aus oder wählen Sie **[alle]** aus, um die Daten aus allen Datenquellen anzuzeigen.

Anfangsdatum
Geben Sie das erste Datum in dem Datumsbereich an, für den Daten im ausgewählten Bericht angezeigt werden sollen. Verwenden Sie das Format MM/TT/JJ. 01/01/01 beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Standardmäßig wird für **Anfangsdatum** das Tagesdatum verwendet.

Enddatum
Geben Sie das letzte Datum in dem Datumsbereich an, für den Daten im ausgewählten Bericht angezeigt werden sollen. Verwenden Sie das Format MM/TT/JJ. 01/01/01 beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Standardmäßig wird für **Enddatum** das Tagesdatum verwendet.

Wenn Sie die Daten eines einzelnen Tages sehen wollen, geben Sie in den Feldern **Anfangsdatum** und **Enddatum** dasselbe Datum an.

Schaltfläche 'Bericht ausführen'
Klicken Sie diese Schaltfläche an, um den Bericht zu generieren.

Fenster 'Kriterien' des Berichts zu offengelegten Beziehungen:

Über dieses Visualizer-Fenster können Sie die Kriterien für die Anzeige des Berichts zu offengelegten Beziehungen angeben, der Sie bei der Anzeige und Verwaltung offengelegter Beziehungen unterstützen kann. Offengelegte Beziehungen werden bei der Entitäts- und Beziehungsauflösung zwar nicht erkannt, hierbei handelt es sich jedoch um manuelle Verknüpfungen zwischen zwei Identitäten. Diese manuellen Verknüpfungen werden in der Regel in Visualizer erstellt, können jedoch auch durch Positionieren des UMF-Tagpaares der offengelegten Beziehungen (<DR> und </DR>) für geladene Identitätsdatensätze erstellt und über die Pipelines verarbeitet werden.

Anfangsdatum
Geben Sie das erste Datum in dem Datumsbereich an, für den Daten im ausgewählten Bericht angezeigt werden sollen. Verwenden Sie das Format MM/TT/JJ. 01/01/01 beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Standardmäßig wird für **Anfangsdatum** das Tagesdatum verwendet.

Enddatum
Geben Sie das letzte Datum in dem Datumsbereich an, für den Daten im ausgewählten Bericht angezeigt werden sollen. Verwenden Sie das Format MM/TT/JJ. 01/01/01 beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Standardmäßig wird für **Enddatum** das Tagesdatum verwendet.

Wenn Sie die Daten eines einzelnen Tages sehen wollen, geben Sie in den Feldern **Anfangsdatum** und **Enddatum** dasselbe Datum an.

Schaltfläche 'Bericht ausführen'
Klicken Sie diese Schaltfläche an, um den Bericht zu generieren.

Fenster 'Kriterien' des Ladeergebnisberichts:

Über dieses Fenster können Sie die Kriterien für die Anzeige des Ladeergebnisberichts in Visualizer angeben. Sie können den Ladeergebnisbericht verwenden, um allgemeine Informationen zur Datenqualität von UMF-Dateien zu ermitteln, die Sie in Visualizer geladen haben. Außerdem werden weitere hilfreiche Informationen angezeigt, beispielsweise die Leistungsstatistikdaten, die Anzahl der Entitätenauflösungen und Alerts, die über das Laden der Datei generiert wurden.

Datenquellencode - Dropdown-Liste mit den Beschreibungen
Wählen Sie eine bestimmte Datenquelle aus, oder wählen Sie **[alle]** aus, um die Daten anzuzeigen, die aus allen Datenquellen geladen wurden. Wenn Sie z. B. Identitätsdatensätze aus mehreren UMF-Dateien für ein einzelnes Datum geladen haben, können Sie die Berichtsdaten auf eine einzelne Datenquelle eingrenzen, indem Sie den entsprechenden Datenquellencode auswählen.

Anfangsdatum
Geben Sie das erste Datum in dem Datumsbereich an, für den Daten im ausgewählten Bericht angezeigt werden sollen. Verwenden Sie das Format `MM/TT/JJ`. `01/01/01` beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Standardmäßig wird für **Anfangsdatum** das Tagesdatum verwendet.

Enddatum
Geben Sie das letzte Datum in dem Datumsbereich an, für den Daten im ausgewählten Bericht angezeigt werden sollen. Verwenden Sie das Format `MM/TT/JJ`. `01/01/01` beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Standardmäßig wird für **Enddatum** das Tagesdatum verwendet.

Wenn Sie die Daten eines einzelnen Tages sehen wollen, geben Sie in den Feldern **Anfangsdatum** und **Enddatum** dasselbe Datum an.

Schaltfläche 'Bericht ausführen'
Klicken Sie diese Schaltfläche an, um den Bericht zu generieren.

Fenster 'Kriterien' des Berichts 'Rollenalertstatus':

Über dieses Visualizer-Fenster können Sie die Kriterien für das Generieren des Berichts 'Rollenalertstatus' anzugeben, der den Status der Rollenalerts innerhalb eines bestimmten Zeitraums zusammenfasst und zur Verwaltung Ihrer Rollenalerts verwendet werden kann.

'Anfangsdatum' und 'Anfangszeit'
Geben Sie das erste Datum im Datumsbereich ein, um Daten für den Bericht zu generieren. Verwenden Sie das Format `MM/TT/JJ`. `01/01/01` beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Geben Sie bei Verwendung des 24-Stunden-Formats die erste Zeitangabe im Zeitbereich ein, um Daten für den Bericht zu generieren. Verwenden Sie das Format `HH:MM`. Beispiel: `09:00` entspricht 9:00 morgens und `20:30` entspricht 8:30 abends.

Die Standardeinstellungen für **Anfangsdatum** und **Anfangszeit** lauten `aktuelles Datum` um `00:00`.

'Enddatum' und 'Endzeit'
Geben Sie das letzte Datum im Datumsbereich ein, um Daten im Bericht

zu drucken. Verwenden Sie das Format MM/TT/JJ. 01/01/01 beispielsweise stellt den 1. Januar 2001 dar. Alternativ können Sie auch den Kalender anklicken und das Datum auswählen.

Die Standardeinstellungen für **Enddatum** und **Endzeit** lauten aktuelles Datum um 23:59.

Wählen Sie eine der folgenden Optionen aus, um die Daten eines bestimmten Tages anzuzeigen:

- Geben Sie in die Felder **Anfangsdatum** und **Enddatum** dasselbe Datum ein.
- Geben Sie 00:00 in das Feld **Anfangszeit** und 23:59 in das Feld **Endzeit** ein.

Berichterstellungsbereich für Beziehungsbewertung
Wenn Sie die Ergebnisse anhand der Beziehungsbewertung begrenzen wollen, geben Sie einen Beziehungsbewertungsbereich in die Felder **Von** und **Bis** ein.

Der Standardbereich liegt zwischen 0 und 100. Dieser Bereich umfasst alle Beziehungsbewertungen.

Dropdown-Liste 'Rollenalertregel'
Wählen Sie eine bestimmte Rollenalertregel aus, über die berichtet werden soll.

Dropdown-Liste 'Rollenalertebene'
Wählen Sie eine bestimmte Rollenalertebene aus, oder wählen Sie **Alle** aus, um zu allen Rollenalerts einen Bericht zu erstellen.

Schaltfläche 'Bericht ausführen'
Klicken Sie diese Schaltfläche an, um den Bericht zu generieren.

Analysieren von Daten mit Analyst Toolkit

Sie können die Tools und Vorlagen in Identity Insight Analyst Toolkit zum Erstellen und Anpassen von Analyseberichten und Informationen in einer browserbasierten Anwendungsumgebung verwenden.

Berichterstellung für Daten mit IBM Cognos-Berichten

Analyst Toolkit stellt eine Gruppe von Cognos-Berichten bereit, die zum Erstellen von angepassten Identity Insight-Berichten verwendet werden können.

Die Integration von IBM Cognos in Identity Insight bildet eine Basis für die Möglichkeit der Anpassung von Identity Insight-Berichten, sodass sie zu den von Ihnen benötigten Informationen passen.

Analyst Toolkit enthält die folgenden Elemente für die Verwendung mit IBM Cognos:

- Cognos Business Intelligence-Tools für die Abfrage- und Anwendungsentwicklung
- Erstellung und Bereitstellung eines mit Cognos Framework Manager entwickelten Identity Insight-Datenmodells
- Vorlagenberichte für Entitätszusammenfassungs- und Rollenalertdetails. Diese dienen als Ausgangspunkt für die Anpassung und die Anwendungsentwicklung.

Die Cognos-Berichterstellung und das Frameworkmodell bieten Ihnen die Tools, die zum Erstellen angepasster Cognos-Benutzerschnittstellen und -Berichte auf der

Grundlage des Identity Insight-Repositorys erforderlich sind. Mit den enthaltenen Cognos-Tools können Sie angepasste Schnittstellen erstellen und von EAS bereitgestellte Vorlagen ändern.

In dieser Produktinformation werden die folgenden Begriffe und Konzepte verwendet:

Analyst Toolkit
Identity Insight-Paket für die installierten Cognos-Komponenten und Beispielvorlagen.

EntitySearcher
Eine Thin-Client-Browseranwendung, die die besten Funktionen für die attribut- und auflösungsbasierte Suche in einem browserbasierten Client kombiniert.

IBM Cognos Business Intelligence
Der allgemeine Produktname der in Identity Insight enthaltenen Cognos-Komponente.

Cognos-Bericht
Eine XML-basierte Ausgabespezifikation, die auf die folgenden Arten wiedergegeben werden kann: als interaktive Benutzerschnittstelle in Cognos Viewer, als PDF-Datei, als XML-Datei (für die angepasste Wiedergabe) oder in Form verschiedener Excel-Formate (einschließlich CSV).

Aktiver Bericht
Cognos 10 hat aktive Berichte eingeführt, die eigenständig sind und deren Darstellung und Funktionsweise eher Webanwendungen als Cognos-Standardberichten ähneln.

Cognos Framework Manager
Ein Cognos-Tool, das zum Modellieren einer Datenquelle (in der Regel einer Datenbank) verwendet wird. Das Identity Insight-Datenmodell wurde mit Framework Manager erstellt.

Cognos-Datenmodell
Eine logische Darstellung mindestens einer Datenquelle. Ersteller von Cognos-Berichten verwenden das Datenmodell zum Erstellen interaktiver Berichte.

Cognos-Content-Store
Eine separate Datenbank, die von Cognos zum Speichern von Cognos-Objekten wie Berichtsdefinitionen, Datenmodelle und Abfragen verwendet wird. Der Content-Store wird nicht zum Speichern Ihrer Identity Insight-Daten verwendet.

Analysieren von Daten mit EntitySearcher Thin Client

EntitySearcher Thin Client kombiniert die besten Funktionen für die attribut- und auflösungsbasierte Suche in einem browserbasierten Client.

Identity Insight bietet zwei primäre Suchfunktionen für die Suche nach Entitäten. Die auflösungsbasierte Suche, auch PSuche (PSearch) oder Pipelinesuche genannt, verwendet die Entitätsauflösung beim Suchen von Ergebnissen. Die attributbasierte Suche, auch EQ (Enhanced Query) oder erweiterte Abfrage genannt, verwendet eine konventionellere SQL-Suchfunktion.

EntitySearcher kombiniert diese zwei Suchmethoden, um optimale Ergebnisse zu erzielen und um Zweifel hinsichtlich der zu verwendenden Methode zu vermeiden. Die Clientschnittstelle bietet die vertraute attributbasierte Schnittstelle zur Ein-

gabe von Suchkriterien. Je nach Eingabekriterien und Ergebnissen werden ein oder mehrere Suchtypen von einer Suche aufgerufen. Die Ergebnisse beider Suchfunktionen werden kompiliert, dedupliziert, eingestuft und in einem Suchergebnisraster angezeigt.

Eine weitere Suchverbesserung ermöglicht die Suche nach Entitäten, die ein Geburtsdatum aufweisen, das innerhalb eines bestimmten Datumsbereichs liegt. Diese Suche wird ausgeführt, wenn das Kontrollkästchen **Expand search by** und die zugehörige Dropdown-Liste verwendet werden. Wäre beispielsweise 1.6.1960 als Datum und ein Bereich von 30 Tagen angegeben, würde der in der Suche verwendete effektive Datumsbereich zwischen 2.5.1960 und 1.7.1960 liegen [1.6.1960 minus 30 Tage und 1.6.1960 plus 30 Tage]. Der Bereich schließt die Endpunkte ein.

Sie können die Option **Strict Search** auswählen, wodurch nur die attributbasierte Suche (EQ) verwendet wird. Eine strikte Suche wird standardmäßig ausgeführt, wenn eine der folgenden Bedingungen erfüllt ist.

- Ein einzelnes Attribut wird für die Suchkriterien eingegeben.
- In den Attributsuchkriterien sind unvollständige Elemente vorhanden.
- In einem Attributsuchkriterium werden Platzhalterzeichen verwendet. Beispiel: *.
- Das Attributsuchkriterium DOB (Date of Birth - Geburtsdatum) umfasst einen Datumsbereich.

Die URL zum Starten von EntitySearcher lautet:

`http://server:installationsport/EntitySearcher/`

Von den Suchergebnissen aus können Sie sich zu einer Cognos-Berichtsversion der Identity Insight-Entitätszusammenfassung, zu einer Diagrammkomponente oder zu einem anderen, über HTTP verknüpfbaren Ziel durchklicken. Bitten Sie hierzu den Systemadministrator, die Werte für URL_ENTITY_DETAIL und URL_ENTITY-_GRAPH der Datenbanktabelle COMPONENT_CONFIG zu konfigurieren.

Suchen von Entitäten mithilfe von EntitySearcher:

Sie suchen auf der Basis von Attributdaten und der Suche, die Sie ausführen wollen, nach Entitäten.

Informationen zu diesem Vorgang

EntitySearcher Thin Client kombiniert die besten Funktionen für die attribut- und auflösungsbasierte Suche in einem browserbasierten Client. Sobald eine Suche ausgeführt wird, steht eine Benutzerschnittstelle zum Anzeigen der Suchergebnisse zur Verfügung.

Vorgehensweise

1. Öffnen Sie EntitySearcher in Ihrem Browser.

   Die URL zum Starten von EntitySearcher lautet:

   `http://server:installationsport/EntitySearcher/`

   Beispiel: `http://localhost:13510/EntitySearcher/`. Der Installationsport ist standardmäßig 13510, die Portnummer kann jedoch geändert werden. Setzen Sie sich mit Ihrem Systemadministrator in Verbindung, wenn Sie sich bezüglich des richtigen Servernamens oder der richtigen Portnummer nicht sicher sind.
2. Geben Sie die Suchkriterien in den Bereich **Suchentitäten** ein. Für die Entitätssuche wird standardmäßig ein einzelnes Attribut angezeigt.

a. Wählen Sie den Attributtyp für Ihre Attributsuchkriterien aus der **Attributliste** aus.
b. Geben Sie die Suchkriterien ein.

Option	Bezeichnung
Sie haben zusätzliche Attributsuchkriterien.	Klicken Sie rechts neben dem vorhandenen Attribut das Symbol + an.
Sie haben keine zusätzlichen Attributsuchkriterien.	Fahren Sie mit dem nächsten Schritt fort. **Anmerkung:** Eine strikte Suche wird ausgeführt, wenn nur ein einzelnes Attribut als Suchkriterium eingegeben wurde.

3. Entscheiden Sie, ob Sie eine kombinierte Suche oder nur eine strikte Suche ausführen wollen.

Option	Bezeichnung
Sie führen eine kombinierte Suche aus.	Die kombinierte Suche wird standardmäßig ausgeführt.
Sie führen nur eine strikte Suche aus.	Wählen Sie das Kontrollkästchen **Strict search** aus. **Anmerkung:** Eine strikte Suche wird standardmäßig ausgeführt, wenn eine der folgenden Bedingungen erfüllt ist. • Ein einzelnes Attribut wird für die Suchkriterien eingegeben. • In den Attributsuchkriterien sind unvollständige Elemente vorhanden. • In einem Attributsuchkriterium werden Platzhalterzeichen verwendet. Beispiel: *. • Das Attributsuchkriterium DOB (Date of Birth - Geburtsdatum) umfasst einen Datumsbereich.

4. Klicken Sie **Suche** an.

Ergebnisse

Im Teilfenster **Suchergebnisse** werden alle Entitätssuchergebnisse aufgeführt. Die Ergebnisse werden entsprechend der Ähnlichkeitsbewertung und, falls verfügbar, entsprechend der Namensbewertung eingestuft. Auflösungsbasierte Suchergebnisse mit hoher Bewertung (>86) werden zuerst eingestuft, gefolgt von den attributbasierten Suchergebnissen mit hoher Bewertung. An dritter Stelle folgen die Auflösungssuchergebnisse mit niedrigeren Bewertungen.

Nächste Schritte

Zeigen Sie eine Entitätszusammenfassung für ein Suchergebnis an.
Klicken Sie in der gewünschten Suchergebniszeile der Spalte **Entitäts-ID** im Teilfenster **Suchergebnisse** den unterstrichenen Zahlenwert **Entitäts-ID** an.

Anmerkung: Möglicherweise muss der Systemadministrator den Wert für URL_ENTITY_DETAIL der Datenbanktabelle COMPONENT_CONFIG konfigurieren, um diese Funktionalität zu aktivieren.

Zeigen Sie ein Entitätsdiagramm für ein Suchergebnis an.

Klicken Sie in der gewünschten Suchergebniszeile der Spalte **Entitäts-ID** im Teilfenster **Suchergebnisse** das Diagrammsymbol an.

Anmerkung: Möglicherweise muss der Systemadministrator den Wert für URL_ENTITY_GRAPH der Datenbanktabelle COMPONENT_CONFIG konfigurieren, um diese Funktionalität zu aktivieren.

Beispielbericht für Cognos-Rollenalerts

Der Beispielbericht für Cognos-Rollenalerts zeigt Informationen zu den am Alert beteiligten Entitäten und Entitätsbeziehungen an und kann mithilfe von Cognos-Tools angepasst werden.

Der Rollenalertbericht verwendet die in Cognos 10 eingeführte Technologie der aktiven Berichte und bietet dem Benutzer eine erweiterte Funktionalität.

Alertinformationen werden zusammen mit allen Pfaden eines Alerts auf einer separaten, dynamisch erstellten Registerkarte angezeigt. Die Informationen der Rollenalertzusammenfassung werden im Bericht oben angezeigt und es sind Momentaufnahmen von Entitäten (Status der Entität zum Zeitpunkt der Alertgenerierung) verfügbar, falls der Benutzer diese Informationen anzeigen will. Ein erweiterter Abgleichsdetailabschnitt enthält Identity Insight-Bewertungsinformationen.

Datenzugriff

Der Rollenalertdetailbericht verwendet in hohem Maße die neuen Identity Insight-Datenbanksichten. Diese Methode ermöglicht mehr Steuerungsmöglichkeiten für den Datenzugriff. Verknüpfungs- und Abfragestrukturen beispielsweise werden nicht über die Cognos-Engine, sondern über die SQL-Sicht definiert. Die Methode bietet auch eine Abstraktionsebene von den zugrunde liegenden Datentabellen, wodurch das zugrunde liegende Schema geändert werden kann, ohne dass dies direkten Einfluss auf die Cognos-Berichte hat.

Es gibt zwar neue Identity Insight-Datenbanksichten, die die Detailanzeige für Cognos-Rollenalerts unterstützen, der Datenzugriff wird jedoch vom Cognos-Server über das Modell bereitgestellt und gesteuert.

Technische Hinweise

Der Detailbericht für Cognos-Rollenalerts verwendet die Technologie der aktiven Berichte. Dies bedeutet, dass HTML der einzige unterstützte Ausgabetyp ist. Im Gegensatz zum Cognos-Standardbericht werden alle vom Bericht verwendeten Daten vor der Anzeige des Berichts abgefragt. Dadurch behalten aktive Berichte ihre Interaktivität bei, wenn ihre Verbindung mit dem Cognos-Server getrennt wird. Aktive Berichte können als MHT-Dateien (MIME HTML) verteilt werden und werden über die Cognos-Homepage erstellt oder über den Zugriff auf eine URL für den Bericht, der über einen beliebigen Web-Browser mit MHT-Dateiunterstützung erfolgt. Ein weiterer Nebeneffekt des Ladens aller Berichtsdaten im Voraus ist, dass die Seite nicht erneut geladen werden muss, wenn der Benutzer mit der Benutzerschnittstelle interagiert.

Der Cognos-Rollenalertbericht benötigt eine Rollenalert-ID als Parameter. Wird auf den Bericht direkt zugegriffen, wird der Benutzer zur Eingabe einer Rollenalert-ID aufgefordert. Erfolgt der Zugriff auf den Bericht als Komponente, kann die Rollenalert-ID als URL-Parameter eingegeben werden. Bei der Weitergabe von Cognos-Parametern per URL wird dem Namen der Eingabeaufforderung **p_** vorangestellt.

Im Fall des Rollenalertberichts lautet der erwartete Parameter **pAlertID**, woraus sich die folgende Syntax ergibt: **p_pAlertID**. Beispiel: **&p_pAlertID=55&**.

Die zur Unterstützung der Cognos-Komponenten erstellten Identity Insight-Datenbanksichten erhalten einen Namen mit dem Präfix COG, damit sie besser erkennbar sind.

Für Firefox 3.x ist die Installation zusätzlicher Plug-ins erforderlich, damit MHT-Dateien korrekt angezeigt werden können.

Beispielbericht für Cognos-Entitätszusammenfassung

Der Beispielbericht für die Cognos-Entitätszusammenfassung enthält alle bekannten Informationen zu einer Entität und kann mit Cognos-Tools angepasst werden.

Im Cognos-Zusammenfassungsbericht werden die Entitätsdaten zusammengefasst und der Benutzer kann entscheiden, welche Entitätsdetails er untersuchen will.

Technische Hinweise

Die Cognos-Entitätszusammenfassung verwendet im Gegensatz zu den tatsächlichen Datenbanksichten in hohem Maße berichtsdefinierte Abfrageobjekte. Diese virtuellen Abfragen basieren auf dem Cognos-Datenmodell und ihre Erstellung erfolgt durch das Ziehen von Modellobjekten in das Berichtsabfrageerstellungsprogramm und das Festlegen von Eigenschaften. Die Zusammenfassung verwendet zum Anzeigen des Detailabschnitts einen *bedingten Block*. Aufgrund der Verwendung eines bedingten Blocks, durch den die Anzeige einer Benutzerschnittstelle (und nicht einem Bericht) ähnelt, entsprechen die Darstellung und Funktionsweise der PDF-, Text- und Excel-Ausgabeversionen dieses Berichts nicht denen der HTML-Standardausgabe.

Der Cognos-Berichtsserver fragt nur die Informationen ab, die er zum Anzeigen der sichtbaren Berichtsabschnitte benötigt. Die Rollenalertinformationen werden beispielsweise nur abgefragt, wenn der Benutzer diese anzeigen will. Dies führt zu kürzeren anfänglichen Ladezeiten und einem intelligenteren Datenzugriff, hat jedoch auch Nachteile. Die Seite muss erneut geladen werden, wenn sich der Detailabschnitt ändert. Das erneute Laden dieser Seite erfolgt automatisch und erfordert keine Benutzerinteraktion. Der Benutzer muss jedoch warten, bis die Seite aktualisiert wurde, bevor er weitere Benutzerinteraktionen ausführen kann.

Für den Cognos-Zusammenfassungsbericht ist lediglich ein Parameter erforderlich, und zwar eine Identity Insight-Entitäts-ID. Wird der Bericht über die Cognos-Homepage ausgeführt, wird der Benutzer zur Eingabe einer Entitäts-ID aufgefordert. Einige Benutzer werden den Bericht möglicherweise über die Cognos-Homepage starten und eine Entitäts-ID eingeben. Es ist jedoch wahrscheinlicher, dass die Cognos-Zusammenfassung als integrierte Komponente vorliegt, die über eine andere Anwendung, beispielsweise ein Workflow- oder Fallverwaltungstool, aufgerufen wird. Ist letzteres der Fall, kann die Identity Insight-Entitäts-ID als URL-Parameter für die Cognos-Zusammenfassung übergeben werden und die Eingabeaufforderungsseite für die Entitäts-ID wird nicht angezeigt.

Bei der Weitergabe von Cognos-Parametern per URL wird dem Namen der Eingabeaufforderung **p_** vorangestellt. Im Fall des Zusammenfassungsberichts lautet der erwartete Parameter **pEntityID**, woraus sich die folgende Syntax ergibt: **p_pEntityID**. Beispiel: **&p_pEntityID=5&**.

Erkennen und Installieren von Cognos-Komponenten

Sie installieren IBM Cognos-Komponenten, um die IBM Identity Insight-Komponenten für die Erstellung von Cognos-Berichten verwenden und modifizieren zu können.

Vorbereitende Schritte

Sie müssen IBM Business Intelligence Reporting installiert haben, bevor Sie die IBM Identity Insight-Berichte für Cognos bereitstellen können.

Anmerkung: Wenn Sie eine vorhandene Instanz von IBM Cognos Business Intelligence Reporting Version 10.1.0 oder höher installiert haben, können Sie die IBM Identity Insight-Berichte für Cognos dort bereitstellen.

Sie müssen IBM Cognos Framework Manager installieren, um die Metadaten der Identity Insight-Berichte für Cognos modifizieren zu können.

Vorgehensweise

1. Installieren Sie IBM Business Intelligence Reporting Version 10.1.0 oder höher.
   a. Befolgen Sie die detaillierten Cognos-Anweisungen, um die Komponente Cognos Reporting zu installieren.
2. Installieren Sie IBM Cognos Framework Manager Version 10.1.0 oder höher.
   a. Befolgen Sie die detaillierten Cognos-Anweisungen, um die Komponente Cognos Reporting zu installieren.

Nächste Schritte

Stellen Sie die Identity Insight-Berichte in Cognos bereit.

Bereitstellen von Identity Insight-Berichten in Cognos:

Sie müssen zunächst die Cognos-Berichte von IBM Identity Insight für Rollenalerts und die Entitätszusammenfassung in IBM Cognos Business Intelligence Reporting bereitstellen, bevor Sie sie aktivieren können.

Vorbereitende Schritte

Installieren Sie IBM Cognos Business Intelligence Reporting.

Vorgehensweise

1. Kopieren Sie das Identity Insight-Paket für die Bereitstellung von Cognos-Berichten in die IBM Cognos Business Intelligence Reporting-Installation. Identity Insight stellt zwei Versionen der Berichte bereit, je nachdem, ob Sie den kompatiblen oder den dynamischen Abfragemodus von Cognos nutzen wollen.

Tabelle 32. Speicherpositionen des Identity Insight-Pakets für die Bereitstellung von Cognos-Berichten

Datei kopieren aus	Datei kopieren in
<*produktinstallationsverzeichnis*>ibm-home/cognos/deployment/IdentityInsight_v9.0_CompatibleQueryMode.zip oder <*produktinstallationsverzeichnis*>/ibm-home/cognos/deployment/IdentityInsight_v9.0_DynamicQueryMode.zip	<*cognos-installationsverzeichnis*>/deployment/

2. Rufen Sie in Ihrem Browser die Seite für Cognos Connection auf. Die Adresse der Seite lautet **http://<*name_oder_ip-adresse_des_cognos-servers*>:<*cognos-port_#*>:cognos/index.html**.
3. Klicken Sie **Starten** > **IBM Cognos Administration** an.

   Anmerkung: Sie müssen über die erforderlichen Berechtigungen für die gesicherte Verwaltungstaskkomponente verfügen, um auf IBM Cognos Administration zugreifen zu können.
4. Rufen Sie die Registerkarte **Konfiguration** auf und klicken Sie **Inhaltsadministration** an. Klicken Sie auf der Symbolleiste das Symbol **Neuer Import** an.
5. Wählen Sie in der Liste der verfügbaren Bereitstellungspakete `IdentityInsight_v9.0_Cognos` aus. Geben Sie `ISII4YOU` ein, wenn Sie zur Eingabe eines Kennworts aufgefordert werden. Klicken Sie **OK** an.
6. Klicken Sie im Teilfenster für Name und Beschreibung die Option **Weiter** an. Im Teilfenster für den Namen und die Beschreibung müssen keine Änderungen vorgenommen werden.
7. Wählen Sie im Inhaltsteilfenster des allgemein zugänglichen Ordners das Kontrollkästchen für den Ordner **ISII** in der Liste der verfügbaren Inhalte der allgemein zugänglichen Ordner aus. Klicken Sie **Weiter** an.
8. Klicken Sie im Teilfenster **Verzeichnisinhalt** die Option **Weiter** an. Im Teilfenster **Verzeichnisinhalt** müssen keine Änderungen vorgenommen werden.
9. Klicken Sie im Teilfenster **Allgemeine Optionen** die Option **Weiter** an. Im Teilfenster **Allgemeine Optionen** müssen keine Änderungen vorgenommen werden.
10. Prüfen Sie die Zusammenfassung und klicken Sie **Weiter** an.
11. Wählen Sie **Speichern und einmal ausführen** aus. Klicken Sie **Fertigstellen** an, um den Bericht zu importieren. Klicken Sie **Ausführen** an. Die Ausführungsoptionen müssen nicht geändert werden.
12. Rufen Sie die Details zum Import auf, bevor Sie das Dialogfenster schließen. Klicken Sie **OK** an. Wenn der Status `Wird ausgeführt` angezeigt wird, klicken Sie **Aktualisieren** an. Nach erfolgreicher Bereitstellung wird der Status `Erfolgreich` angezeigt. Klicken Sie **Schließen** an.

Nächste Schritte

1. Prüfen Sie, ob die Berichte bereitgestellt wurden.
2. Modifizieren Sie die Konfiguration der Datenbank für die Bereitstellung der Identity Insight-Berichte in Cognos.

Prüfen der Bereitstellung der Identity Insight-Berichte:

Nach dem Bereitstellen der Berichte müssen Sie die Bereitstellung prüfen, bevor Sie die Berichte ausführen.

Vorbereitende Schritte

Stellen Sie die Identity Insight-Berichte in Cognos bereit.

Vorgehensweise

1. Rufen Sie in Ihrem Browser die Seite für Cognos Connection auf. Die Adresse der Seite lautet **http://<*name_oder_ip-adresse_des_cognos-servers*>:<*cognos-port_#*>:cognos/index.html**.

2. Prüfen Sie auf der Registerkarte **Öffentliche Ordner**, ob der öffentliche Ordner **ISII** vorhanden ist.
3. Wählen Sie den Ordner **ISII** aus.
4. Prüfen Sie, ob ein einzelnes Paketobjekt **Identity_Insight** vorhanden ist. Ein Paketobjekt wird als blauer Ordner angezeigt.
5. Prüfen Sie, ob die Berichte **ISII_EntityResume** und **ISII_RoleAlertDetailActive** vorhanden sind.

Nächste Schritte

Modifizieren Sie die Konfiguration der Datenbank für die Bereitstellung der Identity Insight-Berichte in Cognos.

Modifizieren der Konfiguration der Datenbank für die Bereitstellung der Identity Insight-Berichte in Cognos:

Nach dem Bereitstellen und Prüfen der Berichte müssen Sie die Konfiguration der Datenbank für die Bereitstellung der Identity Insight-Berichte in Cognos modifizieren. **Anmerkung:** Wenn Sie die Berichte für den dynamischen Abfragemodus verwenden, beachten Sie die Cognos-Dokumentation zum Erstellen einer JDBC-Verbindung innerhalb von Cognos (anstatt der im Folgenden aufgeführten Prozedur).

Vorbereitende Schritte

Stellen Sie die Identity Insight-Berichte in Cognos bereit.

Vorgehensweise

1. Rufen Sie in Ihrem Browser die Seite für Cognos Administrator auf.
2. Wählen Sie **Datenquellenverbindung** auf der linken Seite aus.
3. Wählen Sie das Datenquellenobjekt **ISII** aus.
4. Wählen Sie das Datenquellenverbindungsobjekt **ISII** aus.
5. Wählen Sie das Anmeldeobjekt **ISII** aus.
   a. Klicken Sie **Eigenschaften festlegen** an.
   b. Klicken Sie **Anmeldung bearbeiten...** auf der Registerkarte **Anmelden** ab.
   c. Modifizieren Sie den Link, um den Identity Insight-Datenbankbenutzernamen und das -Kennwort einzuschließen. Klicken Sie **OK** an.
   d. Klicken Sie **OK** an.
6. Klicken Sie **Eigenschaften festlegen** für das Datenquellenverbindungsobjekt an.
7. Vervollständigen Sie auf der Registerkarte **Verbindungen** die Anweisungen für Ihren Identity Insight-Datenbanktyp.

Identity Insight-Datenbanktyp	Anweisungen
DB2	1. Wählen Sie **IBM DB2** als Typ aus. 2. Wählen Sie das Symbol **Verbindungszeichenfolge bearbeiten** aus. 3. Modifizieren Sie den Wert für den DB2-Datenbanknamen. Wenn ein Schema erforderlich ist, fügen Sie dem DB2-Verbindungszeichenfolgeparameter den Eintrag `currentSCHEMA=<schema>` hinzu. 4. Klicken Sie **Die Verbindung testen...** an. 5. Klicken Sie **Testen** an. 6. Stellen Sie sicher, dass der Status `Erfolgreich` lautet.
Oracle	1. Wählen Sie **Oracle** als Typ aus. 2. Klicken Sie **OK** an, wenn eine Warnung angezeigt wird, dass die aktuelle Verbindungszeichenfolge verloren geht. 3. Wählen Sie das Symbol **Verbindungszeichenfolge bearbeiten** aus. 4. Modifizieren Sie die Zeichenfolge für die SQL*Net-Verbindung. 5. Klicken Sie **Die Verbindung testen...** an. 6. Klicken Sie **Testen** an. 7. Stellen Sie sicher, dass der Status `Erfolgreich` lautet.

8. Klicken Sie **Schließen** an, um das Fenster **Testergebnisse** zu schließen.
9. Klicken Sie **Schließen** an, um das Fenster **Verbindungen testen** zu schließen.
10. Klicken Sie **OK** an, um das Fenster **Verbindungen testen** zu schließen.
11. Klicken Sie **OK** an, um das Fenster **Eigenschaften festlegen** zu schließen.

Analysieren von Daten mit dem Diagrammtool

Das InfoSphere Identity Insight-Diagrammtool bietet Benutzern die Möglichkeit, webbasierte Diagramme zu analysieren, in denen Identity Insight-Alerts, Entitätsbeziehungen und andere Entitätsinformationen dargestellt werden.

Für die Wiedergabe von Diagrammen muss beim Diagrammtool eine Produktpipeline im Hintergrund betriebsbereit sein.

Die vom Diagrammtool wiedergegebenen Diagramme ähneln den in der Komponente i2 Analyst's Notebook wiedergegebenen Diagrammen. Ein Vorteil der Verwendung des Diagrammtools besteht jedoch auch darin, dass die Diagramme in ein vorhandenes Fallverwaltungstool oder in eine andere Anwendung integriert und darin gestartet werden können. Benutzer können auch eine URL oder eine Webstartseite verwenden, um die Diagramme in einem Web-Browser anzuzeigen und zu starten. Es ist nicht erforderlich, i2 Analyst's Notebook zum Anzeigen der vom Diagrammtool wiedergegebenen Diagramme zu installieren und zu starten.

Alertdiagramm

Das vom Diagrammtool erzeugte Alertdiagramm zeigt einen bestimmten auf der Alert-ID basierenden Rollenalert an. Im Alertdiagramm können Sie die am Rollenalert beteiligten Entitäten sowie die Attribute anzeigen, die die Entitäten verknüpfen.

Ein Rollenalert tritt auf, wenn mindestens eine über eine Beziehung verknüpfte Entität eine konfigurierte Rollenalertregel erfüllt oder übererfüllt. Rollenalerts basieren auf konfigurierten Rollen und Rollenalertregeln und können Folgendes angeben:

- Warnung oder Problem, beispielsweise, wenn ein Kunde auf einer Beobachtungsliste mit einem verdächtigen Kunden verknüpft ist
- Für den Benutzer interessante Beziehungen, beispielsweise ein Kunde, der gleichzeitig ein Lieferant oder ein Mitarbeiter ist und über eine bestimmte Telefonnummer mit mehreren Kunden verknüpft ist

Tipps zur Verwendung des Alertdiagramms

- Wenn Sie für eine am Alert beteiligte Entität einen Anzeiger für zusammengehörige Entitäten sehen, klicken Sie die Menüoption **Verbleibende zusammengehörige Entitäten anzeigen** mit der rechten Maustaste an, um die verbleibenden zu-

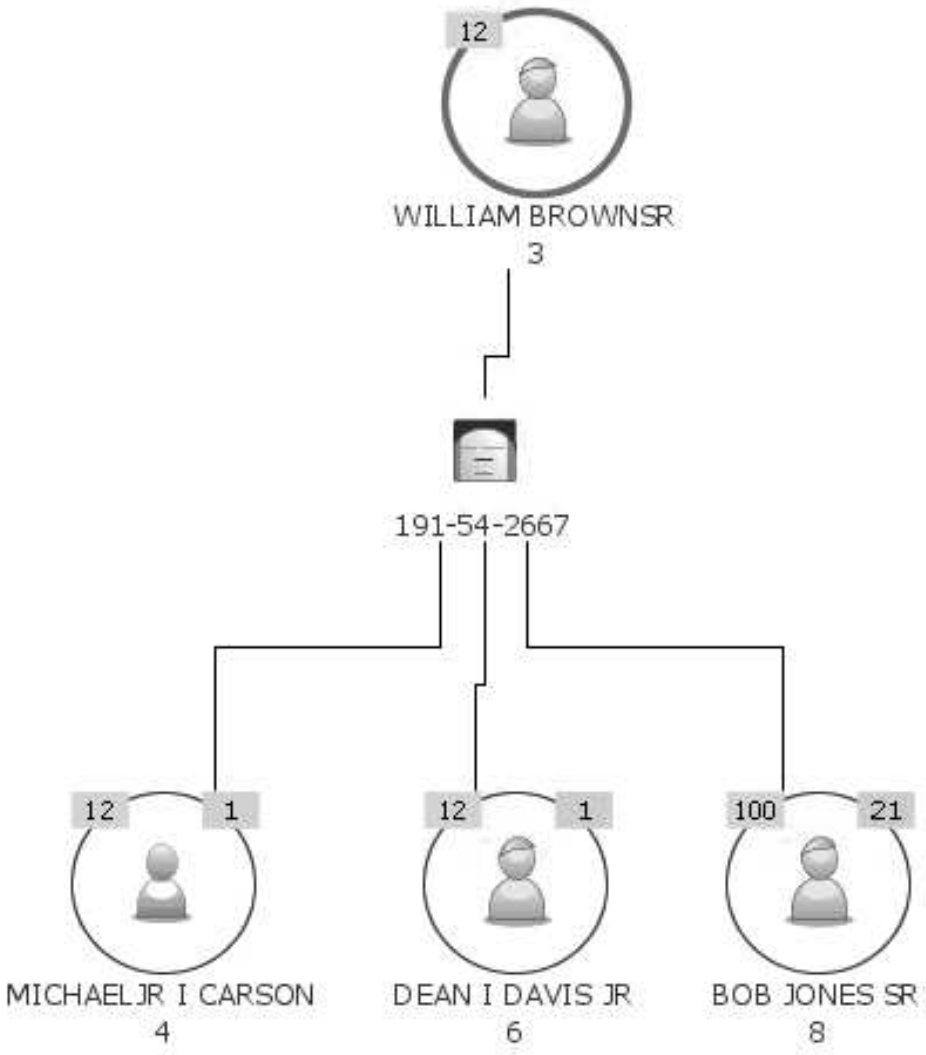
sammengehörigen Entitäten anzuzeigen. Das Diagramm wird erneut gezeichnet, damit alle mit der ausgewählten Entität in Beziehung stehenden Entitäten angezeigt werden. Das Diagramm verknüpft auch automatisch die verbleibenden Entitäten mit allen im Diagramm vorhandenen Entitäten, mit denen diese verbleibenden Entitäten ebenfalls in Beziehung stehen.

- Im Alertdiagramm werden nur die Attribute der Entitäten angezeigt, die am Alert beteiligt waren. Wenn Sie alle einer bestimmten Entität zugeordneten Attribute anzeigen wollen, klicken Sie die Entität mit der rechten Maustaste an und wählen **Verbleibende Attribute anzeigen** aus.
- Wenn Sie die Entitätszusammenfassung für eine bestimmte Entität im Diagramm anzeigen wollen, klicken Sie die Entität mit der rechten Maustaste an und wählen **Zusammenfassung anzeigen** aus. Die Entitätszusammenfassung enthält zusätzliche Details zur Entität, einschließlich der Identitäten dieser Entität und weiterer Alerts, an denen die Entität beteiligt ist. Diese Kontextmenüoption ist nur verfügbar, wenn die Verknüpfung korrekt konfiguriert ist und Sie Zugriff auf das Produkt haben, das die Entitätszusammenfassungen generiert, z. B. Analyst Toolkit.

Entitätsdiagramm

Das vom Diagrammtool erstellte Entitätsdiagramm bietet Unterstützung bei der Darstellung der Beziehungen zwischen der angegebenen Entität und allen Entitäten, die mit ihr in Beziehung stehen, basierend auf den gemeinsam genutzten Attributen.

Im Entitätsdiagramm werden die Beziehungen zwischen den Entitäten mithilfe wechselnder Entitäts- und Attributschichten angezeigt.



Erste Schicht - Hauptentität

Die erste Schicht im Diagramm enthält anfangs die Hauptentität. Die *Hauptentität* ist immer die Entität, die Sie für die Wiedergabe des Entitätsdiagramms angegeben oder ausgewählt haben. Die den Hauptentitätsknoten umgebende Linie wird immer dicker dargestellt. Daran können Sie die Hauptentität ungeachtet ihrer tatsächlichen Position im Diagramm immer erkennen.

Die *oberste Entität* ist die in der ersten Schicht des Diagramms ganz oben angezeigte Entität. Anfangs ist die Hauptentität auch die oberste Entität. Sie können jedoch eine beliebige Entität mithilfe der Kontextmenüoption **Nach oben** zur obersten Entität machen.

Zweite Schicht (und weitere geradzahlige Schichten) - Gemeinsam genutzte Attribute

Die zweite Schicht besteht aus den gemeinsam genutzten Attributen, die die oberste Entität mit den in der dritten Schicht des Diagramms befindlichen Entitäten verknüpft. Für die im Diagramm angezeigten Attribute werden sowohl der Typ als auch der Wert angegeben.

Wenn weitere Schichten im Diagramm vorhanden sind, enthalten die geradzahligen Schichten stets die gemeinsam genutzten Attribute, mit denen die über und unter dieser Attributschicht angezeigten Entitäten verknüpft sind.

Dritte Schicht (und weitere ungeradzahlige Schichten) - zusammengehörige Entitäten Die dritte Schicht des Diagramms enthält Entitäten, die mit der obersten Entität mit einer einstufigen Abgrenzung in Beziehung stehen.

Wenn weitere Schichten im Diagramm vorhanden sind, enthalten die ungeradzahligen Schichten stets die Entitäten, die mit der vorherigen Entitätsschicht in Beziehung stehen, basierend auf den gemeinsam genutzten Attributschichten zwischen den zwei Entitätsschichten. Die in diesen nachfolgenden Entitätsschichten angezeigten Entitäten stehen mit der obersten Entität mit entsprechenden Abgrenzungsgraden in Beziehung: Entitäten in der dritten Schicht stehen über eine zweistufige Abgrenzung mit der obersten Entität in Beziehung. Entitäten der fünften Schicht stehen über eine dreistufige Abgrenzung mit der obersten Entität in Beziehung usw.

Tipps zur Verwendung des Entitätsdiagramms

Entitätsdiagramme können viele Schichten enthalten. Nachfolgend finden Sie einige Tipps hinsichtlich der Einordnung aller in einem Entitätsdiagramm angezeigten Attribut- und Entitätsinformationen.

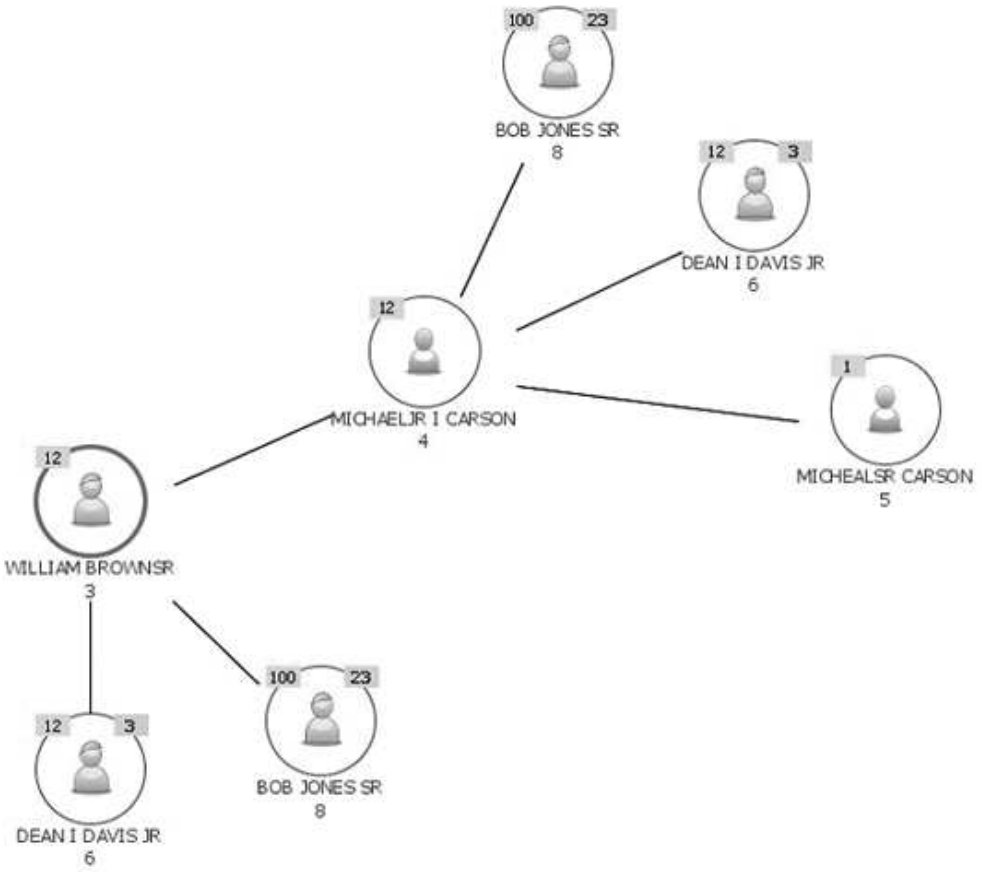
- Gehen Sie wie folgt vor, um weitere Details zu einer Entität aufzurufen:
  - Verwenden Sie die Kontextmenüoption **Verbleibende zusammengehörige Entitäten anzeigen**, um die Beziehungen für eine bestimmte Entität zu untersuchen, die zurzeit nicht im Diagramm angezeigt werden.
  - Verwenden Sie den Schnellfilter **Pfad nach oben anzeigen**, um die Art der Beziehung einer Entität oder eines Attributs zur obersten Entität anzuzeigen. Dieser Filter blendet die Entitäten und Attribute ohne Beziehungen im Diagramm vorübergehend aus.
  - Wechseln Sie in das Diagramm für soziale Netze, um ein Diagramm zu erstellen, in dem Sie die Beziehungen zwischen Entitäten anzeigen und fokussieren können. Im Diagramm für soziale Netze werden keine gemeinsam genutzten Attribute für das Diagramm angezeigt, die gemeinsam genutzten Attribute werden jedoch im Attributexplorer aufgelistet. Klicken Sie die Entität, über die das Diagramm für soziale Netze erstellt werden soll, mit der rechten Maustaste an und wählen Sie anschließend **Neues Diagramm erstellen - Soziales Netz** aus.
  - Verwenden Sie den Schnellfilter **Nur zusammengehörige Entitäten anzeigen**, um ein kleines Diagramm für soziale Netze zu erstellen. Dieser Schnellfilter blendet im Diagramm alle Attribute aus und zeigt nur Entitäten an, die mit einer einstufigen Abgrenzung mit der ausgewählten Entität in Beziehung stehen. (Die *ausgewählte Entität* ist die Entität, die Sie mit der rechten Maustaste angeklickt haben, um den Schnellfilter anzuwenden.)
  - Verwenden Sie den Schnellfilter **Nur zusammengehörige Attribute und Entitäten anzeigen**, um die Entität hervorzuheben und nur die Attribute und Entitäten anzuzeigen, die mit der ausgewählten Entität in Beziehung stehen.
  - Verwenden Sie die Kontextmenüoption **Zusammenfassung anzeigen**, um die Entitätszusammenfassung für eine Entität im Diagramm anzuzeigen. Die Entitätszusammenfassung enthält zusätzliche Details und zusätzlichen Kontext zu dieser Entität, beispielsweise die der Entität zugeordneten Identitäten, weitere Alerts, an denen die Entität beteiligt ist usw. (Ist die Verknüpfung mit der En-

titätszusammenfassung nicht konfiguriert, beispielsweise mit der Entitätszusammenfassung in Analyst Toolkit, wird diese Option nicht im Kontextmenü angezeigt.)

- Gehen Sie wie folgt vor, um den Pfad zwischen zwei Entitäten im Diagramm aufzurufen:
  - Verwenden Sie den Schnellfilter **Pfad nach oben anzeigen**, um die Art der Beziehung einer bestimmten Entität im Diagramm zur obersten Entität anzuzeigen. Dieser Schnellfilter ist insbesondere dann hilfreich, wenn das Diagramm mehrere Schichten enthält.
  - Verwenden Sie die Kontextmenüoption **Nach oben**, um eine Entität in einem Diagramm nach oben zu verschieben und die vorhandenen Attribute und Entitäten entsprechend ihrer Beziehung zur neuen obersten Entität erneut anzuzeigen. Dem Diagramm werden keine neuen Informationen hinzugefügt.
- Gehen Sie wie folgt vor, um weitere Details zu einem Attribut aufzurufen:
  - Verwenden Sie den Schnellfilter **Nur Attribute anzeigen**, um den Fokus im Diagramm auf die Informationen zu einer bestimmten Entität zu setzen. Mithilfe des Filters können Sie sich speziell die Attribute für die ausgewählte Entität anzeigen lassen.
  - Verwenden Sie die Kontextmenüoption **Verbleibende Attribute anzeigen**, um alle Attribute für eine bestimmte Entität anzuzeigen, auch die Attribute, die im aktuellen Diagramm nicht von einer anderen Entität gemeinsam genutzt werden.
  - Verwenden Sie den **Attributexplorer**, um die Entitäten im Diagramm hervorzuheben, die ein bestimmtes Attribut gemeinsam nutzen. Der Wert in der Spalte **Entitäten** gibt Ihnen einen Anhaltspunkt. Je höher die Nummer in der Spalte ist, desto mehr im Diagramm angezeigte Entitäten nutzen dieses Attribut gemeinsam.
- Verwenden Sie zum erneuten Anordnen der Entitäten und Attribute in anderen Mustern und Formen das Kontextmenü, um das Diagrammlayout von **Geschichtet** in **Radial** zu ändern.

Diagramm für soziale Netze

Das Diagramm für soziale Netze unterstützt Sie bei der Darstellung der Beziehungen zwischen der ausgewählten Entität und allen Entitäten, mit denen die ausgewählte Entität verknüpft ist. Dieses eindeutige Diagramm bietet Ihnen eine weitere Möglichkeit, zu sehen, wer wen kennt.



Das Diagramm für soziale Netze enthält die folgenden Elemente:

- Verknüpfungen zwischen Entitäten: Ihnen werden alle Entitäten angezeigt, die mit der Hauptentität (Hubentität) in Beziehung stehen. Die Attribute, mit denen die Entitäten verknüpft sind, werden zwar nicht im Diagramm angezeigt, können jedoch bei Verwendung des Attributexplorers zusammen mit dem Diagramm aufgerufen werden.
- Beziehungscluster: Das Diagramm für soziale Netze ist insofern einmalig, als dass es die miteinander in Beziehung stehenden Entitäten in Gruppen oder Clustern anzeigt. In diesem Diagramm können Sie alle Beziehungscluster sehen, zu denen eine bestimmte Entität gehört, und in den Clustern und Beziehungen nach Mustern suchen.

Sie können das Diagramm erweitern, um alle Entitäten anzuzeigen, die mit einer bestimmten Entität in Beziehung stehen. Bei jeder Anzeige aller Entitäten, die mit einer bestimmten Entität in Beziehung stehen, wird dieser Entitätsknoten zur Hubentität in einem neuen Beziehungscluster.

Zum Beibehalten der Integrität aller Beziehungscluster kann die Entität mehrmals im Diagramm und in mehreren Beziehungsclustern angezeigt werden. Eine Entität wird jedoch nur einmal in einem Beziehungscluster angezeigt. Wählen Sie die Entität durch Anklicken dieses Knotens aus, um alle Beziehungscluster anzuzeigen, an denen die Entität beteiligt ist. Der innere Teil des ausgewählten Entitätsknotens wird bei jedem Beziehungscluster, an dem die Entität beteiligt ist, in blauer Farbe angezeigt.

Stellt eine Entität die Hubentität dar, wird der Anzeiger für zusammengehörige Entitäten nicht angezeigt, da alle mit der Hubentität in Beziehung stehenden Entitäten bereits im Beziehungscluster angezeigt werden. Ist die Entität eine der zusammengehörigen Entitäten im Beziehungscluster und weist sie andere Beziehungen auf, die in diesem Cluster nicht angezeigt werden, wird ein Anzeiger für zusammengehörige Entitäten angezeigt.

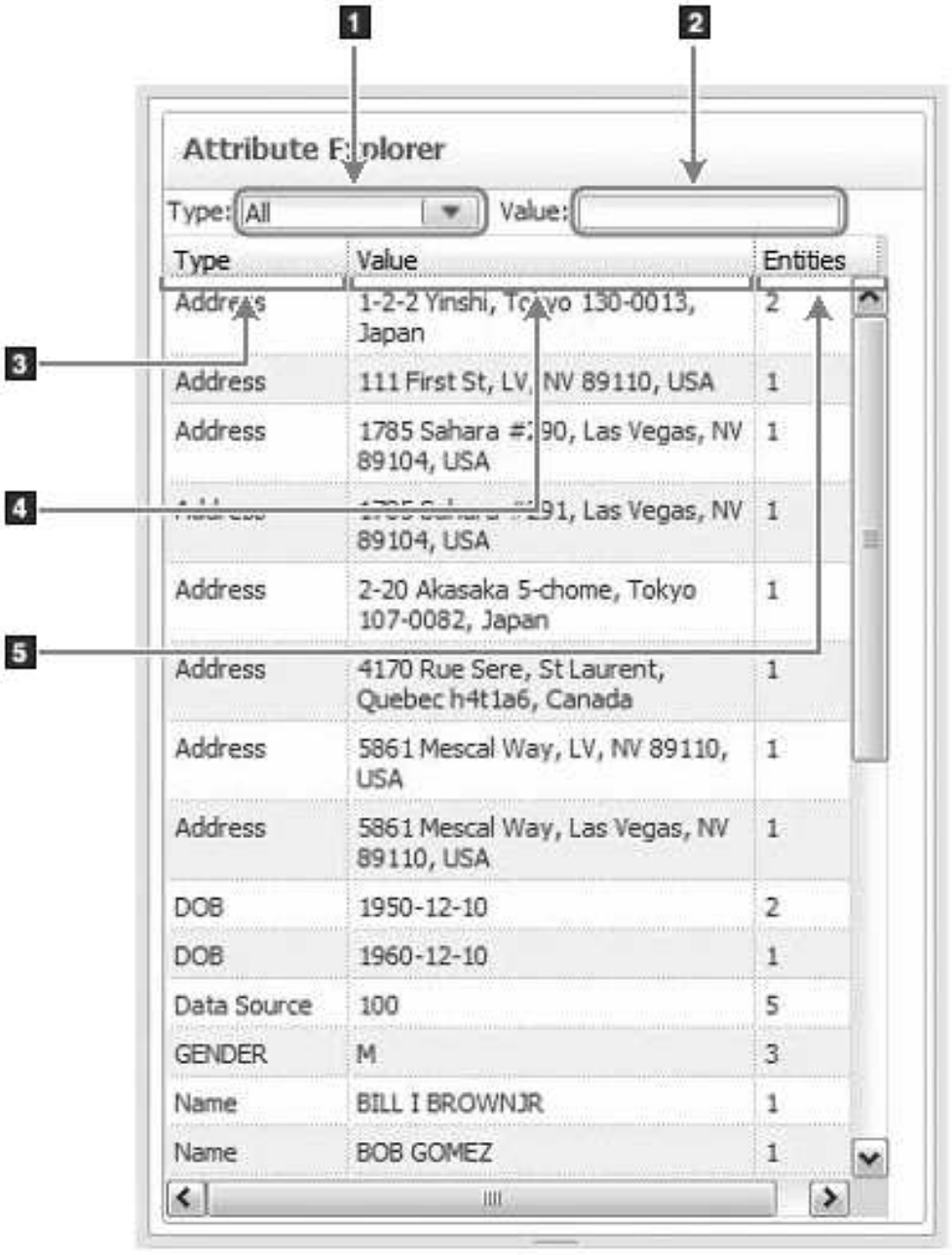
Tipps zur Verwendung des Diagramms für soziale Netze

- Verwenden Sie die Kontextmenüoption **Verbleibende zusammengehörige Entitäten anzeigen**, um die zusammengehörigen Entitäten für mindestens eine Entität im Diagramm zu erweitern. Jede Erweiterung erstellt einen anderen Beziehungscluster. Suchen Sie nach Mustern zwischen Clustern.
- Wenn mehrere Beziehungscluster grafisch dargestellt werden, versuchen Sie diese zu verkleinern, um nach den allgemeineren Mustern und dem allgemeineren Kontext in Clustern zu suchen. Wenn eine bestimmte Entität z. B. in allen oder sehr vielen Clustern angezeigt wird, hat diese Entität innerhalb eines bestimmten Bereichs möglicherweise großen Einfluss. Diese Entität kann jedoch auch eine Schlüsselfunktion beim Herstellen von Verbindungen zwischen mehreren Beziehungsclustern einnehmen.
- Verwenden Sie den Attributexplorer, um zu ermitteln, welche Attribute die zusammengehörigen Entitäten verknüpfen. Wählen Sie eine bestimmte Attributzeile aus, um alle Entitäten im Diagramm hervorzuheben, die dieses Attribut gemeinsam nutzen. Der Wert in der Spalte **Entitäten** zeigt Ihnen, welche Attribute von den meisten Entitäten gemeinsam genutzt werden.

Attributexplorer

Der Attributexplorer, eine Komponente des Diagrammtools, ist eine Tabelle, in der alle Attribute nach Typ und Wert aufgeführt sind, die zu den Entitäten im zurzeit angezeigten Diagramm gehören. Der Attributexplorer ist automatisch rechts vom Erstellungsbereich des Diagramms angedockt.

Bestandteile des Attributexplorers



Nummer in der Abbildung	Element	Beschreibung
1	Dropdown-Liste **Typ**	Wählen Sie einen Attributtyp aus, um die im Attributexplorer angezeigten Attributdaten zu filtern. Wenn Sie die Dropdown-Liste **Typ** verwenden, wird das Diagramm nicht gefiltert. Sie filtern lediglich die Daten im Attributexplorer. Sie können beispielsweise **SSN** auswählen, um die Daten im Attributexplorer zu filtern, damit nur die Sozialversicherungsnummern angezeigt werden. Diese Dropdown-Liste enthält nicht unbedingt alle konfigurierten Attributtypen für das Produkt. Die Liste enthält nur die Attributtypen, die den zurzeit im Diagramm angezeigten Entitäten zugeordnet sind.
2	Textfeld **Wert**	Geben Sie Daten in dieses Feld ein, um die in der Tabelle angezeigten Attributinformationen anhand von Attributwerten einzugrenzen. Der Attributexplorer prüft jedes eingegebene Zeichen und gibt eine Liste der Attributwerte zurück, die mit der Eingabe exakt oder teilweise übereinstimmen. Wenn Sie beispielsweise 123 eingeben, filtert der Attributexplorer in der Liste der Attribute nur die Attributtypen heraus, in denen die Zahlenfolge 123 an einer beliebigen Stelle im Attributwert vorkommt. **Anmerkung:** Der Attributexplorer erkennt keine Platzhalterzeichen. Der Attributexplorer sucht nach der genauen Literalübereinstimmung mit dem Zeichen, das Sie in das Textfeld eingeben. Wenn Sie also ein Platzhalterzeichen, beispielsweise einen Stern (*) eingeben, sucht der Attributexplorer in den Datenwerten nach einer genauen Literalübereinstimmung mit dem Zeichen *.

Nummer in der Abbildung	Element	Beschreibung
3	Spalte **Typ**	Zeigt die zurzeit im Diagramm angezeigten Attributtypen an. Die Spaltenelemente stimmen mit den Beschreibungen überein, die in der Konfigurationskonsole für Attributtypen konfiguriert sind. Ein Kreditkartenattributtyp wird möglicherweise als **CC** oder **Credit Card (Kreditkarte)** angezeigt, je nachdem, wie er in der Konfigurationskonsole konfiguriert wurde. Die Spalte enthält nicht unbedingt alle konfigurierten Attributtypen für das Produkt. Sie enthält nur die zurzeit im Diagramm angezeigten Attributtypen.
4	Spalte **Wert**	Zeigt die zurzeit im Diagramm angezeigten Werte für die Attributtypen an. Ihnen wird möglicherweise der Wert **04-01-1962** angezeigt, der dem Attributtyp für das Geburtsdatum entspricht.
5	Spalte **Entitäten**	Gibt an, wie viele im Diagramm angezeigte Entitäten diesen Attributtyp und -wert gemeinsam nutzen. Anhand dieser Informationen können Sie die am häufigsten gemeinsam genutzten Attribute ermitteln, um diese weiter zu untersuchen.

Tipps zur Verwendung des Attributexplorers

Der Attributexplorer bietet Unterstützung bei der Analyse der Diagramme, insbesondere, wenn diese viele Daten enthalten.

- Suchen Sie über die Spalte **Entitäten** nach Attributen, die nur einer Entität im Diagramm zugeordnet sind. Suchen Sie in der Spalte nach dem Wert 1. Im Diagramm werden nur die Attribute angezeigt, die Entitäten miteinander verknüpfen. Im Attributexplorer werden hingegen alle Attribute angezeigt, die allen im Diagramm enthaltenen Entitäten zugeordnet sind. Diese Attribute verknüpfen die Entität nicht mit einem anderen Entitätsknoten im Diagramm, geben jedoch möglicherweise einen Hinweis auf eine bestimmte Entität, die weiter untersucht werden sollte.
- Grenzen Sie die im Attributexplorer angezeigten Informationen auf einen Attributtyp ein, indem Sie einen Typ aus der Dropdown-Liste **Typ** auswählen. Wird beispielsweise **Rufnummern** angezeigt und von Ihnen ausgewählt, zeigt der Attributexplorer nur Rufnummernattribute und deren Werte an.
- Heben Sie alle Entitäten im Diagramm hervor, die dasselbe Attribut gemeinsam nutzen, indem Sie ein Attribut (Tabellenzeile) im Attributexplorer auswählen.
- Durchsuchen Sie die Daten im vorhandenen Diagramm nach übereinstimmenden oder allgemeinen Attributwerten, indem Sie Daten in das Feld **Wert** eingeben. Wenn Sie beispielsweise 123 eingegeben haben, gibt der Attributexplorer möglicherweise eines oder alle der folgenden übereinstimmenden Attribute zurück:

Typ	Wert
Adresse	**123** Main Street, Anywhere, California, 1**123**4, USA
Adresse	97-**123** Rue Sere, St. Laurent, Quebec, H4T1A6, Canada
Rufnummer	555-222-5**123**
Steuernummer	554-**123**-3**123**

- Sie können auch mehrere vollständige oder partielle Werte in das Feld **Wert** eingeben. Der Attributexplorer behandelt die verschiedenen Werte dann wie eine über AND verknüpfte Abfrage. Wenn Sie beispielsweise `Hund Katze` eingeben, durchsucht der Attributexplorer alle Zeilen nach einer Zeile, die `Hund` UND `Katze` enthält. Die Reihenfolge der verschiedenen Werte in der Abfrage ist nicht relevant. Wenn beispielsweise einer der Attributwerte im Attributexplorer `ihre Katzen und seine Hunde` lautet, ist dieser Wert in den Ergebnissen der Abfrage `Hund Katze` enthalten.
- Sortieren Sie die Informationen im Attributexplorer nach Spalte. Wenn Sie die Spaltenüberschrift anklicken, wird ein Pfeil angezeigt, der die Sortierrichtung angibt.

Ausgewählte Eigenschaften

In der Tabelle **Ausgewählte Eigenschaften**, einer Komponente des Diagrammtools, werden die Eigenschaften des im Diagramm ausgewählten Attributs oder Entitätsknotens angezeigt. In der Tabelle werden nur die Eigenschaften für jeweils einen ausgewählten Knoten (Attribut oder Entität) angezeigt.

- Wenn Sie eine Entität auswählen, werden in diesem Abschnitt alle Attribute (Typen und Werte) angezeigt, die der ausgewählten Entität zugeordnet sind.
- Wenn Sie ein Attribut auswählen, werden in diesem Abschnitt alle Entitäten angezeigt, die das ausgewählte Attribut gemeinsam nutzen, einschließlich der Entitäts-ID für jede Entität. In der dritten Spalte dieses Abschnitts wird Ihnen auch die Entitäts-ID der Datenquelle angezeigt, aus der die Attributdaten stammen.

Navigieren in den Diagrammen des Diagrammtools und Durchsuchen der Diagramme

Sie können mithilfe der Navigationsleiste oder der Kontextmenüoptionen in den einzelnen im Diagrammtool dargestellten Diagrammen navigieren und die Diagramme durchsuchen.

Navigationsleiste

Die Navigationsleiste direkt unter dem Diagrammtitel enthält Symbole für die Standarddiagrammnavigation.

- Auswahlmodusoptionen: Wählen Sie einzelne oder mehrere Diagrammelemente aus (oder wählen Sie einen bestimmten Diagrammbereich aus)
- Positionieren Sie das Diagramm auf dem Erstellungsbereich neu
- Setzen Sie das Diagramm auf die Standardsicht zurück
- Zoomoptionen: Vergrößern oder verkleinern Sie das Diagramm

Auswahl und Hervorhebung

Wird in den Alert- und Entitätsdiagrammen per linkem Mausklick ein Knoten ausgewählt, werden die zugehörigen Attribute und Entitäten hervorgehoben. Das Aus-

sehen des ausgewählten Knotens ändert sich. Ein blaues Auswahlrechteck wird nun auf dem Knoten angezeigt. Der innere Teil der hervorgehobenen Knoten wird jetzt blau angezeigt.

Tabelle 33. Beschreibung der Kontextmenüoptionen des Diagrammtools

Ausgewählter Knotentyp	Diagrammtyp	Hervorgehobene Daten
Attribut	Alertdiagramm Entitätsdiagramm	Alle Entitäten, die dieses Attribut gemeinsam nutzen Alle zugehörigen Attribute
Entität	Alertdiagramm Entitätsdiagramm	Alle Entitäten, die mit der ausgewählten Entität in einer Beziehung ersten Grades stehen Die Attribute, die die Beziehung ersten Grades verursachen
Entität	Diagramm für soziale Netze	Alle Vorkommen der ausgewählten Entität in allen Hubs, mit denen sie in Beziehung steht. (Eine Entität kann bei diesem Diagrammtyp in verschiedenen Hubs mehrmals angezeigt werden.)

Sie können mehrere Knoten auswählen, indem Sie die Taste **Strg** drücken. Sie können auch zurzeit ausgewählte Knoten verschieben, indem Sie sie auf das Diagramm ziehen und dort übergeben.

Kontextmenüoptionen

Wählen Sie eine Entität oder ein Attribut aus, indem Sie den Cursor darauf setzen und mit der rechten Maustaste klicken.

Tabelle 34. Beschreibung der Kontextmenüoptionen des Diagrammtools

Kontextmenüoption...	Aktion...	Alert-dia-gramm	Entitäts-dia-gramm	Dia-gramm für sozia-le Netze
Zoomen	Vergrößert oder verkleinert das Diagramm oder passt den Erstellungsbereich des Diagramms an die Anzeigegröße an.	X	X	X

Tabelle 34. Beschreibung der Kontextmenüoptionen des Diagrammtools (Forts.)

Kontextmenüoption...	Aktion...	Alert-diagramm	Entitäts-diagramm	Diagramm für soziale Netze
Schnellfilter (allgemein)	Hilft Ihnen, den Fokus auf interessante Diagrammdaten zu setzen, indem die weniger relevanten Daten vorübergehend ausgeblendet werden. Schnellfilter fügen dem Diagramm weder Daten hinzu noch entfernen sie Daten. Wird ein Schnellfilter aktiviert, wird die Diagrammtitelleiste angezeigt [Schnellfilter eingeschaltet]. Es kann jeweils nur ein Schnellfilter aktiv sein. Sie können jedoch einen anderen Schnellfilter auswählen, wenn die Schnellfilterung aktiv ist. **Anmerkung:** Ist ein Schnellfilter aktiv, zeigt der Filter nur die Diagrammdaten an, die für die zurzeit ausgewählte Entität oder das zurzeit ausgewählte Attribut gelten. Wenn Sie beispielsweise Entität ABC auswählen und den Schnellfilter **Nur zusammengehörige Entitäten anzeigen** wählen, erhalten Sie die zurzeit im Diagramm angezeigten Entitäten, die eine Beziehung ersten Grades mit ABC aufweisen.	X	X	
Schnellfilter - Nur Attribute anzeigen	Blendet Entitäten aus, damit Ihnen nur die der Entität zugeordneten Attribute angezeigt werden, die Sie mit der rechten Maustaste angeklickt haben.	X	X	

Tabelle 34. Beschreibung der Kontextmenüoptionen des Diagrammtools (Forts.)

Kontextmenüoption...	Aktion...	Alert-diagramm	Entitäts-diagramm	Diagramm für soziale Netze
Schnellfilter - Nur zusammengehörige Entitäten anzeigen	Blendet alle Attribute aus, einschließlich derer, die die Entitäten mit einer anderen Entität verknüpfen. Dadurch können Sie die Entitäten sehen, die mit der von Ihnen mit der rechten Maustaste angeklickten Entität eine Beziehung ersten Grades aufweisen. Dieser Schnellfilter bietet Ihnen die Darstellung eines Diagramms für soziale Netze über ein Alert- oder Entitätsdiagramm.	X	X	
Schnellfilter - Nur zusammengehörige Attribute und Entitäten anzeigen	Blendet alle Diagrammdaten aus, mit Ausnahme der zu Entitäten gehörigen Daten, die eine Beziehung ersten Grades mit der von Ihnen mit der rechten Maustaste angeklickten Entität aufweisen sowie der Attribute, die diese Beziehung ersten Grades verursachen. Dieser Schnellfilter ist insbesondere dann hilfreich, wenn das Diagramm viele Daten enthält und Sie die für Sie irrelevanten Daten entfernen wollen.	X	X	

Tabelle 34. Beschreibung der Kontextmenüoptionen des Diagrammtools (Forts.)

Kontextmenüoption...	Aktion...	Alert-diagramm	Entitäts-diagramm	Diagramm für soziale Netze
Schnellfilter - Pfad nach oben anzeigen	Filtert die Diagrammdaten, um den Pfad anzuzeigen, der die Entität oder das Attribut mit der obersten Entität verknüpft. Wenn Sie ein Attribut mit der rechten Maustaste angeklickt haben, berücksichtigt der Filter alle Entitäten und Attribute im Beziehungspfad bis zur obersten Entität. Wenn Sie eine Entität mit der rechten Maustaste angeklickt haben, berücksichtigt der Filter alle Attribute und Entitäten im Pfad bis zur obersten Entität.	X	X	
Schnellfilter - Schnellfilterung inaktivieren	Schaltet den aktuellen Schnellfilter aus und zeigt erneut die aus dem Diagramm gefilterten Daten an.	X	X	
Nach oben	Verschiebt die ausgewählte Entität im Diagramm nach oben, wodurch die Entität zur obersten Entität wird. Diese Option fügt dem Diagramm oder dem Attributexplorer keine neuen Daten hinzu. Das Diagramm wird jedoch erneut gezeichnet, damit die Daten aus der Perspektive der neuen obersten Entität angezeigt werden.	X	X	

Tabelle 34. Beschreibung der Kontextmenüoptionen des Diagrammtools (Forts.)

Kontextmenüoption...	Aktion...	Alert-diagramm	Entitäts-diagramm	Diagramm für soziale Netze
Verbleibende Attribute anzeigen	Zeigt alle Attribute an, die der von Ihnen mit der rechten Maustaste angeklickten Entität zugeordnet sind, auch wenn diese Attribute die Entität nicht mit einer anderen Entität im Diagramm verknüpfen. Der Attributexplorer listet immer alle einer Entität zugeordneten Attribute auf, d. h., diese Option ändert keine Daten im Attributexplorer. Über die Anzeige weiterer Attribute für eine Entität können Sie weitere Informationen abrufen oder Sie können eine Entität oder ein Attribut näher untersuchen.	X	X	
Verbleibende Attribute ausblenden	Entfernt die Attribute aus dem Diagramm, die keine im Diagramm angezeigten Entitäten verknüpfen. Wenn alle im Diagramm angezeigten Attribute Entitäten verknüpfen, die zurzeit im Diagramm angezeigt werden, ist diese Option nicht verfügbar.	X	X	
Verbleibende zusammengehörige Entitäten anzeigen	Es werden alle bisher noch nicht angezeigten Beziehungen für die von Ihnen mit der rechten Maustaste angeklickten Entität angezeigt. Außerdem werden auch die Attribute angezeigt, die die Beziehungen verursachen.	X	X	X
Neues Diagramm erstellen	Erstellt ein neues Diagramm mit dem von Ihnen ausgewählten Typ, in dem die Entität, die Sie mit der rechten Maustaste angeklickt haben, als Hauptentität gilt.	X	X	X

Tabelle 34. Beschreibung der Kontextmenüoptionen des Diagrammtools (Forts.)

Kontextmenüoption...	Aktion...	Alert-diagramm	Entitäts-diagramm	Diagramm für soziale Netze
Diagrammlayout	Steuert die Anzeige des Diagrammlayouts: • Geschichtet: Zeigt die Diagrammdaten in Schichten an, wobei abwechselnd Attributzeilen und die mit diesen Attributen verknüpften Entitäten angezeigt werden. Dieses Layout stellt das Standardlayout für die Alert- und Entitätsdiagramme dar. • Radial: Zeigt die Diagrammdaten als Knoten und Verbindungslinien an, die im Erstellungsbereich des Diagramms zufällig verteilt sind. Dieses Layout kann hilfreich sein, wenn Sie die Entitäten und Attribute selbst anordnen wollen.	X	X	

Tabelle 34. Beschreibung der Kontextmenüoptionen des Diagrammtools (Forts.)

Kontextmenüoption...	Aktion...	Alert-diagramm	Entitäts-diagramm	Diagramm für soziale Netze
Zusammenfassung anzeigen	Zeigt die Entitätszusammenfassung in einem neuen Fenster an, wenn die Verknüpfung in der Datei `graph.properties` konfiguriert ist. Die Entitätszusammenfassung bietet detaillierte Informationen zur ausgewählten Entität, einschließlich aller Alerts, an denen die Entität beteiligt ist, sowie aller der Entität zugeordneten Identitäten. Die Zusammenfassung ist insbesondere dann ein hilfreiches Analysetool, wenn sie mit den Diagrammen des Diagrammtools verwendet wird. Diese Kontextmenüoption ist nur verfügbar, wenn die Entitätszusammenfassungs-URL in der Datei `graph.properties` konfiguriert ist. Wenn Ihre Organisation beispielsweise Analyst Toolkit installiert hat, kann Ihr Identity Insight-Systemadministrator die Verknüpfung so konfigurieren, dass die Cognos-basierte Entitätszusammenfassung in einem neuen Web-Browserfenster angezeigt wird. Wenn Ihnen diese Verknüpfung nicht angezeigt wird, setzen Sie sich mit Ihrem Identity Insight-Systemadministrator in Verbindung.	X	X	X

Einheitliche Elemente in Diagrammen des Diagrammtools

Diagramme enthalten viele einheitliche Elemente: Symbole, Anzeiger und die Linienstärke. Diese einheitlichen Elemente bieten zusätzliche Informationen, anhand

derer Sie ein umfassenderes Verständnis jedes Diagramms erhalten und die für Sie interessanten Bereiche leichter finden können.

Entitätssymbole

Jeder Entitätsknoten wird als ein mit einem festen Kreis umgebenes Symbol angezeigt.

Entitäten können als Personen, Orte oder Dinge (wie Organisationen, Schiffe oder Flugzeuge) definiert werden. Entitäten sind in der Regel jedoch Personen. Der häufigste Entitätsknoten wird als Personensymbol angezeigt: männlich, weiblich oder unbekannt. Das vom Symbol angezeigte Geschlecht basiert auf einer der zwei möglichen Geschlechtszuweisungen:

- Dem während der Namensanalyse der Entitätsauflösung zugeordneten Geschlecht
- Dem Wert des Attributs GENDER, das Bestandteil der Daten für den eingehenden Identitätsdatensatz ist

Ist das Geschlecht nicht eindeutig, wird ein generisches Personenentitätssymbol angezeigt.

Die folgende Tabelle zeigt die Standardsymbole für Personenentitäten, die in den Diagrammen des Diagrammtools verwendet werden.

Tabelle 35. Beispiel der in den Diagrammen des Diagrammtools verwendeten Standardentitätssymbole

Symbol	Darstellung des folgenden Entitätstyps
 Symbol für die weibliche Entität (Person) im Diagrammtool	Weibliche Entität (Person)
 Symbol für die männliche Entität (Person) im Diagrammtool	Männliche Entität (Person)
 Symbol für die Entität (Person) mit unbekanntem Geschlecht im Diagrammtool	Entität unbekannten Geschlechts

Die Hauptentität eines Entitätsdiagramms oder eines Diagramms für soziale Netze weist stets einen dickeren Kreis auf. Ungeachtet der Position, an der die Hauptentität im Diagramm angezeigt wird, können Sie sie stets aufgrund des dickeren Kreises erkennen.

In einem Alertdiagramm weisen alle Entitäten im Alertpfad einen dickeren Kreis auf. Ungeachtet dessen, wie viele Entitäten im Diagramm angezeigt werden, beispielsweise wenn Sie die verbleibenden zusammengehörigen Entitäten anzeigen wollen, können Sie die am Alert beteiligten Entitäten immer erkennen.

Attributsymbole

Attributknoten werden in den Diagrammen des Diagrammtools in Form von Symbolen dargestellt. Jedes Symbol stellt einen bestimmten Attributtyp dar. Die folgende Tabelle enthält ein Beispiel der in den Diagrammen des Diagrammtools angezeigten Standardattributsymbole.

Tabelle 36. Beispiel der im Diagrammtool angezeigten Standardsymbole

Symbol	Darstellung des folgenden Attributtyps
 Symbol für das Adressattribut im Diagrammtool	Adresse
 Symbol für das Namensattribut im Diagrammtool	Name
 Symbol für das Sozialversicherungsnummernattribut im Diagrammtool	Sozialversicherungsnummer
 Symbol für das Geburtsdatumsattribut im Diagrammtool	Geburtsdatum
 Symbol für andere Attributtypen im Diagrammtool	Anderes Attribut (keinem vorhandenen Attributsymbol zugeordnet)

Sie können die Symbole anpassen, die Attribute in den Diagrammen darstellen. Ersetzen Sie dazu das Standardattributsymbol oder fügen Sie Symbole hinzu, die unternehmensspezifische Attribute darstellen sollen. Weitere Informationen finden Sie in „Hinzufügen benutzerdefinierter Symbole zu den Diagrammen des Diagrammtools” auf Seite 372.

Alertanzeiger

Für jede Entität wird ein Anzeiger angezeigt, der die Anzahl Alerts für die Entität angibt. Der Alertanzeiger wird in der linken oberen Ecke des festen Kreises angezeigt, der das Entitätssymbol umgibt.

Der Alertanzeiger weist einen goldfarbenen Hintergrund auf und die Zahl der Alerts wird als schwarzer Text angezeigt. Der Alertanzeiger  auf einem Entitätssymbol gibt beispielsweise an, dass diese Entität 25 Alerts aufweist.

Anzeiger für zusammengehörige Entitäten

Entitätsknoten können auch einen Anzeiger haben, der basierend auf den gemeinsam genutzten Attributen die Anzahl der zu dieser Entität gehörenden Beziehungen angibt. Diese Beziehungen werden noch nicht als zu dieser Entität gehörend angezeigt.

Der Anzeiger für zusammengehörige Entitäten weist einen hellblauen Hintergrund auf und die Zahl der Beziehungen wird als fettgedruckter schwarzer Text angezeigt. Der Anzeiger  für zusammengehörige Entitäten gibt beispielsweise an, dass sechs zusätzliche Entitäten noch nicht mit ihrer Beziehung zur Entität angezeigt werden.

Der Anzeiger für zusammengehörige Entitäten weist je nach Diagrammtyp ein unterschiedliches Verhalten auf:

- Verhalten im Alertdiagramm: Für beide am Alert beteiligten Entitäten wird ein Anzeiger für zusammengehörige Entitäten angezeigt, wenn die Entität mit mehreren anderen Entitäten in Beziehung steht, die zurzeit nicht im Diagramm angezeigt werden. Sie können das Diagramm erweitern, um alle zusammengehörigen Entitäten für jede im Diagramm angezeigte Entität anzuzeigen. In diesem Fall wird auf den Entitäten kein Anzeiger für zusammengehörige Entitäten mehr angezeigt.
- Verhalten im Entitätsdiagramm:
  - Die Hauptentität weist keinen Anzeiger für zusammengehörige Entitäten auf. Im Diagramm werden automatisch alle Entitäten angezeigt, die mit dieser Hauptentität in Beziehung stehen.
  - Für die anderen Entitäten im Entitätsdiagramm wird ein Anzeiger für zusammengehörige Entitäten angezeigt, wenn diese mit anderen Entitäten in Beziehung stehen, die noch nicht im Diagramm angezeigt werden. Sie können über das Kontextmenü die verbleibenden Entitäten für solch eine Entität anzeigen, wodurch der Anzeiger für zusammengehörige Entitäten von der Anzeige entfernt wird.
  - Sie können das Diagramm wie das Alertdiagramm erweitern, damit alle im Diagramm angezeigten zusammengehörigen Entitäten dargestellt werden. In diesem Fall weist keine Entität einen Anzeiger für zusammengehörige Entitäten auf.
- Verhalten im Diagramm für soziale Netze:
  - Die Hubentität (in der Mitte des Clusters) weist keinen Anzeiger für zusammengehörige Entitäten auf, da im Diagramm alle in der Clusterformation zusammengehörigen Entitäten automatisch angezeigt werden.
  - Entitäten, die nicht die Hubentität eines Beziehungsclusters darstellen, weisen möglicherweise einen Anzeiger für zusammengehörige Entitäten auf, wenn diese in Beziehung mit anderen Entitäten stehen, die noch nicht mit dem angegebenen Knoten verknüpft sind.
  - Wenn Sie das Diagramm erweitern, um mehrere Beziehungscluster einzubeziehen, kann eine Entität auch mehrmals auf dem Diagramm angezeigt werden. Ist die Entität der Hub eines Clusters, wird kein Anzeiger für zusam-

mengehörige Entitäten angezeigt. Ist diese Entität jedoch Bestandteil eines Beziehungsclusters und nicht die Hubentität und liegen zusätzliche zusammengehörige Entitäten für diese Entität vor, die noch nicht im Diagramm angezeigt werden, dann wird der Anzeiger für zusammengehörige Entitäten angezeigt. Aus diesem Grund werden immer bestimmte Anzeiger für zusammengehörige Entitäten im Diagramm angezeigt.

Linienanzeiger

Die Linien, die Entitätsknoten umgeben und Entitäten mit Attributen verbinden, können zusätzliche Informationen bereitstellen:

- Gestrichelte Linien, die Attribute verbinden, geben eine enge Attributübereinstimmung an.
- Eine dicke Linie, die einen Entitätsknoten umgibt, zeigt die Hauptentität an – die beim Erstellen dieses Diagramms ausgewählte oder angeforderte Entität.

URL-Syntax und Parameter des Diagrammtools

Sie müssen eine Verknüpfung zur entsprechenden URL vornehmen, um Zugriff auf ein Diagramm des Diagrammtools zu haben. Die URL kann in eine vorhandene kundenspezifische Anwendung eingebettet sein (beispielsweise eine Webstartseite, ein Dashboard oder ein Fallverwaltungstool) oder manuell in einen Web-Browser eingegeben werden.

Die korrekte URL-Syntax und die Parameter für die Diagramme der Diagrammkomponente sieht wie folgt aus:

`http://`*`server`*`:`*`port`*`/graphs/run/`*`grafiktyp`*`.jsp?height=`*`nnnn`*`&width=`*`yyyy`*`&`*`kennung=xxxx`*

server*:*port
: Gibt den Namen des Produktanwendungsservers und die Portnummer an, auf denen sich IBM InfoSphere Identity Insight befindet. Der Produktanwendungsserver ist in der Regel der WebSphere-Server.

  Die Portnummer ist standardmäßig auf 13510 gesetzt.

/graphs/run
: Verweist auf die Produktverzeichnisse, in denen sich die Diagrammtooldateien befinden. Das Produktinstallationsprogramm installiert das Diagrammtool standardmäßig in den `/graphs/run`-Verzeichnissen.

***grafiktyp*.jsp**
: Gibt an, welches Diagramm erstellt werden soll:
  - Geben Sie `role-alert.jsp` ein, wenn ein Alertdiagramm erstellt werden soll.
  - Geben Sie `entity.jsp` ein, wenn ein Entitätsdiagramm erstellt werden soll.
  - Geben Sie `social-network.jsp` ein, wenn ein Diagramm für soziale Netze erstellt werden soll.

?
: Gibt ein URL-Element an.

height=*nnnn*
: Gibt die Höhe des Erstellungsbereichs des Diagramms an. Das ist die Höhe, mit der der Erstellungsbereich des Diagramms im Web-Browserfenster wiedergegeben werden soll. Geben Sie die Pixelzahl ein.

  Die Diagrammhöhe wird auf folgende Art festgelegt:
  - Ist in der URL eine Höhe angegeben, ist dies die Standarddiagrammhöhe.

- Ist in der Eigenschaft **defaultGraphHeight** der Datei graph.properties ein Wert festgelegt, ist dies die Standarddiagrammhöhe.
- Wenn in der URL oder in der Eigenschaft **defaultGraphHeight** keine Diagrammhöhe angegeben ist, werden 800 Pixel als Standarddiagrammhöhe festgelegt.

.

Legen Sie eine Höhe von 450 Pixel fest, um sich dem Erstellungsbereich eines Diagramms zu nähern, der in ein Web-Browserstandardfenster von 1024 x 768 eingefügt werden kann.

? Gibt ein URL-Trennzeichentoken zwischen Parametern an.

width=*yyyy*
Gibt die Breite des Erstellungsbereichs des Diagramms an. Das ist die Breite, mit der der Erstellungsbereich des Diagramms im Web-Browserfenster wiedergegeben werden soll. Der Attributexplorer wird bei dieser Angabe nicht berücksichtigt, da er als separate Komponente gilt, die rechts vom Erstellungsbereich des Diagramms im Web-Browserfenster angedockt ist.

Die Diagrammbreite wird auf folgende Art festgelegt:

- Ist in der URL eine Breite angegeben, ist dies die Standarddiagrammbreite.
- Ist in der Eigenschaft **defaultGraphWidth** der Datei graph.properties ein Wert festgelegt, ist dies die Standarddiagrammbreite.
- Wenn in der URL oder in der Eigenschaft **defaultGraphHeight** keine Diagrammbreite angegeben ist, werden 800 Pixel als Standarddiagrammbreite festgelegt.

.

Legen Sie eine Höhe von 640 Pixel fest, damit der Erstellungsbereich eines Diagramms annähernd so groß ist, dass er in einem Web-Browserstandardfenster mit einer Auflösung von 1024 x 768 angezeigt werden kann.

ID=xxxx
Gibt den ID-Typ (Entität oder Alert) und die Nummer für diese Entität oder diesen Alert an. Wenn Sie die Entitäts-ID verwenden, ist der Wert der ID die Hauptentität im Entitätsdiagramm oder die Hubentität im Diagramm für soziale Netze. Wenn Sie die Alert-ID verwenden, entspricht der Wert dem im Alertdiagramm anzuzeigenden Alert.

- Geben Sie alertID=*bestimmte_alert-id* ein, wenn Sie ein Alertdiagramm verwenden.
- Geben Sie entityID=*bestimmte_entitäts-id* ein, wenn Sie ein Entitätsdiagramm oder ein Diagramm für soziale Netze verwenden.

Allgemeine Verwaltungstasks für das Diagrammtool

Einige Tasks für das Diagrammtool können nur von einem Benutzer mit Administratorberechtigung ausgeführt werden.

Hinzufügen benutzerdefinierter Symbole zu den Diagrammen des Diagrammtools:

Das Diagrammtool enthält Standardsymbole, die die verschiedenen in den Diagrammen angezeigten Attributtypen darstellen. Sie können das Standardsymbol für ein oder mehrere Attribute ändern oder Symbole für angepasste Attribute hinzufügen, die in Ihrem Produkt konfiguriert sind. Alle Diagramme des Diagrammtools

verwenden dieselbe Gruppe von Bildsymbolen auf dem Produktanwendungsserver. Wenn Sie also die Attributsymbolgruppe anpassen, werden allen Benutzern dieselben Attributsymbole angezeigt.

Vorbereitende Schritte

Diagrammsymbole sind zunächst SVG-Dateien (Scalable Vector Graphic). SVG-Dateien können mithilfe verschiedener vektorbasierter Tools erstellt werden oder sie können aus verschiedenen Quellen im Internet heruntergeladen werden. Es wird dringend empfohlen, die Größe der für Symbole verwendeten SVG-Dateien möglichst klein zu halten, um die Lesbarkeit beim Skalieren der Bilder zu verbessern.

Für das Diagramm ist eine im JSON-Format (JSON - Javascript Object Notation) gespeicherte Formdefinition erforderlich. Zum Konvertieren vom SVG- in das JSON-Format müssen die beiden separat verfügbaren Befehlsdienstprogramme **xlstproc** und **sed** verwendet werden.

Auf einem UNIX-basierten Computer sind diese Tools möglicherweise bereits vorhanden. Auf einem Windows-basierten Computer müssen Sie diese UNIX-basierten Tools über einen UNIX-Emulator (wie die kostenlose Cygwin-Anwendung) beziehen. *Anmerkung: Falls Sie Cygwin verwenden, stellen Sie sicher, dass Sie die Bibliotheken 'libxml2' und 'libxslt' in Ihre Installation einschließen, damit Sie die erforderlichen Dienstprogramme erhalten.*

Abschließend benötigen Sie noch die Datei svg2gfx.xsl aus der kostenlosen Dojo-Bibliothek (verfügbar unter https://dojotoolkit.org/download). Nachdem Sie DOJO heruntergeladen haben, finden Sie die Datei svg2gfx.xsl im Verzeichnis <installationsstammverzeichnis>/dojox/gfx/resources.

Vorgehensweise

1. Kopieren Sie die Datei svg2gfx.xsl aus der DOJO-Speicherposition in das Verzeichnis, das auch die SVG-Datei(en) enthält, die Sie konvertieren wollen.
2. Öffnen Sie ein UNIX-Terminalfenster/Befehlszeilenfenster und navigieren Sie zum Verzeichnis mit der bzw. den SVG-Datei(en).
3. Führen Sie den folgenden Befehl aus: `xsltproc ./svg2gfx.xsl <ihre svg-datei> > <temporärer_dateiname>.json`
4. Führen Sie den folgenden Befehl aus: `sed -e 's/,}/}/g' -e 's/,]/]/g' <temporärer_dateiname.json> > <endgültiger_name>.json`
5. Navigieren Sie zu Ihrem Identity Insight-Installationsordner.
6. Navigieren Sie im Installationsordner zu /ibm-home/graphs.
7. Erstellen Sie einen Ordner mit dem Namen customImages (unter Beachtung der Groß-/Kleinschreibung).
8. Verschieben Sie das benutzerdefinierte Symbol (die JSON-Datei) in den Ordner 'customImages'.

Beispiel

Wenn Sie einen Attributtyp mit dem Namen `FLIGHT` erstellt haben und wollen, dass dieser Attributtyp in den Diagrammen des Diagrammtools durch ein benutzerdefiniertes Diagrammsymbol dargestellt wird, führen Sie die folgenden Schritte aus:

1. Erstellen Sie für die Darstellung des Attributtyps `FLIGHT` eine geeignete Bilddatei oder stellen Sie eine entsprechende Bilddatei bereit. Stellen Sie sicher, dass

der Name der Bilddatei dem Namen des in der Konfigurationskonsole konfigurierten Attributtyps entspricht und nur Kleinbuchstaben enthält wie zum Beispiel der Dateiname `flight.svg`.

2. Stellen Sie sicher, dass sich die Datei svg2gfx.xsl im selben Verzeichnis wie die Datei `flight.svg` befindet.
3. Öffnen Sie ein UNIX-Terminalfenster/Befehlszeilenfenster und navigieren Sie zum Verzeichnis mit der Datei `flight.svg`.
4. Führen Sie den folgenden Befehl aus: `xsltproc ./svg2gfx.xsl flight.svg > flight_tmp.json`
5. Führen Sie den folgenden Befehl aus: `sed -e 's/,}/}/g' -e 's/,]/]/g' flight_tmp.json > flight.json`
6. Kopieren Sie die Symboldatei `flight.json` in den Ordner `/customImages`.

Anforderungen an benutzerdefinierte Diagrammsymbole:

Sie können die in den Diagrammen angezeigten Attributsymbole anpassen. Die neuen Symbole müssen jedoch die Anforderungen an benutzerdefinierte Diagrammsymbole erfüllen, damit die Diagramme die Symbole erkennen und anzeigen können.

Anforderungen an benutzerdefinierte Symbole

Die Attributsymbole müssen die folgenden Anforderungen erfüllen, damit Produktdiagramme die benutzerdefinierten Symbole erkennen und anzeigen können:

- Dateiformat: Scalable Vector Graphics (SVG)
- Name:
  - Der Name eines benutzerdefinierten Symbols muss dem Namen des entsprechenden in der Konfigurationskonsole konfigurierten Attributtyps entsprechen.
  - Der Name eines benutzerdefinierten Symbols darf nur Kleinbuchstaben enthalten.
- Die SVG-Datei muss in eine JSON-Formdefinition konvertiert werden (siehe „Hinzufügen benutzerdefinierter Symbole zu den Diagrammen des Diagrammtools" auf Seite 372).

Wenn Sie beispielsweise ein Attributsymbol mit dem Attributtyp FINGERPRINTS zuordnen wollen, das in der Konfigurationskonsole konfiguriert ist, muss `fingerprints.svg` als Name für die Symboldatei gewählt werden.

Beispiele für Namen

Zum Überschreiben eines vorhandenen Basistypsymbols muss das benutzerdefinierte Symbol einen der folgenden Namen (in Kleinbuchstaben) erhalten:

- address.json
- female.json
- male.json
- name.json
- undetermined_gender.json

Für Entitätsnummern muss der Name der JSON-Symboldatei dem Nummerntypcode (NUM_TYPE.NUM_TYPE in der Datenbank) entsprechen. Beispiel:

- cc.json

- dl.json
- ff.json
- ssn.json
- pp.json
- ph.json

Für Entitätsmerkmale muss der Name der JSON-Symboldatei dem Attributtypcode (ATTR_TYPE.ATTR_TYPE in der Datenbank) entsprechen. Beispiel:

- dob.json
- died.json
- marital.json
- circa_dob.json
- pop.json
- nat.json
- cit.json

Herstellen einer Verknüpfung mit der Entitätszusammenfassung aus dem Diagrammtool:

Die Entitätszusammenfassung bietet detaillierte Informationen zu einzelnen Entitäten und ist beim Analysieren von Alert- und Entitätsbeziehungen hilfreich. Wenn Sie die URL-Eigenschaften auf die Webanwendung setzen, von der die Entitätszusammenfassung generiert wird, können Diagrammtoolbenutzer die Entitätszusammenfassung in einem der Diagramme des Diagrammtools öffnen.

Informationen zu diesem Vorgang

Das Herstellen der Verknüpfung ist eine globale Task. Nach dem Herstellen der Verknüpfung haben alle Benutzer, die Diagramme des Diagrammtools anzeigen, über das Kontextmenü Zugriff auf die Verknüpfung. Sind die Verknüpfungseigenschaften nicht gesetzt, wird die Kontextmenüoption **Zusammenfassung anzeigen** nicht angezeigt.

Vorgehensweise

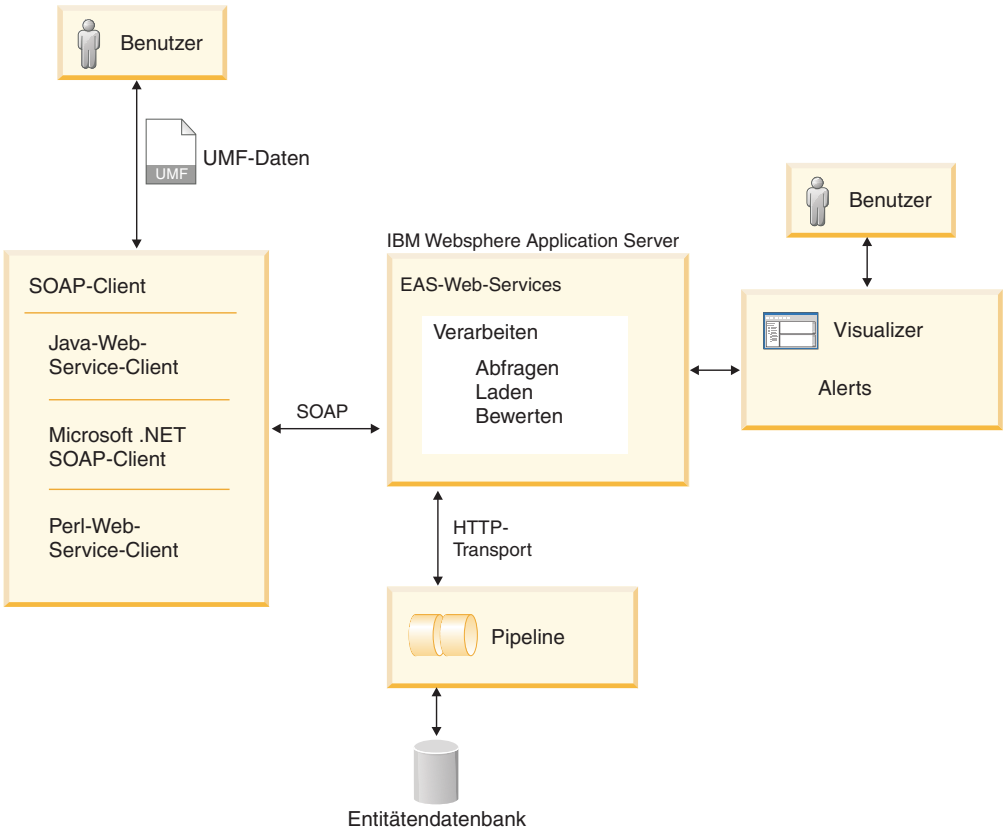
1. Bitten Sie Ihren Systemadministrator, die Eigenschaft RESUMESERVER der Tabelle COMPONENT_CONFIG mit einer Verknüpfung zum Cognos-Toolkitbericht zu aktualisieren.
   a. Ersetzen Sie den Wert dieser Eigenschaft durch die tatsächliche URL. Geben Sie den Host-Server, den Portnamen und den Pfad der Webanwendung an. Anhand des Beispielwerts können Sie sich ein Bild vom Aussehen des Pfads machen. Wenn Ihre Organisation beispielsweise das Cognos-basierte Programm Analyst Toolkit installiert hat und verwendet, geben Sie den Pfad zur von Analyst Toolkit generierten Entitätszusammenfassung an.
   b. Stellen Sie sicher, dass das Token **%ISIIEntityID%** innerhalb des Parameterwerts liegt. Dieser Parameter sendet die entsprechende Entitäts-ID an die Webanwendung, um die korrekte Entitätszusammenfassung zu generieren.
2. Optional: Testen Sie die Verknüpfung.

Kapitel 9. Entwickeln

Wenn in Ihrer Umgebung der Einsatz von Web-Services erforderlich ist, stellt IBM InfoSphere Identity Insight einen einfachen XML-basierten Web-Service bereit.

Web-Services

IBM InfoSphere Identity Insight stellt eine Gruppe von Web-Services bereit, mit denen Sie externe Anwendungen erstellen können, die UMF-Daten (Universal Message Format) für Pipelineverarbeitung oder Suchen nach Entitäten in die Entitätendatenbank laden können. Sie können die bidirektionale Transportmethode HTTP (Hypertext Transfer Protocol) verwenden, die eine Standardfunktion in der Pipeline ist.



IBM InfoSphere Identity Insight-Web-Services verwenden vier SOAP-Methoden (Simple Object Access Protocol): Verarbeiten, Suchen, Laden und Bewerten. Das Produkt unterstützt SOAP Version 1.1.

Das Produkt wird mit mehreren Komponenten ausgeliefert, die Sie in die Verwendung von Web-Services einführen.

srd.wsdl
: Diese Datei enthält eine Definition der Web-Service-Beschreibungssprache für die Produkt-Web-Services. Sie können diese Datei mit allen SOAP-Toolkits oder -Technologien verwenden, um die Web-Services zu starten. Sie ru-

fen diese Datei auf, indem Sie WebSphere Liberty starten und die Datei http://hostname:port/easws/resources/wsdl/srd.wsdl laden.

wsutil.jar
Diese Datei ist ein Web-Service-Testclient, der für das Testen Ihrer Web-Service-Installation und -Konfiguration bereitgestellt wird. Dieses Dienstprogramm finden Sie im Verzeichnis `ibm-home/easws`.

Softwarevoraussetzungen für Web-Services

Für IBM InfoSphere Identity Insight-Web-Services muss eine bestimmte Software installiert und aktiv sein.

Bevor Sie Web-Services verwenden, müssen Sie sicherstellen, dass die folgende Software installiert und aktiv ist:

- IBM InfoSphere Identity Insight-Web-Services müssen installiert und aktiv sein.
- Die eingebettete Komponente IBM WebSphere Application Server muss auf dem System aktiv sein, auf dem die IBM InfoSphere Identity Insight-Web-Services bereitgestellt werden. In der Regel handelt es sich dabei um denselben Anwendungsserver, auf dem auch die Konfigurationskonsole und Visualizer installiert sind.
- Eine Web-Service-Pipeline muss gestartet und an der entsprechenden HTTP-URL empfangsbereit sein. Der Anwendungsserver versucht, über die angegebene HTTP-URL UMF-Daten an diese Web-Service-Pipeline zu senden, sobald er eine SOAP-Anforderung empfängt.

  Anmerkung: Die HTTP-URL, die für die Kommunikation zwischen dem Anwendungsserver und der Pipeline verwendet wird, ist *nicht* mit der URL identisch, die von Web-Service-Clients zum Senden von SOAP-Anforderungen verwendet wird. Wenn SOAP-Anforderungen direkt an die HTTP-URL der Web-Service-Pipeline gesendet werden, verursacht dies einen Fehler.

  Wenn WebSphere Application Server beispielsweise mit dem Standardportbereich konfiguriert ist, sind die Portnummern und die Belegung wie folgt:
  - *nnn*0 - HTTP-Port für Web-Server
  - *nnn*1 - HTTPS-Port für Web-Server
  - *nnn*2 - HTTP-Verwaltungsport
  - *nnn*3 - HTTPS-Verwaltungsport
  - *nnn*4 - SOAP-Port
  - *nnn*5 - Anwendungsserverport
- Die Datei webservices.properties muss mit der HTTP-URL der aktiven Pipeline konfiguriert werden, damit die integrierte WebSphere Application Server-Instanz weiß, wo sich die Pipeline befindet, die die Web-Service-Anforderungen bearbeitet. Diese Datei befindet sich normalerweise im folgenden Verzeichnis: *produktausgangsverzeichnis*`/srd-home/easws`
- Ein SOAP- und WSDL-kompatibler Web-Service-Client zum Aufrufen der IBM InfoSphere Identity Insight-Web-Services muss vorhanden sein. Ein Beispielclient, wsutil.jar, wird zum Testen vorhergehender Release-Services mit IBM InfoSphere Identity Insight-Web-Services installiert, gilt jedoch nicht für die erweiterten Services für Version 8.0 Fixpack 2.

Starten der Web-Service-Pipelines

Starten Sie die Pipelines unter Verwendung des bidirektionalen HTTP-Transports, um Daten zu senden und zu verarbeiten, die über einen Web-Service gesendet

wurden. In der Regel bleiben Pipelines, die mit Web-Services verwendet werden, ständig im Hintergrund aktiv und sind an den zugeordneten Ports für zu verarbeitende Daten empfangsbereit. Verwenden Sie die folgenden Schritte, um eine Web-Service-Pipeline zu starten.

Vorbereitende Schritte

- Stellen Sie sicher, dass Sie die Pipeline-URL-Einstellung kennen, die in der Datei `webservices.properties` konfiguriert ist. Diese Einstellung gibt die Web-Service-Komponente an, die auf der integrierten IBM Websphere Application Server-Instanz für die Pipeline ausgeführt wird, und muss mit der URL übereinstimmen, die zum Starten der Web-Service-Pipelines verwendet wurde.
- Für den Pipelineknoten, von dem diese Pipeline gehostet wird, muss die ausführbare Datei für die Pipeline installiert sein.
- Es muss mindestens eine Pipelinekonfigurationsdatei für die Verwendung mit der Pipeline konfiguriert sein, die Sie starten wollen. Sie können die zu verwendende Pipelinekonfigurationsdatei als Teil des Befehls zum Starten der Pipeline angeben. Wenn Sie den Namen der Konfigurationsdatei nicht als Teil des Pipelinebefehls angeben, muss sich die Pipelinekonfigurationsdatei auf dem Pipelineknoten befinden und sie muss den Standardnamen für die Pipelinekonfigurationsdatei, `pipeline.ini`, verwenden.
- Wenn Sie ein Script zum Starten von Pipelines verwenden, müssen Sie sicherstellen, dass sich das Script in demselben Verzeichnis befindet, in dem Sie die Pipeline starten.
- Wenn Sie die Verarbeitungsergebnisse von dieser Pipeline weiterleiten oder die Statistikdaten und den Status dieser Pipeline überwachen wollen, registrieren Sie die Pipeline auf der Registerkarte **Pipelines** der Konfigurationskonsole. Sie müssen einen der bereits registrierten Pipelinenamen verwenden, um diese Pipeline zu starten, damit Überwachungen und Routing erfolgreich ausgeführt werden.
- Wenn Sie mit dem Anwendungsmonitor den Status und die Statistikdaten der Pipeline überwachen, müssen Sie sicherstellen, dass auf dem Pipelineknoten ein SNMP-Agent installiert und aktiv ist, bevor Sie diese Pipeline starten.
- Wenn diese Pipeline ihre Ergebnisse an ein anderes System oder eine andere Datenbank weiterleitet, müssen Sie sicherstellen, dass sich die Routing-Datei für diese Pipeline in demselben Verzeichnis befindet, in dem Sie die Pipeline starten.
- Wenn der Wert des Systemparameters *DEFAULT_CONCURRENCY* auf einen Wert größer-als 1 gesetzt ist oder Sie den Parameter *concurrency* in der Pipelinekonfigurationsdatei für den Pipelineknoten konfiguriert haben, können Sie mit *einem* Befehl zum Starten einer Pipeline mehrere parallel ablaufende Pipelineverarbeitungsthreads starten.

Informationen zu diesem Vorgang

Das Starten einer Pipeline erfolgt in drei Schritten:

Vorgehensweise

1. Stellen Sie sicher, dass zu dieser Zeit auf dem Pipelineknoten keine anderen Pipelines ausgeführt werden, die denselben Namen haben wie die Pipeline, die Sie starten wollen. Jede Pipeline muss auf ihrem Pipelineknoten über einen eindeutigen Namen verfügen. (Der Standardpipelinename ist `pipeline`.) Es gibt zwei Methoden, dies zu prüfen:
   a. Wenn Sie den Anwendungsmonitor verwenden, um den Status von Pipelines zu überprüfen oder um die Ergebnisse an andere Systeme weiterzulei-

ten, sehen Sie sich die Registerkarte **Pipelinestatus** an, um zu prüfen, ob bereits eine Pipeline mit dem Namen ausgeführt wird, den Sie verwenden wollen.

b. Alternativ können Sie auch in einer Eingabeaufforderung den folgenden Befehl eingeben:

```
pipeline -n pipelinename -l
```

Dabei ist *pipelinename* der Name, mit dem Sie die neue Pipeline starten wollen. Stellen Sie sicher, dass dieser Name mit dem Namen übereinstimmt, der in der Konfigurationskonsole für diese Pipeline registriert ist.

2. Starten Sie an einer Eingabeaufforderung eine Pipeline oder mehrere Pipelines, indem Sie die entsprechenden Optionen und Parameter des Befehls 'pipeline' im folgenden Format eingeben:

```
pipeline -option parameter
```

Anmerkung: Wenn Sie den Anwendungsmonitor für diese Pipeline verwenden und sie in der Konfigurationskonsole für die Überwachung oder das Routing registriert wurde, müssen Sie sicherstellen, dass im Befehl zum Starten der Pipeline die Option `-n` und der Name der registrierten Pipeline angegeben werden. Wenn der angegebene Pipelinename nicht genau mit dem Namen der registrierten Pipeline übereinstimmt (einschließlich Groß-/Kleinschreibung), wird der Status der Pipeline auf der Registerkarte **Pipelinestatus** der Konfigurationskonsole nicht korrekt angezeigt und für diese Pipeline ggf. konfigurierte Routing-Operationen werden nicht erfolgreich ausgeführt.

Anmerkung: In der Regel verwenden Sie die Option `-s` oder `-d`, um die Pipeline den Anforderungen entsprechend im Service-/Dämon- oder Debugmodus zu starten.

3. Prüfen Sie, ob der Befehl erfolgreich ausgeführt wurde und ob die Pipeline gestartet wurde und aktiv ist.

a. Wenn Sie den Anwendungsmonitor verwenden und diese Pipeline in der Konfigurationskonsole registriert wurde, prüfen Sie die Registerkarte **Pipelinestatus**. Ist die Pipeline aktiv, wird der Status `Aktiv` angezeigt.

b. Wenn Ihr System auf einer Microsoft Windows-Plattform ausgeführt wird und Sie die Pipelineoption für Services verwenden, können Sie den Status der Pipeline in der Microsoft Windows-Systemsteuerung unter **Dienste** sehen.

c. Wenn Ihr System auf einer UNIX-Plattform ausgeführt wird und Sie die Pipelineoption für Dämonen verwenden, können Sie den folgenden Befehl eingeben, um auf aktive Prozesse zu prüfen:

```
ps -fu benutzer-id
```

Dabei ist *benutzer-id* die Kennung des Benutzers, der die Pipeline startet.

d. Alternativ können Sie auch in einer Eingabeaufforderung den folgenden Befehl eingeben:

```
pipeline -npipelinename -l
```

Dabei ist *pipelinename* der Name der Pipeline, die Sie gerade gestartet haben. Wenn die Pipeline aktiv ist, gibt die Eingabeaufforderung die Information `Aktiv` zurück.

Nächste Schritte

Dieser Pipelinebefehl startet dieselbe Anzahl von Pipelineverarbeitungsthreads wie der Parameter für den gemeinsamen Zugriff in der Pipelinekonfigurationsdatei.

Die Anzahl Datensätze, die gleichzeitig verarbeitet werden, wird vom Parameter für den gemeinsamen Zugriff festgelegt, der in der HTTP-Transportoption angegeben ist.

Testen von Web-Services

Sie können mithilfe des bereitgestellten Testclients, wsutil.jar, die Installation und Konfiguration Ihrer IBM InfoSphere Identity Insight-Web-Services testen.

Vorbereitende Schritte

- Web-Services müssen installiert sein.
- Stellen Sie sicher, dass die WebSphere Application Server-Instanz aktiv ist.
- Der Anwendungsserver sollte mindestens über eine Pipelinekonfigurationsdatei verfügen, die für Web-Service-Pipelines konfiguriert ist.
- Stellen Sie sicher, dass die Datei `webservices.properties` mit der richtigen Pipeline-URL-Einstellung konfiguriert ist. Diese Web-Service-Pipeline muss aktiv sein.
- Erstellen Sie mindestens ein Test-UMF-Eingabedokument, das beim Test verwendet werden soll.

Vorgehensweise

1. Wechseln Sie in der integrierten WebSphere Application Server-Instanz in das Verzeichnis, das die Datei `wsutil.jar` enthält. Diese Datei befindet sich normalerweise in *installationsstammverzeichnis*`/ewas/webservice/wsutil.jar`
2. Geben Sie in einer Befehlszeile von diesem Verzeichnis aus den Befehl wsutil.jar mit der für die Operation erforderlichen Syntac ein: `java -jar wsutil.jar –-<soap-methode>=<uri> --input=<url> –-output=<uri>`

Beispiel für das Testen der Web-Service-Lademethode

Der folgende wsutil.jar-Befehl lädt Datensätze aus einer UMF-Datei namens „raw_entities.umf" und speichert die Ergebnisse in einer UMF-Datei namens „results-.umf":

```
java -jar wsutil.jar --load=http://localhost:13510/easws/services/SRDWebService
--input=raw_entities.umf --output=results.umf
```

Datei 'srd.wsdl'

Sie benötigen einen Web-Service-Client, um mit IBM InfoSphere Identity Insight-Web-Services kommunizieren zu können. Wenn Sie IBM InfoSphere Identity Insight-Web-Services installieren, wird auch die Datei 'srd.wsdl' installiert. Sie enthält die SRDWebService-Methoden, die zur Kommunikation mit InfoSphere Identity Insight-Web-Services verwendet werden. Mit der Datei 'srd.wsdl' können Sie einen Web-Service-Client zur Verwendung mit IBM InfoSphere Identity Insight-Web-Services erstellen.

Sie können auf die Datei 'srd.wsdl' über den Web-Browser zugreifen, indem Sie auf die integrierte WebSphere Application Server-Instanz zugreifen, von der die Web-Services gehostet werden. Diese Datei befindet sich in der Regel auf dem Anwendungsserver an der folgenden Stamm-URL:

`http://`*IBM_WebSphere_Application_Server-host*`:`*installationsport*`/easws/resources/wsdl/srd.wsdl`

Beispiel:

```
http://localhost:13510/easws/resources/wsdl/srd.wsdl
```

Anmerkung: Stellen Sie sicher, dass der Anwendungsserver aktiv ist, bevor Sie versuchen, auf die Datei 'srd.wsdl' zuzugreifen.

Sie können einen Web-Service-WSDL-Client auch mit einer beliebigen Entwicklungsplattform erstellen, die Web-Services mit einem SOAP-Toolkit unterstützt. Beispiele:

- Java mit IBM WebSphere Application Server
- Java mit Apache Axis
- Microsoft .NET
- Perl

Anweisungen zum Erstellen eines Web-Service-Clients mit einer WSDL-Datei finden Sie in der Dokumentation zu Ihrer Entwicklungsplattform.

Wenn Sie eine andere Web-Service-Client-WSDL als den Web-Service-Client 'srd.wsdl' erstellen, stellen Sie sicher, dass die Bereitstellungs-URL ordnungsgemäß auf den WSDL-Client zeigt.

SRDWebService-Methoden

Die Datei srd.wsdl enthält die SRDWebService-Methoden, mit denen die Kommunikation mit den IBM InfoSphere Identity Insight-Web-Services ausgeführt wird. SRDWebService enthält drei Methoden: eine zum Laden von Daten in die Entitätendatenbank, eine für eine Suche, um die Entitätendatenbank abzufragen und eine zur Verarbeitung der gesamten Pipelinefunktionalität, die durch UMF verfügbar ist.

loadRecord-Methode

```
LoadResult loadRecord(String umfEntity)
```

Das von der Methode loadRecord() zurückgegebene Objekt LoadResult enthält zwei Einträge:

Eintrag	Beschreibung	Typ
entityID	Kennung der zurückgegebenen Entität	Langzeichen
merged	Markierung, die anzeigt, ob die Entität in eine vorhandene Entität aufgelöst wurde oder eine neue Entität war	Boolescher Wert

Der Parameter umfEntity ist eine XML-Zeichenfolge in UMF, die die Daten für eine einzelne Entität darstellt. Anweisungen zur ordnungsgemäßen Erstellung eines UMF_ENTITY-Datensatzes finden Sie in der UMF-Spezifikation. Stellen Sie sicher, dass dabei die entsprechenden Werte für DSRC_ACCT und DSRC_REF definiert werden.

Die Lademethode ermöglicht zwar die Verarbeitung von UMF_ENTITY-Dokumenten, sie gibt jedoch nicht das unformatierte UMF-Ausgabedokument als Ergebnis zurück. Stattdessen wird ein Objekt LoadResult zurückgegeben, das die Entitäts-ID und eine Markierung enthält, die anzeigt, ob es sich um eine neue Entität oder um eine Entität handelt, die in eine vorhandene aufgelöst wurde. Sie können die Methode process anstelle der Lademethode verwenden, wenn Sie das Parsing des UMF-Ausgabedoku-

ments selbst ausführen wollen. Bei der Lademethode müssen Sie das Parsing des aus der Ladeoperation resultierenden UMF-Ausgabedokuments nicht selbst ausführen.

basicQuery()-Methode

```
String basicQuery(String umfSearch)
```

Die Eingabezeichenfolge für die Methode basicQuery() muss das Format eines UMF_SEARCH-Datensatzes haben. Die von basicQuery() zurückgegebene XML-Zeichenfolge enthält das UMF-Suchergebnis (UMF-_SEARCH_RESULT) aus der Abfrage.

Es gibt zwei Arten integrierter Abfragen: Zusammenfassungsabfragen und Detailabfragen.

Anmerkung: Diese Methode ist nur aus Gründen der Abwärtskompatibilität vorhanden. In diesem Release ist die Funktionsweise der Methode mit der der Methode process identisch. Verwenden Sie die Methode process anstelle der Methode basicQuery() für alle neuen Clientanwendungen.

Methode process()

```
String process(String umfRequestDocument)
```

Mit der Methode process können Sie alle UMF-Eingabedokumente verarbeiten und ein UMF-Ausgabedokument als Ergebnis erhalten. Die Methode process dient zur Bearbeitung aller Anforderungen und Antworten, die von der Pipeline unterstützt werden, und sollte für alle Operationen bevorzugt verwendet werden.

Diese Methode verfügt über einen Zeichenfolgeparameter (String) und gibt ein Zeichenfolgeergebnis zurück.

wsutil.jar

wsutil.jar ist eine befehlszeilenbasierte Java-Anwendung, die bei der Installation der IBM InfoSphere Identity Insight-Web-Services installiert wird. Hierbei handelt es sich um einen Beispielclient, mit dem Sie jede SOAP-Methode der Web-Services zum Testen der Installation und Konfiguration Ihrer Web-Services ausprobieren können.

Der Testclient wsutil.jar sollte sich an der folgenden Speicherposition befinden:

installationsstammverzeichnis/ewas/webservice

wsutil.jar-Syntax

Wsutil.jar ist eine befehlszeilenbasierte Java-Anwendung, die als Testclient zum Testen Ihrer Installation und Konfiguration der IBM InfoSphere Identity Insight-Web-Services zur Verfügung gestellt wird. Um wsutil.jar zu verwenden, geben Sie einen wsutil.jar-Operator mit den entsprechenden Eingabe- und Ausgabeänderungswerten an.

Die Syntax für die Verwendung von wsutil.jar ist davon abhängig, welche Web-Service-Operation Sie testen wollen:

```
wsutil (unix) oder wsutil.bat (win) --operator=URI --input=URI --output=URI
```

help

Zeigt Onlinehilfe und Befehlszeileninformationen für den wsutil.jar-Testclient an.

```
wsutil (unix) oder wsutil.bat (win) --help
```

load=*URI*
Gibt UMF-Datensätze im Pipelinestil und den URI (Uniform-Resource-Identifier) für die Schnittstelle der IBM InfoSphere Identity Insight-Web-Services an.

```
wsutil (unix) oder wsutil.bat (win) --load=URI [--xslt=URI][--
input=URI][--output=URI]
```

Diese Operation lädt die UMF-Datensätze zur Entitätsauflösungsverarbeitung aus dem angegebenen URI in die Web-Service-Pipelines. Nach der Verarbeitung gibt die Operation die Entitäts-ID und einen Anzeiger zurück, der anzeigt, ob die eingehende Entität mit einer vorhandenen Entität gemischt wurde oder die Erstellung einer neuen Entität verursachte.

process=*URI*
Gibt generische XML- oder UMF-Datensätze und den URI (Uniform Resource Identifier) für die Schnittstelle der IBM InfoSphere Identity Insight-Web-Services an.

```
wsutil (unix) oder wsutil.bat (win) --process=URI [--xslt=URI][--
input=URI][--output=URI]
```

Mit dieser Operation können Sie alle UMF-Eingabedokumente verarbeiten und ein UMF-Ausgabedokument als Ergebnis erhalten. Die Methode process dient zur Bearbeitung aller Anforderungen und Antworten, die von der Pipeline unterstützt werden. Hierbei handelt es sich in der Regel um die bevorzugte Methode für alle Operationen.

search=*URI*
Gibt UMF-Anforderungen und -Antworten im Pipelinesuchstil mit dem URI (Uniform-Resource-Identifier) für die Schnittstelle der IBM InfoSphere Identity Insight-Web-Services an.

```
wsutil (unix) oder wsutil.bat (win) --score=URI [--xslt=URI][--
input=URI][--output=URI]
```

Diese Operation kann eine Suche in der Entitätendatenbank nach einer bestimmten Entität ausführen und angeforderte Informationen zu dieser Entität zurückgeben. Sie kann auch die Entitätendatenbank nach Entitäten abfragen, die einem bestimmten Attribut entsprechen, und die Liste der Entitäten zurückgeben, die der Abfrage entsprechen.

xslt=*URI*
Gibt die XSLT-Umwandlung und die XML-Datei an, die die Operation in UMF-Datensätze umwandelt.

```
wsutil (unix) oder wsutil.bat (win) --xslt=URI][--input=URI][--
output=URI]
```

Mit dieser Operation wandeln Sie XML-Datensätze in UMF um, bevor eine der Web-Service-Operationen verwendet wird.

wsutil.jar-Änderungswerte

Verwenden Sie diese Änderungswerte mit wsutil.jar-Operatoren, um die Eingabe- und Ausgabemethoden für den Web-Service-Befehl anzugeben.

input=*URI*
Gibt die Eingabemethode für UMF-Datensätze an. Die Standardeingabemethode ist stdin.

output=*URI*
Gibt die Ausgabemethode für UMF-Datensätze an. Die Standardausgabemethode ist stdout. Sie können mit dieser Methode eine Speicherposition und einen Dateinamen zum Speichern der UMF-Ausgabe angeben.

wsutil.jar-Beispielsyntax

Der folgende wsutil.jar-Befehl lädt auf einem UNIX-System Datensätze aus einer Datei, wandelt diese Sätze in UMF um und zeigt die Ergebnisse in der Konsole der Befehlszeilenschnittstelle an:

```
wsutil --load=http://localhost:13510/easws/services/SRDWebService
--input=raw_entities.xml --xslt=transform.xsl
```

Der folgende wsutil.jar-Befehl ruft auf einem Windows-System Anforderungen aus stdin ab und zeigt die Ergebnisse in der Konsole der Befehlszeilenschnittstelle an:

```
wsutil.bat --process=http://localhost:13510/SRDWebService
```

Erstellen von Abfragen mithilfe der Entitätendatenbank

Mit IBM InfoSphere Identity Insight können Sie die Entitätendatenbank auf mehrere Arten abfragen. Sie können Web-Service-Pipeline-Suchen erstellen, um die Entitätendatenbank auf Entitäten zu durchsuchen, die mit bestimmten Attributsuchkriterien übereinstimmen. Sie können auch Web-Service-Pipeline-Suchen erstellen, um die Datenbank auf eine bestimmte Entität abzufragen.

Web-Service-Pipeline-Suchen

In die Pipelines ist eine dynamische Such- und Abfrageschnittstelle integriert, über die die Web-Services die Entitätendatenbank zentral abfragen können. Mit UMF-Eingabedokumenten können Sie die Anforderung strukturieren und das UMF-Eingabedokument anschließend über Web-Services zur Verarbeitung an die Pipelines senden. Nach der Verarbeitung gibt die Pipeline ein UMF-Ausgabedokument zurück, das die Ergebnisse enthält.

Web-Service-Pipeline-Suchen stellen Antworten auf zwei Arten von Fragen bereit:

Welche Entitäten in der Entitätendatenbank stimmen mit einem bestimmten Attribut oder einer Attributgruppe überein? (UMF_SEARCH)
Diese Art von Web-Service-Pipeline-Suche nutzt die Entitätsauflösung optimal, um die eingehenden Suchkriterien zu erkennen sowie zu standardisieren und um dann die Suchkriterien mit Entitäten in der Datenbank abzugleichen. Sie wird als Übersichts- oder Ergebnismengenabfrage bezeichnet und gibt eine Entitätsliste mit Datenwerten zurück, die mit dem angeforderten Attributwert oder der Attributwerteliste übereinstimmen.

Zur Ausführung einer Übersichts- oder Ergebnismengenabfrage erstellen Sie ein UMF_SEARCH-Eingabedokument, das die Suchkriterien enthält, mit denen die Pipeline die Entitätsauflösung ausführt. Die Pipeline gibt ein UMF_SEARCH_RESULT-Ausgabedokument mit den Abfrageergebnissen zurück. Dabei handelt es sich um eine Liste der Entitäten, die mit den Suchkriterien übereinstimmen.

Was weiß die Entitätendatenbank über eine bestimmte Entität? (UMF_QUERY)
Diese Art von Web-Service-Pipeline-Suche verwendet SQL-Anweisungen und -Parameter, um die Entitätendatenbank abzufragen. Sie wird als Detail- oder Drilldown-Abfrage bezeichnet und gibt eine detaillierte Liste mit Informationen zu einer einzelnen Entität zurück.

Zur Ausführung einer Detail- oder Drilldown-Abfrage erstellen Sie ein UMF_QUERY-Eingabedokument, das angibt, zu welcher Entität in der Entitätendatenbank Sie Informationen abrufen wollen. Die Pipeline gibt ein UMF_QUERY_RESULT-Ausgabedokument mit den Details zur angeforderten Entität zurück.

Während der Ausführung von Web-Service-Pipeline-Suchen führen die Pipelines alle Standardpipelinefunktionen einschließlich Protokollierung aus.

Sowohl die Eingabe (Anforderung) als auch die Ausgabe (Antwort) für Web-Service-Pipeline-Suchen verwenden UMF-Dokumente und strukturieren die Informationen in UMF.

Formate der Web-Service-Pipeline-Suchen

Das Produkt wird mit mehreren integrierten Formaten für jede der Web-Service-Pipeline-Suchen ausgeliefert:

UMF_SEARCH-Formate

WS_SUMMARY_TOP10
Gibt eine Liste der 10 Topentitäten in der Datenbank zurück, die mit den in den Suchkriterien angegebenen Attributdaten am stärksten übereinstimmen.

WS_SUMMARY_TOP100
Gibt eine Liste der 100 Topentitäten in der Datenbank zurück, die mit den in den Suchkriterien angegebenen Attributdaten am stärksten übereinstimmen.

WS_SUMMARY
Gibt eine Liste aller Entitäten in der Datenbank zurück, die mit den in den Suchkriterien angegebenen Attributdaten übereinstimmen.

UMF_QUERY-Formate

WS_DETAIL
Gibt alle Daten aus der Entitätendatenbank für die angeforderte Entitäts-ID zurück.

WS_RELATION
Gibt eine Liste aller Entitäten in der Entitätendatenbank zurück, die über eine einstufige Beziehung mit der Eingabeentität verbunden sind.

WS_ALERT
Gibt eine Liste aller Alerts in der Entitätendatenbank zurück, die die Eingabeentitäts-ID einbeziehen.

Sie geben im Tag FORMAT_CODE des entsprechenden UMF-Eingabedokuments an, welches integrierte Format verwendet werden soll.

Leistungsaspekte

Wenn Web-Service-Pipeline-Suchanforderungen eine hohe Anzahl Suchkriterien enthalten, bedeutet dies in der Regel, dass das System die Daten mit weniger Entitäten in der Datenbank vergleicht. Daher gibt das System Ergebnisse schneller zurück als bei Anforderungen mit weniger Suchkriterien.

Erzeugen von Web-Service-Abfragen zum Suchen nach einer bestimmten Entität

Verwenden Sie diese Anweisungen, um ein UMF_QUERY-Eingabedokument zu erzeugen, mit dem Sie eine bestimmte Entität in der Datenbank suchen können. Das UMF_QUERY-Eingabedokument senden Sie über Web-Services zur Verarbeitung an eine Web-Service-Pipeline. Nachdem die Pipeline die Abfrage verarbeitet hat, gibt Web-Services ein UMF_QUERY_RESULT-Ausgabedokument zurück, das die Details zu der angeforderten Eingabe-Entität enthält.

Vorbereitende Schritte

Die integrierte WebSphere Application Server-Instanz muss aktiv sein und mindestens eine Web-Service-Pipeline muss gestartet und aktiv sein, um das UMF_QUERY-Eingabedokument zu empfangen und zu verarbeiten.

Informationen zu diesem Vorgang

Da die Suchanforderung ein UMF-Eingabedokument ist, müssen die Kriterien mit gültigen UMF-Tags formatiert werden. Sie können jeden Texteditor bzw. jedes Dienstprogramm verwenden, das UMF erstellt.

Vorgehensweise

1. Erstellen Sie ein neues UMF_QUERY-Eingabedokument.
2. Geben Sie im ROOT-Segment die erforderlichen UMF-Tags und Werte ein:
   a. Geben Sie den Datenquellencode in den Tag DSRC_CODE ein. Der Standarddatenquellencode für Web-Service-Pipeline-Suchen ist 1589. Wenn Sie einen anderen Datenquellencode verwenden als den Standarddatenquellencode für Web-Service-Pipeline-Suchen, müssen Sie sicherstellen, dass dieser andere Code so konfiguriert ist, dass er keine Entitäten auflöst.
   b. Geben Sie den Datenquellenreferenzcode, der auf die anfordernde Nachrichtentransaktion verweist, in den Tag DSRC_REF ein. Der Datenquellenreferenzcode sollte aussagekräftig sein, weil er an die aufrufende Anwendung zurückgegeben wird.
   c. Geben Sie den Formatcode mit dem Tag FORMAT_CODE ein, um das Ausgabeformat der Ergebnisse anzugeben. Im Lieferumfang der Pipelines sind drei integrierte Formatcodes für Web-Service-Pipeline-Suchen mit UMF_QUERY enthalten:
      - WS_DETAIL - gibt alle verfügbaren Entitätsdaten für die Eingabe-Entitäts-ID zurück.
      - WS_RELATION - gibt eine Liste aller Entitäten zurück, die eine einstufige Beziehung zu der Eingabe-Entität unterhalten.
      - WS_ALERT-Abfrage - gibt alle Rollenalerts im System zurück, an denen die Eingabe-Entitäts-ID beteiligt ist.

      Wenn Sie einen anderen Formatcode verwenden, muss dieser Formatcode in der Tabelle UMF_OUTPUT_FORMAT konfiguriert sein.
   d. Geben Sie im Tag ENTITY_ID die Entitäts-ID der Entität ein, für die Informationen zurückgegeben werden sollen.
3. Geben Sie eventuelle weitere Abfragekriterien über die optionalen UMF-Segmente <NAME>, <ADDRESS>, <EMAIL>, <ATTRIBUTE> und <NUMBER> ein.
4. Senden Sie das UMF_QUERY-Eingabedokument an eine Web-Service-Pipeline.

Ergebnisse

Die Web-Service-Pipeline empfängt das UMF_QUERY-Dokument und verwendet die angegebenen Kriterien, um in der Datenbank nach Entitäten zu suchen, die der Abfrage entsprechen. Anschließend verarbeitet die Pipeline die Abfrage, erstellt normale Protokolldateien und gibt die Ergebnisse über Web-Services in einem UMF_QUERY_RESULT-Ausgabedokument an die aufrufende Anwendung zurück.

Beispiel für UMF_QUERY-Suche

Bei dieser UMF_QUERY-Beispielsuche werden alle Informationen zur Entitäts-ID 1223 gesucht:

Anmerkung: Dieses Beispiel ist aus Gründen der Lesbarkeit formatiert. Die Formatvorgabe, dass jeder UMF-Datensatz eine Zeile enthalten muss, wird nicht beachtet.

```
<UMF_QUERY>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>546</DSRC_REF>
  <FORMAT_CODE>WS_DETAIL</FORMAT_CODE>
  <ENTITY_ID>1223</ENTITY_ID>
</UMF_QUERY>
```

UMF_QUERY-Eingabedokument

Das UMF_QUERY-Eingabedokument enthält die Gruppe der UMF-Segmente, die die eingehenden Daten strukturieren, um die Entitätendatenbank zu durchsuchen und anschließend nach Informationen zu einer bestimmten Entität zu suchen und diese an die aufrufende Anwendung zurückzugeben. Es enthält die Anforderungs- und Suchkriterien für eine Web-Service-Pipeline-Abfrage.

Die Informationen in einem UMF_QUERY-Eingabedokument basieren auf SQL-Anweisungen. Die Ergebnisse dieser Web-Service-Pipeline-Suche werden in einem UMF_QUERY_RESULT-Ausgabedokument an die aufrufende Anwendung zurückgegeben. UMF_QUERY führt eine erweiterte bzw. eine attributbasierte Abfrage aus.

Das UMF_QUERY-Eingabedokument besteht aus den folgenden erforderlichen UMF-Elementen und -Segmenten:

DSRC_CODE
: UMF-Tag des Datenquellencodes, der erforderlich ist, weil er auf die aufrufende Anwendung verweist und sie angibt. Dieser Datenquellencode wird während der normalen Pipelineprotokollierung für jedes verarbeitete Dokument UMF_QUERY in der Tabelle UMF_LOG protokolliert.

  Das System ist bereits mit dem Datenquellencode 1589 konfiguriert, der für alle Web-Service-Pipeline-Suchen verwendet werden kann. Dieser Datenquellencode führt die Entitätsauflösungsverarbeitung durch, ohne die eingehenden Suchkriterien in die Entität in der Entitätendatenbank aufzulösen, die mit der Suche übereinstimmt. Sie können Ihren eigenen Datenquellencode für eine bestimmte aufrufende Anwendung erstellen. Nur müssen Sie dazu sicherstellen, dass der Datenquellencode so eingestellt ist, dass er keine Entitäten auflöst.

DSRC_REF
: UMF-Tag des Datenquellenverweises, der erforderlich ist, weil er auf die anfordernde Nachrichtentransaktion verweist und an die aufrufende Anwendung zurückgegeben wird.

FORMAT_CODE

UMF-Tag, der zu einem UMF-Ausgabedokumentformat in Wechselbeziehung steht, das in der Tabelle UMF_OUTPUT_FORMAT angegeben ist. Im Lieferumfang von IBM InfoSphere Identity Insight sind drei integrierte Formatcodes für Web-Service-Pipeline-Suchen mit UMF_QUERY enthalten:

- WS_DETAIL gibt alle verfügbaren Entitätsdaten für die angeforderte Entitäts-ID zurück.
- WS_RELATION gibt eine Liste aller Entitäten zurück, die eine einstufige Beziehung zu der Eingabeentität haben.
- Die Abfrage WS_ALERT gibt alle Alerts im System zurück, die die Entitäts-ID der Eingabe betreffen.

Wenn die erweiterte Suche (EQ - Enhanced Query/attributbasierte Suche) über dieses Eingabedokument ausgeführt wird, muss FORMAT_CODE wie folgt angegeben werden.

Beispiel für ENHANCED_QUERY_RESULT:

```
<UMF_QUERY>
<FORMAT_CODE>ENHANCED_QUERY_RESULT</FORMAT_CODE>
 <ATTRIBUTE>
    <ATTR_TYPE>CIT</ATTR_TYPE>
    <ATTR_VALUE>CANADA</ATTR_VALUE>
  </ATTRIBUTE>
</UMF_QUERY>
```

ENTITY_ID

Dieser erforderliche UMF-Tag gibt die Entitäts-ID für die Entität in der Suche an. Das System gibt - gemäß den anderen Abfragekriterien - eine Antwort mit Details zu den bekannten Daten dieser Entität aus der Entitätendatenbank zurück.

Sie geben dann die optionalen Suchkriterien mithilfe der anderen verfügbaren UMF-Segmente und ihrer gültigen Tags für Namen, Adressen, Nummern, Merkmale und E-Mail-Adressen an.

NAME

Fragen Sie Namensattribute ab, die den Namen der Person, des Unternehmens, des Bereichs oder des Elements entsprechend dem Entitätsmodell und der eingehenden Identität definieren.

NUMBER

Fragen Sie Nummernattribute ab, die aus Daten bestehen, die in der Regel als Nummer beschrieben werden, z. B. Kreditkartennummern, Telefonnummern und Passnummern.

ADDRESS

Fragen Sie Adressattribute ab, die einen Standort der Identität definieren und in der Regel Standardadressinformationen enthalten: Straßenname und Hausnummer, Gebäudenummer, Ort, Bundesland/-staat, Land und Postleitzahl.

ATTRIBUTE

Fragen Sie Merkmalattribute ab, die weitere Identitätseigenschaften oder -informationen definieren, die durch die anderen Attributarten nicht ausgedrückt werden.

EMAIL

Fragen Sie E-Mailattribute ab, die Internet-E-Mail-Adressen definieren.

Beispiel für UMF_QUERY-Suche

In diesem Beispiel für UMF_QUERY wird der Formatcode WS_DETAIL zum Abfragen der Entitätendatenbank und zur Rückgabe aller bekannten Daten zur Entitäts-ID 1223 verwendet:

Anmerkung: Dieses Beispiel ist aus Gründen der Lesbarkeit formatiert. Die Formatvorgabe, dass jeder UMF-Datensatz eine Zeile enthalten muss, wird nicht beachtet.

```
<UMF_QUERY>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>546</DSRC_REF>
  <FORMAT_CODE>WS_DETAIL</FORMAT_CODE>
   <ENTITY_ID>1223</ENTITY_ID>
</UMF_QUERY>
```

Formatcode WS_DETAIL:

Wenn Sie eine Web-Service-Pipeline-Suche erstellen, bei der die Details zu einer bestimmten Entität in der Entitätendatenbank zurückgegeben werden sollen, verwenden Sie den integrierten Formatcode WS_DETAIL. Dieser Formatcode ist im UMF-_QUERY-Eingabedokument angegeben, das die Kriterien für die Abfrage enthält.

Beispiel einer Web-Service-Pipeline-Suche mit dem Formatcode WS_DETAIL

Dieses Beispiel einer Web-Service-Pipeline-Suche gibt alle Informationen in der Entitätendatenbank zu Joe Franklin, Entitäts-ID 87, zurück.

Anmerkung: Dieses Beispiel ist aus Gründen der Lesbarkeit formatiert. Die Formatvorgabe, dass jeder UMF-Datensatz eine Zeile enthalten muss, wird nicht beachtet.

Erstellen Sie ein neues UMF_QUERY-Eingabedokument mit der folgenden Anforderung, um die Details für Entitäts-ID 87 (Joe Franklin) anzufordern:

```
<UMF_QUERY>
  <FORMAT_CODE>WS_DETAIL</FORMAT_CODE>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>ABC-003</DSRC_REF>
  <ENTITY_ID>87</ENTITY_ID>
</UMF_QUERY>
```

Nachdem dieses UMF_QUERY-Dokument über Web-Services zur Verarbeitung durch eine Web-Service-Pipeline gesendet wurde, empfängt die aufrufende Anwendung im folgenden UMF_QUERY_RESULT-Dokument eine Antwort:

```
<UMF_QUERY_RESULT>
  <DSRC_CODE>1589</DSRC_CODE>
  <ENTITY>
   <ENTITY_ID>87</ENTITY_ID>
    <SOURCE>
    <ACCT>OFAC</ACCT>
  <NAME>
      <NAME_TYPE>MAIN</NAME_TYPE>
      <FIRST_NAME>JOSEPH</FIRST_NAME>
     <LAST_NAME>FRANKLIN</LAST_NAME>
     </NAME>
    <ADDRESS>
      <ADDR_TYPE>H</ADDR_TYPE>
      <ADDR1>5559 W. 4TH ST</ADDR1>
      <CITY>SAN FRANCISCO</CITY>
      <STATE>CA</STATE>
```

```
      <POSTAL_CODE>94123-4567</POSTAL_CODE>
      <COUNTRY>USA</COUNTRY>
    </ADDRESS>
  <NUMBER>
     <NUM_TYPE>PHONE</NUM_TYPE>
     <NUM_VALUE>415-555-3325</NUM_VALUE>
  </NUMBER>
    </SOURCE>
    <SOURCE>
    <ACCT>FBI</ACCT>
   <NAME>
       <NAME_TYPE>MAIN</NAME_TYPE>
        <FIRST_NAME>JOEY</FIRST_NAME>
      <LAST_NAME>FRANKLIN</LAST_NAME>
      </NAME>
    <ADDRESS>
      <ADDR_TYPE>H</ADDR_TYPE>
      <ADDR1>392 S.E. MULLENS AVE</ADDR1>
      <CITY>OAKLAND</CITY>
      <STATE>CA</STATE>
      <POSTAL_CODE>94126-1566</POSTAL_CODE>
      <COUNTRY>USA</COUNTRY>
    </ADDRESS>
  <NUMBER>
     <NUM_TYPE>PHONE</NUM_TYPE>
     <NUM_VALUE>415-555-3325</NUM_VALUE>
  </NUMBER>
  <NUMBER>
      <NUM_TYPE>CC</NUM_TYPE>
      <NUM_VALUE>1111-22-3333</NUM_VALUE>
  </NUMBER>
    </SOURCE>
    <SOURCE>
    <ACCT>A9</ACCT>
  <NAME>
      <NAME_TYPE>MAIN</NAME_TYPE>
     <FIRST_NAME>JOE</FIRST_NAME>
     <LAST_NAME>FRANKLIN</LAST_NAME>
     </NAME>
    <ADDRESS>
      <ADDR_TYPE>B</ADDR_TYPE>
      <ADDR1>392 S.E. MULLENS AVE</ADDR1>
      <CITY>OAKLAND</CITY>
      <STATE>CA</STATE>
      <POSTAL_CODE>94126-1566</POSTAL_CODE>
      <COUNTRY>USA</COUNTRY>
    </ADDRESS>
  <NUMBER>
     <NUM_TYPE>PHONE</NUM_TYPE>
     <NUM_VALUE>415-555-3325</NUM_VALUE>
  </NUMBER>
  <NUMBER>
      <NUM_TYPE>CC</NUM_TYPE>
      <NUM_VALUE>1111-22-3333</NUM_VALUE>
  </NUMBER>
    </SOURCE>
  </ENTITY>
  <FROM_NODE>ABC-003</FROM_NODE>
  <PAGE_NUM>1</PAGE_NUM>
  <FORMAT_CODE>WS_DETAIL</FORMAT_CODE>
</UMF_QUERY_RESULT>
```

Dieser Antwort können Sie entnehmen, dass es drei Datenquellen mit Informationen zu Joe Franklin gibt: die OFAC-Liste, eine FBI-Liste und die A9-Liste. Joe verwendet zwei verschiedene Adressen, in beiden Fällen verwendet er jedoch dieselbe Telefonnummer und dieselbe Kreditkarte.

Formatcode WS_ALERT:

Wenn Sie eine Web-Service-Pipeline-Suche erstellen, bei der alle Rollenalerts in der Entitätendatenbank zurückgegeben werden sollen, die eine bestimmte Entität betreffen, verwenden Sie den integrierten Formatcode WS_ALERT. Dieser Formatcode ist im UMF_QUERY-Eingabedokument angegeben, das die Kriterien für die Abfrage enthält.

Beispiel einer Web-Service-Pipeline-Suche mit dem Formatcode WS_ALERT

Dieses Beispiel einer Web-Service-Pipeline-Suche gibt eine Liste aller Rollenalerts zurück, bei denen Joe Franklin, Entitäts-ID 87, betroffen ist.

Anmerkung: Dieses Beispiel ist aus Gründen der Lesbarkeit formatiert. Die Formatvorgabe, dass jeder UMF-Datensatz eine Zeile enthalten muss, wird nicht beachtet.

Erstellen Sie ein neues Eingabedokument UMF_QUERY mit der folgenden Anforderung, um die Rollenalerts für Entitäts-ID 87 (Joe Franklin) anzufordern:

```
<UMF_QUERY>
  <FORMAT_CODE>WS_ALERT</FORMAT_CODE>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>BB123-9003</DSRC_REF>
  <ENTITY_ID>87</ENTITY_ID>
</UMF_QUERY>
```

Nachdem dieses UMF_QUERY-Dokument über Web-Services zur Verarbeitung durch eine Web-Service-Pipeline gesendet wurde, empfängt die aufrufende Anwendung im folgenden UMF_QUERY_RESULT-Dokument eine Antwort:

```
<UMF_QUERY_RESULT>
   <ALERT>
    <CONFLICT_ID>2</CONFLICT_ID>
    <CONFLICT_RULES_DESC>Krimineller kennt Angestellten</CONFLICT_RULES_DESC>
    <CONF_ENTITY1>87</CONF_ENTITY1>
    <CONF_ENTITY2>376</CONF_ENTITY2>
    <DEGREE_OF_SEP>1</DEGREE_OF_SEP>
    <INBOUND_ENTITY_ID>87</INBOUND_ENTITY_ID>
    <NAME1>FRANKLIN, JOSEPH</NAME1>
    <NAME2>MILLER, SUSAN</NAME2>
    <PATH_STRENGTH>80</PATH_STRENGTH>
  </ALERT>
  <ALERT>
    <CONFLICT_ID>5</CONFLICT_ID>
    <CONFLICT_RULES_DESC>Krimineller kennt Lieferanten</CONFLICT_RULES_DESC>
    <CONF_ENTITY1>87</CONF_ENTITY1>
    <CONF_ENTITY2>10651</CONF_ENTITY2>
    <DEGREE_OF_SEP>1</DEGREE_OF_SEP>
    <INBOUND_ENTITY_ID>87</INBOUND_ENTITY_ID>
    <NAME1>FRANKLIN, JOSEPH</NAME1>
    <NAME2>MARTINEZ, JULIO</NAME2>
    <PATH_STRENGTH>64</PATH_STRENGTH>
  </ALERT>
  <DSRC_CODE>1589</DSRC_CODE>
  <FROMNODE>BB123-9003</FROMNODE>
</UMF_QUERY_RESULT>
```

Dieser Antwort können Sie entnehmen, dass es zwei Rollenalerts für Joe Franklin gibt: Einen Alert, in dem die Angestellte Susan Miller Joe kennt, und einen Alert, in dem der Lieferant Julio Martinez Joe kennt.

Formatcode WS_RELATION:

Wenn Sie eine Web-Service-Pipeline-Suche erstellen, bei der eine Liste aller Entitäten zurückgegeben werden soll, die eine einstufige Beziehung zu einer bestimmten Entität haben, verwenden Sie den integrierten Formatcode WS_RELATION. Dieser Formatcode ist im UMF_QUERY-Eingabedokument angegeben, das die Kriterien für die Abfrage enthält.

Beispiel einer Web-Service-Pipeline-Suche mit dem Formatcode WS_RELATION

Dieses Beispiel einer Web-Service-Pipeline-Suche gibt eine Liste aller Entitäten zurück, die eine einstufige Beziehung zu Joe Franklin, Entitäts-ID 87, haben.

Anmerkung: Dieses Beispiel ist aus Gründen der Lesbarkeit formatiert. Die Formatvorgabe, dass jeder UMF-Datensatz eine Zeile enthalten muss, wird nicht beachtet.

```
<UMF_QUERY>
  <FORMAT_CODE>WS_RELATION</FORMAT_CODE>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>ABC-003</DSRC_REF>
  <ENTITY_ID>87</ENTITY_ID>
</UMF_QUERY>
```

Nachdem dieses UMF_QUERY-Dokument über Web-Services zur Verarbeitung durch eine Web-Service-Pipeline gesendet wurde, empfängt die aufrufende Anwendung im folgenden UMF_QUERY_RESULT-Dokument eine Antwort:

```
<UMF_QUERY_RESULT>
  <DSRC_CODE>1589</DSRC_CODE>
  <RELATION>
    <DETAIL>
    <ENTITY_ID>87</ENTITY_ID>
      <INBOUND_VALUE_ABST>415-555-3325</INBOUND_VALUE_ABST>
      <MATCHED_CODE>6</MATCHED_CODE>
      <MATCHED_DSRC_ACCT>6</MATCHED_DSRC_CODE>
      <MATCHED_ENTITY_ID>376</MATCHED_ENTITY_ID>
      <MATCHED_KEY_ID>16</MATCHED_KEY_ID>
      <MATCHED_TYPE>NUMBER</MATCHED_TYPE>
      <MATCHED_VALUE_ABST>415-555-3325</MATCHED_VALUE_ABST>
      <MATCH_PRECISION>EXACT MATCH</MATCH_PRECISION>
      <SIMILARITY_ID>1</SIMILARITY_ID>
    </DETAIL>
    <DETAIL>
    <ENTITY_ID>87</ENTITY_ID>
      <LIKE_CONF>40</LIKE_CONF>
      <MATCH_ID>376</MATCH_ID>
      <RELTO_ID>6</RELTO_ID>
    </DETAIL>
    <DETAIL>
    <ENTITY_ID>87</ENTITY_ID>
      <INBOUND_VALUE_ABST>1111-22-3333</INBOUND_VALUE_ABST>
      <MATCHED_CODE>6</MATCHED_CODE>
      <MATCHED_DSRC_ACCT>6</MATCHED_DSRC_CODE>
   <MATCHED_ENTITY_ID>10651/MATCHED_ENTITY_ID>
      <MATCHED_KEY_ID>16</MATCHED_KEY_ID>
      <MATCHED_TYPE>NUMBER</MATCHED_TYPE>
      <MATCH_PRECISION>EXACT MATCH</MATCH_PRECISION>
      <SIMILARITY_ID>1</SIMILARITY_ID>
    </DETAIL>
    <DETAIL>
    <ENTITY_ID>87</ENTITY_ID>
      <LIKE_CONF>40</LIKE_CONF>
      <MATCH_ID>10651</MATCH_ID>
```

```
      <RELTO_ID>6</RELTO_ID>
  </RELATION>
  <FORMAT_CODE>WS_RELATION</FORMAT_CODE>
<UMF_QUERY_RESULT>
```

Erzeugen von Web-Service-Abfragen zum Suchen von Entitäten mit ähnlichen Attributen

Verwenden Sie diese Anweisungen, um ein UMF_SEARCH-Eingabedokument zu erzeugen, mit dem Sie Entitäten in der Entitätendatenbank suchen können, die den Datenwerten der in den Suchkriterien angegebenen Attributen entsprechen. Das UMF_SEARCH-Eingabedokument senden Sie über Web-Services zur Verarbeitung an eine Web-Service-Pipeline. Nachdem die Pipeline die Abfrage verarbeitet hat, geben die Web-Services ein UMF_SEARCH_RESULTS-Ausgabedokument zurück, das eine Liste der Entitäten enthält, die den Suchkriterien entsprechen.

Vorbereitende Schritte

Die integrierte WebSphere Application Server-Instanz muss aktiv sein und mindestens eine Web-Service-Pipeline muss gestartet und aktiv sein, um das UMF-_SEARCH-Eingabedokument zu empfangen und zu verarbeiten.

Informationen zu diesem Vorgang

Da die Suchanforderung ein UMF-Eingabedokument ist, müssen die Kriterien mit gültigen UMF-Tags formatiert werden. Sie können jeden Texteditor bzw. jedes Dienstprogramm verwenden, das UMF erstellt.

Vorgehensweise

1. Erstellen Sie ein neues UMF_SEARCH-Eingabedokument.
2. Geben Sie im ROOT-Segment die erforderlichen UMF-Tags und die zugehörigen Werte sowie eventuelle optionale UMF-Tags und die zugehörigen Werte ein, die Sie für die Angabe der Suchkriterien verwenden wollen. Geben Sie mindestens Werte für die folgenden UMF-Tags ein:
   a. Geben Sie den Datenquellencode in den Tag DSRC_CODE ein. Der Standarddatenquellencode für Web-Service-Pipeline-Suchen ist 1589. Wenn Sie einen anderen Datenquellencode verwenden als den Standarddatenquellencode für Web-Service-Pipeline-Suchen, müssen Sie sicherstellen, dass dieser andere Code so konfiguriert ist, dass er keine Entitäten auflöst.
   b. Geben Sie den Datenquellenreferenzcode, der auf die anfordernde Nachrichtentransaktion verweist, in den Tag DSRC_REF ein. Der Datenquellenreferenzcode sollte aussagekräftig sein, weil er an die aufrufende Anwendung zurückgegeben wird.
   c. Geben Sie den Formatcode mit dem Tag FORMAT_CODE ein, um das Ausgabeformat der Ergebnisse anzugeben. Im Lieferumfang der Pipelines sind drei integrierte Formatcodes für Web-Service-Pipeline-Suchen mit UMF-_SEARCH enthalten:
      - WS_SUMMARY_TOP10, gibt die 10 Entitäten zurück, die am besten mit den Suchkriterien übereinstimmen
      - WS_SUMMARY_TOP100, gibt die 100 Entitäten zurück, die am besten mit den Suchkriterien übereinstimmen
      - Abfrage WS_SUMMARY, gibt alle Entitäten zurück, die mit den Suchkriterien übereinstimmen

Wenn Sie einen anderen Formatcode verwenden, muss dieser Formatcode in der Tabelle UMF_OUTPUT_FORMAT konfiguriert sein.

d. Geben Sie die Mindestauflösungsbewertung in den Tag MIN_LIKE_SCORE ein. Damit legen Sie die niedrigste numerische Bewertung fest, die als Übereinstimmung zwischen den Attributwerten in den Suchkriterien und den Entitäten in der Entitätendatenbank, die dieselben Attribute enthalten, angesehen wird. Je höher die Bewertung ist, umso genauer muss die Übereinstimmung sein. Eine Bewertung von 100 zeigt eine exakte Übereinstimmung an.

3. Verwenden Sie die übrigen gültigen Segmente des UMF-Eingabedokuments, um die Datenwerte für die Attribute einzugeben, die die Suchkriterien bilden. Diese Werte sind die Attribute, die bei der Pipelinesuche über Web-Services verglichen werden, um die Liste der Entitäten mit übereinstimmenden oder ähnlichen Werten zu erzeugen. Die Genauigkeit der Übereinstimmung ist vom Wert in MIN_LIKE_SCORE abhängig.
4. Senden Sie das UMF_SEARCH-Eingabedokument über Web-Services.

Ergebnisse

Die Web-Service-Pipeline empfängt das UMF_SEARCH-Dokument und verwendet den Entitätsauflösungsprozess, um gemäß den angegebenen Kriterien in der Datenbank nach Entitäten zu suchen. Anschließend verarbeitet die Pipeline die Abfrage, erstellt normale Protokolldateien und gibt die Ergebnisse über Web-Services in einem UMF_SEARCH_RESULTS-Dokument im ausgewählten Format an die aufrufende Anwendung zurück.

Beispiel für UMF_SEARCH-Dokumentabfrage

Bei diesem UMF_SEARCH-Beispieleingabedokument wird der Formatcode WS-_SUMMARY_TOP10 für die Abfrage der Entitätendatenbank verwendet. Es sollen die 10 Entitäten gesucht werden, deren Datenwerte für die Sozialversicherungsnummer dem Datenwert 555-09-8761 am genauesten entsprechen:

Anmerkung: Dieses Beispiel ist aus Gründen der Lesbarkeit formatiert. Die Formatvorgabe, dass jeder UMF-Datensatz eine Zeile enthalten muss, wird nicht beachtet.

```
<UMF_SEARCH>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>1223</DSRC_REF>
  <MIN_LIKE_SCORE>100</MIN_LIKE_SCORE>
  <FORMAT_CODE>WS_SUMMARY_TOP10</FORMAT_CODE>
 <NUMBER>
    <NUM_TYPE>SSN</NUM_TYPE>
    <NUM_VALUE>555-09-8761</NUM_VALUE>
 </NUMBER>
</UMF_SEARCH>
```

UMF_SEARCH-Eingabedokument

Das UMF_SEARCH-Eingabedokument enthält die Anforderungs- und Suchkriterien für eine Web-Service-Pipeline-Suche. Es enthält die Sammlung von UMF-Segmenten, die die eingehenden Daten strukturieren, um die Entitätendatenbank nach Entitäten zu durchsuchen, die den Suchkriterien entsprechende Attributwerte enthalten, und um dann die Liste der Entitäten an die aufrufende Anwendung zurückzusenden. Die Ergebnisse dieser Web-Service-Pipeline-Suche werden in einem UMF_SEARCH_RESULT-Ausgabedokument an die aufrufende Anwendung zurückgegeben. UMF_SEARCH führt einen vollständigen auflösungsbasierten Prozess aus.

Diese erforderlichen UMF-Elemente und -Segmente enthalten das UMF_SEARCH-Eingabedokument:

DSRC_CODE
UMF-Tag des Datenquellencodes, der erforderlich ist, weil er auf die aufrufende Anwendung verweist und sie angibt. Dieser Datenquellencode wird während der normalen Pipelineprotokollierung für jedes verarbeitete UMF_SEARCH-Dokument in der Tabelle UMF_LOG protokolliert.

Das System ist bereits mit dem Datenquellencode 1589 konfiguriert, der für alle Web-Service-Pipeline-Suchen verwendet werden kann. Dieser Datenquellencode führt die Entitätsauflösungsverarbeitung durch, ohne die eingehenden Suchkriterien in die Entität in der Entitätendatenbank aufzulösen, die mit der Suche übereinstimmt. Sie können Ihren eigenen Datenquellencode für eine bestimmte aufrufende Anwendung erstellen. Nur müssen Sie dazu sicherstellen, dass der Datenquellencode so eingestellt ist, dass er keine Entitäten auflöst.

DSRC_REF
UMF-Tag des Datenquellenverweises, der erforderlich ist, weil er auf die anfordernde Nachrichtentransaktion verweist und an die aufrufende Anwendung zurückgegeben wird.

SRC_CREATE_DT
Der UMF-Tag für das Quellenerstellungsdatum ist optional. Wenn dieser Tag einen Wert enthält, wird er für die Protokollierung verwendet.

SRC_LSTUPD_DT
Der UMF-Tag für das Datum der letzten Aktualisierung der Quelle ist optional. Wenn dieser Tag einen Wert enthält, wird er für die Protokollierung verwendet.

SRC_LSTUP_US
Der UMF-Tag für den Benutzer, der die letzte Aktualisierung der Quelle vorgenommen hat, ist optional. Wenn dieser Tag einen Wert enthält, wird er für die Protokollierung verwendet.

MIN_LIKE_SCORE
UMF-Tag für die Mindestauflösungsbewertung (oder Ähnlichkeitsbewertung), der für die Erstellung des niedrigsten übereinstimmenden Werts für die anderen angegebenen UMF-Segmente und -Tags erforderlich ist. Diese numerische Bewertung legt fest, was zwischen den angeforderten Attributwerten und den Entitäten in der Entitätendatenbank, die dieselben Attribute enthalten, als Übereinstimmung betrachtet wird. Je höher die Bewertung ist, umso genauer muss die Übereinstimmung sein. Eine Bewertung von 100 zeigt eine exakte Übereinstimmung an.

Sollen bei der Suche beispielsweise alle Entitäten mit einer bestimmten Sozialversicherungsnummer gefunden werden, legt MIN_LIKE_SCORE fest, wie groß die Übereinstimmung zwischen einer Sozialversicherungsnummer und dem in der Abfrage angegebenen Wert für die Sozialversicherungsnummer sein muss, damit eine Entität in der Datenbank in der Ergebnismenge für diese Abfrage enthalten ist.

FORMAT_CODE
UMF-Tag, der zu einem UMF-Ausgabedokumentformat in Wechselbeziehung steht, das in der Tabelle UMF_FORMAT_CODE angegeben ist. Im Lieferumfang von IBM InfoSphere Identity Insight sind drei integrierte Formatcodes für Web-Service-Pipeline-Suchen mit UMF_SEARCH enthalten:

- WS_SUMMARY_TOP10, gibt die 10 Entitäten zurück, die am besten mit den Suchkriterien übereinstimmen
- WS_SUMMARY_TOP100, gibt die 100 Entitäten zurück, die am besten mit den Suchkriterien übereinstimmen
- Abfrage WS_SUMMARY, gibt alle Entitäten zurück, die mit den Suchkriterien übereinstimmen

Der einzige Unterschied zwischen diesen Abfragen liegt in der Anzahl der zurückgegebenen Datensätze, die im Abfragenamen angegeben ist.

Sie geben dann die optionalen Suchkriterien mithilfe der anderen verfügbaren UMF-Segmente und ihrer gültigen Tags für Namen, Adressen, Nummern, Merkmale und E-Mail-Adressen an.

NAME
Suchen Sie nach Namensattributen, die den Namen der Person, des Unternehmens, des Bereichs oder des Elements entsprechend dem Entitätsmodell und der eingehenden Identität definieren.

NUMBER
Suchen Sie nach Nummernattributen, die aus Daten bestehen, die in der Regel als Nummer beschrieben werden, z. B. Kreditkartennummern, Telefonnummern und Passnummern.

ADDRESS
Suchen Sie nach Adressattributen, die einen Standort der Identität definieren und in der Regel Standardadressinformationen enthalten: Straßenname und Hausnummer, Gebäudenummer, Ort, Bundesland/-staat, Land und Postleitzahl.

ATTRIBUTE
Suchen Sie nach Merkmalattributen, die weitere Identitätseigenschaften oder -informationen definieren, die durch die anderen Attributarten nicht ausgedrückt werden.

EMAIL
Suchen Sie nach E-Mailattributen, die Internet-E-Mail-Adressen definieren.

UMF_SEARCH-Beispielabfrage

Diese UMF_SEARCH-Beispielabfrage gibt die ersten 5 Entitäten in der Entitätendatenbank zurück, die eine Sozialversicherungsnummer haben, die exakt mit der Sozialversicherungsnummer 555-09-8761 übereinstimmt. Auch wenn mehr Entitäten gefunden werden, werden nur die ersten 5 Entitäten in der Liste zurückgegeben.

Anmerkung: Dieses Beispiel ist aus Gründen der Lesbarkeit formatiert. Die Formatvorgabe, dass jeder UMF-Datensatz eine Zeile enthalten muss, wird nicht beachtet.

```
<UMF_SEARCH>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>1223</DSRC_REF>
  <MIN_LIKE_SCORE>100</MIN_LIKE_SCORE>
  <MAX_RETURN_CNT>5</MAX_RETURN_CNT>
  <FORMAT_CODE>WS_SUMMARY</FORMAT_CODE>
 <NUMBER>
    <NUM_TYPE>SSN</NUM_TYPE>
    <NUM_VALUE>555-09-8761</NUM_VALUE>
 </NUMBER>
</UMF_SEARCH>
```

Formatcodes WS_SUMMARY:

IBM InfoSphere Identity Insight wird mit drei vordefinierten Formatcodes für das Eingabedokument UMF_SUMMARY geliefert: WS_SUMMARY, WS_SUMMARY-_TOP10 und WS_SUMMARY_TOP100. Diese Formatcodes geben eine Liste der Entitäten zurück, die den im Eingabedokument UMF_SUMMARY angegebenen Kriterien entsprechen. Der einzige Unterschied zwischen diesen Formatcodes liegt in der maximalen Anzahl der zurückgegebenen Datendatensätze, die im Formatcodenamen angegeben ist.

Beispiel einer Web-Service-Pipeline-Suche mit dem Formatcode WS_SUMMARY-_TOP10

Dieses Beispiel einer Web-Service-Pipeline-Suche gibt die ersten 10 Entitäten in der Entitätendatenbank zurück, die die größte Übereinstimmung mit den folgenden Suchkriterien aufweisen:

- Name: Joe Franklin
- Telefonnummer: 415-555-3325
- Geburtsdatum: 2. Januar 1956

Zur Angabe dieser Kriterien wird das UMF_SEARCH-Eingabedokument verwendet, das auch den Formatcode `WS_SUMMARY_TOP10` angibt.

Anmerkung: Dieses Beispiel ist aus Gründen der Lesbarkeit formatiert. Die Formatvorgabe, dass jeder UMF-Datensatz eine Zeile enthalten muss, wird nicht beachtet.

```
<UMF_SEARCH>
  <FORMAT_CODE>WS_SUMMARY_TOP10</FORMAT_CODE>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>556</DSRC_REF>
  <MIN_LIKE_SCORE>80</MIN_LIKE_SCORE>
 <NAME>
    <NAME_TYPE>M</NAME_TYPE>
    <LAST_NAME>FRANKLIN</LAST_NAME>
    <FIRST_NAME>JOE</FIRST_NAME>
    </NAME>
 <NUMBER>
    <NUM_TYPE>PHONE</NUM_TYPE>
    <NUM_VALUE>415-555-3325</NUM_VALUE>
 </NUMBER>
 <ATTRIBUTE>
    <ATTR_TYPE>DOB</ATTR_TYPE>
    <ATTR_VALUE>01/02/1956</ATTR_VALUE>
  </ATTRIBUTE>
</UMF_SEARCH>
```

Nachdem dieses UMF_SEARCH-Dokument über Web-Services zur Verarbeitung durch eine Web-Service-Pipeline gesendet wurde, empfängt die aufrufende Anwendung im folgenden UMF_SEARCH_RESULT-Dokument eine Antwort:

```
<UMF_SEARCH_RESULT>
  <DSRC_CODE>1589</DSRC_CODE>
  <ENTITY>
    <MATCHED_ENTITY_ID>38763</MATCHED_ENTITY_ID>
    <ENT_NAME>FRANKLIN, JOEY</ENT_NAME>
    <ENT_PHONE>415-555-3325</ENT_PHONE>
    <ENT_DOB>01/02/1956</ENT_DOB>
    <LIKE_SCORE>90</LIKE_SCORE>
  </ENTITY>
  <ENTITY>
    <MATCHED_ENTITY_ID>87</MATCHED_ENTITY_ID>
```

```
    <ENT_NAME>FRANKLIN, JOSEPH</ENT_NAME>
    <ENT_PHONE>415-555-3325</ENT_PHONE>
    <ENT_DOB>02/01/1956</ENT_DOB>
    <LIKE_SCORE>80</LIKE_SCORE>
  </ENTITY>
  <ENTITY>
    <MATCHED_ENTITY_ID>330</MATCHED_ENTITY_ID>
    <ENT_NAME>FRANKLIN, J</ENT_NAME>
    <ENT_PHONE>451-555-3325</ENT_PHONE>
    <ENT_DOB>01/02/1956</ENT_DOB>
    <LIKE_SCORE>80</LIKE_SCORE>
  </ENTITY>
  <FROM_NODE>556</FROM_NODE>
  <FORMAT_CODE>WS_SUMMARY_TOP10</FORMAT_CODE>
  <MIN_LIKE_SCORE>80</MIN_LIKE_SCORE>
  <PAGE_NUM>1</PAGE_NUM>
  <RETURN_CNT>3</RETURN_CNT>
</UMF_SEARCH_RESULT>
```

In diesem Fall enthielt die Entitätendatenbank nur 3 Entitäten, die den Suchkriterien mit einer Mindestähnlichkeitsbewertung von 80 entsprachen.

Kapitel 10. Fehlerbehebung und Unterstützung

In diesem Abschnitt werden Informationen zum Beheben von Fehlern in Ihrer IBM InfoSphere Identity Insight-Software bereitgestellt. Hierzu gehören Anweisungen zum Durchsuchen von Wissensbasen, Herunterladen von Programmkorrekturen und Anfordern von Unterstützung.

Übersicht über Fehlerbehebung

Fehlerbehebung ist ein systematischer Ansatz zum Lösen von Problemen. Das Ziel ist die Ermittlung, warum etwas nicht wie erwartet funktioniert und wie das Problem gelöst werden kann.

Der erste Schritt im Fehlerbehebungsprozess ist eine vollständige Beschreibung des Problems. Ohne eine Problembeschreibung haben weder Sie noch IBM einen Ausgangspunkt für das Ermitteln der Problemursache. Stellen Sie sich die folgenden grundlegenden Fragen:

- An welchen Symptomen zeigt sich das Problem?
- Wo tritt das Problem auf?
- Wann tritt das Problem auf?
- Unter welchen Bedingungen tritt das Problem auf?
- Kann das Problem reproduziert werden?

Die Antworten auf diese Fragen führen in der Regel zu einer guten Beschreibung des Problems. Dies ist die beste Methode, die Problemlösung in Angriff zu nehmen.

An welchen Symptomen zeigt sich das Problem?

Die erste zu stellende Frage am Anfang einer Problembeschreibung lautet: "Was ist das Problem?" Diese allgemein gehaltene Frage kann in mehrere präzisere Fragen aufgeteilt werden, die ein anschaulicheres Bild des Problems liefern. Sie können folgende Fragen stellen:

- Wer oder was berichtet das Problem?
- Wie lauten die Fehlercodes und Nachrichten?
- Wie schlägt das System fehl? Handelt es sich z. B. um eine Schleife, eine Blockierung, einen Absturz, Leistungseinbußen oder ein falsches Ergebnis?
- Wie beeinflusst das Problem die Geschäftsabläufe?

Wo tritt das Problem auf?

Es ist nicht immer einfach, die Ursache eines Problems zu ermitteln, aber dies ist einer der wichtigsten Schritte beim Lösen des Problems. Zwischen der Komponente, die das Problem meldet, und der fehlgeschlagenen Komponente können viele Technologieschichten liegen. Netze, Datenträger und Treiber sind nur einige der Komponenten, die beim Untersuchen von Problemen in Betracht gezogen werden müssen.

Die folgenden Fragen sollen Ihnen helfen, die Problemschicht einzugrenzen.

- Trifft das Problem auf nur eine Plattform oder ein Betriebssystem zu?

- Tritt das Problem auf mehreren Servern auf?
- Werden die aktuelle Umgebung und Konfiguration unterstützt?

Selbst wenn eine Schicht das Problem meldet, bedeutet dies nicht unbedingt, dass das Problem von dieser Schicht verursacht wird. Wenn Sie feststellen wollen, wodurch ein Problem verursacht wird, muss auch die Umgebung geklärt werden, in der das Problem auftritt. Nehmen Sie sich genügend Zeit, die Problemumgebung vollständig zu beschreiben. Schließen Sie dabei das Betriebssystem, seine Version, die gesamte zugehörige Software mit Versionsangabe und Hardwareinformationen ein. Stellen Sie sicher, dass Sie in einer Umgebung arbeiten, die eine unterstützte Konfiguration ist. Viele Probleme können auf inkompatible Softwareversionen zurückgeführt werden, die nicht für gemeinsame Ausführung konzipiert sind oder nicht vollständig zusammen getestet wurden.

Wann tritt das Problem auf?

Ermitteln Sie den detaillierten zeitlichen Ablauf der Ereignisse, die zu einem Fehler geführt haben, vor allem für jene Fälle, die nur einmal aufgetreten sind. Sie arbeiten hierfür am einfachsten rückwärts: Starten Sie an dem Zeitpunkt, zu dem ein Fehler gemeldet wurde (so genau wie möglich, d. h. bis auf die Millisekunde), und arbeiten Sie sich rückwärts durch die verfügbaren Protokolle und Informationen. In der Regel brauchen Sie nur das erste suspekte Ereignis in einem Protokoll der Diagnoseprogramme zu finden. Dies ist jedoch nicht immer einfach und bedarf einiger Übung. Es ist schwer zu ermitteln, wann die Suche gestoppt werden soll, wenn mehrere Technologieschichten beteiligt sind und jede Schicht über eigene Diagnoseinformationen verfügt.

Versuchen Sie, die folgenden Fragen zu beantworten, um einen detaillierten Zeitplan der Ereignisse zu entwickeln:

- Tritt das Problem zu einer bestimmten Tages- oder Nachtzeit auf?
- Wie häufig tritt das Problem auf?
- Welche Reihe von Ereignissen ist bis zu dem Zeitpunkt aufgetreten, zu dem das Problem berichtet wird?
- Tritt das Problem nach einer Umgebungsänderung wie der Durchführung eines Upgrades oder einer Installation von Software oder Hardware auf?

Die Antworten auf derartige Fragen helfen Ihnen bei der Bereitstellung eines Kontextes, mit dessen Hilfe das Problem untersucht werden kann.

Unter welchen Bedingungen tritt das Problem auf?

Es ist wichtig zu wissen, welche anderen Systeme und Anwendungen ausgeführt werden, wenn das Problem auftritt. Die folgenden und andere Fragen zu Ihrer Umgebung können Ihnen beim Feststellen der eigentlichen Fehlerursache helfen:

- Tritt das Problem immer auf, wenn dieselbe Task ausgeführt wird?
- Muss eine bestimmte Ereignisfolge ablaufen, damit das Problem auftritt?
- Schlagen andere Anwendungen zur selben Zeit fehl?

Antworten auf diese Arten von Fragen können Ihnen beim Überprüfen der Umgebung, in der das Problem auftritt, und beim Korrelieren von Abhängigkeiten helfen. Beachten Sie, dass ein Auftreten mehrerer Probleme zur ungefähr gleichen Zeit nicht unbedingt auf eine Zusammengehörigkeit der Probleme hinweist.

Kann das Problem reproduziert werden?

Aus Sicht der Fehlerbehebung ist ein Problem 'ideal', wenn es reproduziert werden kann. In der Regel stehen ihnen bei der Überprüfung reproduzierbarer Probleme umfangreichere Gruppen von Tools oder Prozeduren zur Verfügung. Daher sind reproduzierbare Probleme häufig einfacher zu testen und beheben. Reproduzierbare Probleme haben jedoch einen Nachteil: Wenn das Problem die Geschäftsabläufe entscheidend beeinflusst, wollen Sie ein erneutes Auftreten vermeiden. Reproduzieren Sie das Problem in einer Test- oder Entwicklungsumgebung, sofern möglich. Diese Umgebung bietet Ihnen in der Regel größere Flexibilität und Steuerung während der Untersuchung.

- Kann das Problem auf einem Testsystem reproduziert werden?
- Stoßen mehrere Benutzer oder Anwendungen auf dieselbe Art von Problem?
- Kann das Problem durch die Ausführung eines einzelnen Befehls, einer Befehlsgruppe oder einer bestimmten Anwendung bzw. einer eigenständigen Anwendung reproduziert werden?

Fehlerbehebung in IBM InfoSphere Identity Insight

Die folgenden Fragen sollen Ihnen beim Identifizieren und Lösen von Problemen helfen, die in IBM InfoSphere Identity Insight auftreten.

1. Wurden bei der Ausführung des Installationsprogramms Nachrichten angezeigt, dass die Installation einer oder mehrerer Komponenten nicht erfolgreich war? Ist dies der Fall, prüfen Sie die Installationsprotokolldateien, um den Fehler zu ermitteln und zu beheben.
2. Sind Ihre Funktionsaktualisierungen auf dem neuesten Stand?
3. Wird eine Fehlernachricht angezeigt?
4. Haben Sie die Protokolldateien der Komponenten überprüft, um festzustellen, ob sie Nachrichten enthalten, die sich auf den Fehler beziehen?
5. Tritt der Fehler bei Verwendung einer der folgenden Komponenten auf?
   - Analyst Toolkit-Webanwendungen - Überprüfen Sie die „Prüfliste zur Fehlerbehebung für Analyst Toolkit-Webanwendungen" auf Seite 405.
   - Pipelines - Überprüfen Sie die Prüfliste zur Fehlerbehebung für Pipelines.
6. Haben Sie die Wissensbasen des Produkts auf Informationen überprüft, mit denen der Fehler behoben werden könnte?
7. Wenn Sie alle diese Möglichkeiten geprüft haben und Ihr Problem immer noch besteht, wenden Sie sich an den IBM Software Support.

Prüfliste zur Fehlerbehebung für Pipelines

Treten Probleme mit den Pipelines auf, prüfen Sie zunächst diese Liste der am häufigsten auftretenden Pipelineprobleme, bevor Sie sich an den IBM Software Support wenden.

1. Pipeline berichtet den Status 'Inaktiv' oder keinen Status
2. Pipeline wird beendet
3. Pipelines berücksichtigen keine in der Konfigurationskonsole vorgenommenen Konfigurationsänderungen
4. Pipelines starten nicht unter AIX
5. Pipeline verarbeitet nur einen Teil eines eingehenden Datensatzes
6. Transport funktioniert nicht
7. Pipeline lädt Zahlen in Exponentialschreibweise oder Gleitkommazahlen nicht

8. Nach dem Start einer Pipeline wird eine Warnung empfangen, dass keine Routen definiert sind

1. **Pipeline berichtet den Status 'Inaktiv' oder keinen Status**
   - Liegt ein Fehler des Pipelineknotens vor, oder ist er nicht aktiv?
   - Ist die Syntax der im Pipelinebefehl angegebenen Transportmethode korrekt?
   - Wurde die Pipeline beendet?
2. **Pipeline wird beendet oder fällt aus**
   - Traten bei der Verarbeitung eingehender Datendateien zu viele Fehler in der Pipeline auf?
     – Überprüfen Sie die Protokolldateien auf weitere Informationen zu den Fehlern. Beheben Sie das Problem mithilfe dieser Informationen.
     – Überprüfen Sie die Einstellung für *ErrorLimit* in der Pipelinekonfigurationsdatei. Sie müssen diesen Wert unter Umständen erhöhen.
   - Sind die Speicherressourcen der Pipeline erschöpft?
   - Wird das Problem aus einem der folgenden Gründe durch die Datenbank verursacht?
     – Zu wenig Plattenspeicherplatz
     – Verbindung zur Pipeline unterbrochen
     – Benutzername und Kennwort für diese Datenbank wurden geändert
3. **Pipelines berücksichtigen keine in der Konfigurationskonsole vorgenommenen Konfigurationsänderungen**
   - Pipelines wenden Konfigurationsänderungen erst an, nachdem sie gestoppt und erneut gestartet wurden. Beim Neustart der Pipelines werden die Konfigurationsänderungen im Rahmen des Prozesses zur Initialisierung der Pipelines angewendet.
   - Stoppen Sie nach einer Konfigurationsänderungen alle aktiven Pipelines und starten Sie die Pipelines erneut, um die Datenintegrität sicherzustellen.
4. **Pipeline startet nicht unter AIX**
   - Wurde eine Fehlernachricht angezeigt, dass das abhängige Modul libicuio.a nicht gefunden wurde?
     – Ist dies der Fall, müssen Sie sicherstellen, dass sich die Bibliothek in einem der folgenden Verzeichnisse befindet: `/usr/lib`, `/lib`, `$DB2INSTHOM/sqllib/lib`. Sie können auch das Verzeichnis *`installationsverzeichnis`*`/lib` in der Umgebungsvariablen `LIBPATH` definieren.
   - Überprüfen Sie die Version und Position der C++-Laufzeitbibliotheken. Das Problem könnte durch falsche Einstellungen in der RunTime-Aktualisierung und in der Umgebungsvariablen `LIBPATH` verursacht werden. Lesen Sie die Veröffentlichung „IBM InfoSphere Identity Insight Installation and Configuration Guide" oder die aktuellen Supportinformationen.
5. **Pipeline verarbeitet nur einen Teil eines eingehenden Datensatzes**
   - Überprüfen Sie die BAD-Protokolldatei auf ungültige UMF-Nachrichten. Diese Protokolldatei zeigt den Namen der eingehenden Datenquellendatei an, die verarbeitet wurde.
   - Überprüfen Sie die Registerkarte **UMF-Ausnahmebedingungen** in der Konfigurationskonsole.
6. **Pipelinetransport funktioniert nicht**
   - Stellen Sie sicher, dass die für die Transportmethode verwendete Syntax korrekt ist. Haben Sie zum Beispiel bei der Angabe einer Datenbanktransportmethode Anführungszeichen an der richtigen Stelle eingegeben?

- Handelt es sich um eine Warteschlangentransportmethode: Ist die Nachrichtenwarteschlange vorhanden?
- Handelt es sich um eine Dateitransportmethode: Ist die Datei vorhanden? Befindet sich die Datei in dem Verzeichnis, das in der Transportmethode angegeben ist?

7. **Pipeline lädt Zahlen in Exponentialschreibweise oder Gleitkommazahlen nicht**
   - Dies ist eine bekannte Einschränkung der Pipeline. Ersetzen Sie die Exponentialschreibweise bzw. die Gleitkommazahlen in UMF durch eine Zahl mit Standardschreibweise. Beispiel: `-1.267E-05` wird durch `-0.00001267` ersetzt.
8. **Nach dem Start einer Pipeline wird eine Warnung empfangen, dass keine Routen definiert sind**
   - Hierbei handelt es sich um eine Warnung. Sie können sie ignorieren. (Die Nachricht informiert Sie über die Tatsache, dass für diese Pipeline keine Routen definiert sind. Routen sind für die Ausführung einer Pipeline nicht erforderlich.)

Prüfliste zur Fehlerbehebung für Analyst Toolkit-Webanwendungen

Treten Probleme mit den Webanwendungen auf, prüfen Sie zunächst diese Liste der am häufigsten auftretenden Probleme, bevor Sie sich an den IBM Software Support wenden:

1. Die Anmeldeanzeige der Konfigurationskonsole wird nicht angezeigt
2. Anmeldung an der Konfigurationskonsole nicht möglich
3. Der Bericht wird im Web-Browser geöffnet, der Bericht ist jedoch leer
4. Der Status einer Pipeline wird auf der Registerkarte für den Pipelinestatus nicht angezeigt
5. In der Konfigurationskonsole vorgenommene Änderungen werden von den Pipelines nicht berücksichtigt

1. **Die Anmeldeanzeige wird nicht angezeigt.**
   - Wird eine Nachricht angezeigt, dass die Seite nicht angezeigt werden kann?
     - Wahrscheinlich ist die Webanwendungs-URL falsch. Geben Sie die URL erneut ein. Wenn Sie die korrekte URL nicht kennen, wenden Sie sich an Ihren Systemadministrator oder an die interne technische Unterstützung.
     - Weitere mögliche Ursachen: Der Port, der Ihr System mit dem WebSphere Liberty-Server verbindet, ist möglicherweise blockiert oder der WebSphere Liberty-Server ist möglicherweise nicht gestartet. Bitten Sie den Systemadministrator oder die interne technische Unterstützung um Hilfe.
   - Ist die Anzeige leer?
     - Wenden Sie sich an Ihren Systemadministrator oder an die interne technische Unterstützung. Der Port, der Ihr System mit dem WebSphere Liberty-Server verbindet, ist möglicherweise nicht gestartet oder das Identity Insight-Datenbankkennwort wurde möglicherweise geändert.
   - Lässt sich das Problem durch keine dieser Lösungen beheben, bitten Sie Ihren Systemadministrator oder die interne technische Unterstützung um Hilfe.
2. **Anmeldung an der Webanwendung nicht möglich.**
   - Stellen Sie sicher, dass Sie den korrekten Benutzernamen und das korrekte Kennwort eingeben. Die Analyst Toolkit-Anwendungen sperren Benutzerkonten nicht, auch nicht nach mehreren ungültigen Anmeldeversuchen. Wiederholen Sie daher die Eingabe Ihres Benutzernamens und Ihres Kennworts.

- Haben Sie Ihren Benutzernamen und Ihr Kennwort vergessen, bitten Sie Ihren Systemadministrator oder die interne technische Unterstützung um Hilfe. Möglicherweise muss Ihr Kennwort zurückgesetzt werden.

3. **In der Konfigurationskonsole vorgenommene Änderungen werden von der Pipeline nicht berücksichtigt.**
   - Pipelines wenden Konfigurationsänderungen erst an, nachdem sie gestoppt und erneut gestartet wurden. Beim Neustart der Pipelines werden die Konfigurationsänderungen im Rahmen des Prozesses zur Initialisierung der Pipelines angewendet.
   - Stoppen Sie nach einer Konfigurationsänderungen alle aktiven Pipelines und starten Sie die Pipelines erneut, um die Datenintegrität sicherzustellen.

Prüfliste zur Fehlerbehebung für Visualizer

Treten Probleme mit Visualizer auf, prüfen Sie die folgende Liste der häufigsten Probleme, die bei Verwendung von Visualizer auftreten können, bevor Sie sich an den IBM Support wenden. Sie können Ihr Problem in Visualizer möglicherweise selbst lösen.

1. Visualizer kann nicht gestartet werden
2. Keine Anmeldung an Visualizer möglich
3. Ein Visualizer-Bericht wurde generiert. Der Bericht wird im Web-Browser geöffnet, ist jedoch leer
4. Fehlernachrichten zur Pipeline werden empfangen
5. Visualizer blockiert
6. Die attributbasierte Suche gibt nicht die erwarteten Ergebnisse zurück
7. Beim Suchen über das Fenster 'Attributbasierte Suche' wird eine Fehlernachricht zu 'unzureichenden Indizes' empfangen
8. Die benutzerdefinierten Symbole für die Visualizer-Diagramme werden nicht oder fehlerhaft angezeigt
9. Links (oder Hyperlinks) funktionieren in Visualizer nicht
1. **Visualizer kann nicht gestartet werden**
   - Stellen Sie zunächst sicher, dass auf Ihrem Workstation-Client die erforderliche Clientversion von Java installiert ist.
   - Wenn Sie mehrere Java-Versionen auf Ihrer Clientmaschine installiert haben, handelt es sich bei der Standardsystemversion von Java Web Start wahrscheinlich nicht um die zum Ausführen von Visualizer erforderliche Version. Beachten Sie auch, dass die zum Öffnen und Ausführen von Visualizer erforderliche Java-Version des Clients möglicherweise nicht die neueste auf Ihrer Maschine installierte Java-Version ist. Dieses Problem kann auf zwei Arten gelöst werden: Ordnen Sie in Ihrem Web-Browser die erforderliche Clientversion von Java Web Start zu oder verwenden Sie eine Direktstartmethode.
     – Ist Visualizer die einzige Web Start-Anwendung, die Sie auf diesem Workstation-Client verwenden? Wenn dies der Fall ist, konfigurieren Sie Ihren Web-Browser so, dass der Dateityp JNLP die erforderliche Clientversion von Java Web Start verwendet.
     – Führen Sie auf dieser Workstation neben Visualizer weitere Web Start-Anwendungen aus oder wollen Sie eine Änderung der System- und Java-Einstellungen verhindern? Wenn dies der Fall ist, starten Sie Visualizer direkt über die Java Web Start-Datei.

- Erhalten Sie eine Fehlernachricht, die darüber informiert, dass die Anwendung eine nicht installierte JRE-Version angefordert hat? Wenn dies der Fall ist, konfigurieren Sie Java version 1.6 so, dass automatische Downloads akzeptiert werden.
- Wird die Visualizer Web Start-Seite angezeigt?
  - Ja, die Visualizer Web Start-Seite wird angezeigt. Es wird jedoch eine Nachricht angezeigt, die darüber informiert, dass Java Web Start zum Starten von Visualizer erforderlich ist. Es wird kein Link angezeigt, über den IBM InfoSphere Identity Insight Visualizer gestartet werden kann.
    - Wird nur dieser Workstation-Client für Visualizer verwendet? Wenn dies der Fall ist, konfigurieren Sie Ihren Web-Browser so, dass der Dateityp JNLP die erforderliche Clientversion von Java Web Start verwendet.
    - Verwenden Sie diesen Workstation-Client, um weitere Web Start-Anwendungen zu öffnen oder wollen Sie eine Änderung der System- und Java-Einstellungen vermeiden? Wenn dies der Fall ist, starten Sie Visualizer direkt über die Java Web Start-Datei.
  - Ja, die Visualizer-Startseite und eine Begrüßungsanzeige wurden angezeigt, jedoch kein Visualizer-Anmeldefenster.
    - Haben Sie den Link zum Starten von IBM InfoSphere Identity Insight Visualizer angeklickt?
      - Wenn dies der Fall ist, dann ist Java möglicherweise gerade dabei, Visualizer zu öffnen, was einige Minuten dauern kann. Wenn Visualizer gerade geöffnet wird, sehen Sie in der Regel eine Java-Begrüßungsanzeige oder ein Java Web Start-Fenster.
      - Wenn dies nicht der Fall ist, klicken Sie zum Starten von Visualizer den Link an.
    - Das Problem steht sehr wahrscheinlich mit der integrierten Version von WebSphere Application Server in Zusammenhang. WebSphere Application Server weist einen Fehler oder ein Problem auf und muss möglicherweise erneut gestartet werden oder er kann keine Verbindung zur korrekten Produktdatenbank herstellen. Wenden Sie sich an Ihren Systemadministrator oder an die interne technische Unterstützung.
  - Nein, die Visualizer Web Start-Seite wird nicht angezeigt.
    - Informiert eine Nachricht darüber, dass die Seite nicht angezeigt werden kann, prüfen Sie die Visualizer-URL. Die URL enthält möglicherweise einen Schreibfehler oder ist nicht die für Visualizer korrekte URL. Geben Sie die URL erneut ein. Wenn Sie die Visualizer-URL nicht kennen, wenden Sie sich an Ihren Systemadministrator oder an die interne technische Unterstützung.
    - Ist die URL korrekt, kann die Visualizer Web Start-Seite möglicherweise aus einem der folgenden Gründe nicht angezeigt wird:
      - WebSphere Application Server weist einen Fehler oder ein Problem auf und muss möglicherweise erneut gestartet werden.
      - Der Port, der Ihren Workstation-Client mit WebSphere Application Server verbindet, ist möglicherweise blockiert oder wird bereits von einer anderen Anwendung verwendet.
- Lässt sich das Problem durch keine dieser Maßnahmen beheben, bitten Sie Ihren Systemadministrator oder die interne technische Unterstützung, sich an den IBM Software Support zu wenden.

2. **Keine Anmeldung an Visualizer möglich**
   - Wird die Visualizer-Anmeldeanzeige angezeigt?

– Nein, die Visualizer-Anmeldeanzeige wird nicht angezeigt.
  - Das Problem steht sehr wahrscheinlich mit der integrierten Version von WebSphere Application Server in Zusammenhang. WebSphere Application Server weist einen Fehler oder ein Problem auf (keine Verbindung) oder er kann keine Verbindung zur korrekten Produktdatenbank herstellen. Bitten Sie den Systemadministrator oder die interne technische Unterstützung um Hilfe.
– Ja, der Visualizer-Anmeldebildschirm wird angezeigt, eine Anmeldung ist jedoch nicht möglich.
  - Stellen Sie sicher, dass Sie den korrekten Benutzernamen und das korrekte Kennwort für das Visualizer-Benutzerkonto eingegeben haben. Visualizer sperrt keine Benutzerkonten, auch nicht nach mehreren ungültigen Anmeldeversuchen. Wiederholen Sie daher die Eingabe Ihres Benutzernamens und Ihres Kennworts. Sie können Ihr Benutzerkonto nicht selbst sperren.
  - Klicken Sie **Anmelden** an. Die Schaltfläche **Anmelden** wird nicht automatisch ausgewählt. Wenn Sie Ihren Benutzernamen und Ihr Kennwort eingeben und die **Eingabetaste** drücken, passiert daher nichts. Sie müssen die Schaltfläche **Anmelden** mit der Maus anklicken oder über die Tastatur auswählen.

• Haben Sie Ihren Benutzernamen und Ihr Kennwort vergessen?
  – Ja. Wenden Sie sich an den Systemadministrator oder die interne technische Unterstützung, wenn Sie Ihren Benutzernamen nicht kennen oder Ihr Kennwort für das Visualizer-Benutzerkonto in der Konfigurationskonsole zurücksetzen wollen.

3. **Ein Visualizer-Bericht wurde generiert. Der Bericht wird im Web-Browser geöffnet, ist jedoch leer**
   • Warten Sie noch ein oder zwei Minuten, weil der Bericht möglicherweise noch generiert wird. Wenn das System einen Bericht generiert, beginnt es mit der Anzeige eines leeren Bildschirms im Browser. Sobald der Bericht vollständig generiert und für die Anzeige bereit ist, wird er vom System angezeigt.
   • Stellen Sie sicher, dass auf Ihrem lokalen System Adobe Acrobat Reader ab Version 7.0 installiert ist. Ist dies nicht der Fall, können Sie die aktuelle Version von Adobe Acrobat Reader kostenlos von der Adobe-Website herunterladen.
   • Verfügt Ihr System über eine Firewall? Ist dies der Fall, überprüfen Sie, ob sowohl localhost als auch dem Anwendungsserver der Zugriff über die Firewall gewährt wurde.
4. **Fehlernachrichten zur Pipeline werden empfangen**
   • Lesen Sie die Fehlernachricht aufmerksam, um weitere Informationen zur Ursache des Problems zu erhalten.
   • Stellen Sie sicher, dass die Visualizer-Pipeline eine HTTP-Pipeline ist.
   • Ist auf Ihrer Workstation die Visualizer-Clientprotokollierung aktiviert?
     – Nein.
       - Aktivieren Sie „Aktivieren der Visualizer-Clientprotokollierung" auf Seite 426 auf Ihrer Maschine. Setzen Sie die Protokollebene auf **Debug**. Wenden Sie sich anschließend an Ihren Systemadministrator oder an die interne technische Unterstützung, teilen Sie den Text der Fehlernachricht mit und geben Sie an, dass Sie die Visualizer-Clientprotokollierung aktiviert haben. Möglicherweise werden Sie von Ihrem Systemadminist-

rator oder der internen technischen Unterstützung gebeten, erneut zu versuchen, eine Verbindung zur Pipeline herzustellen und dann die Protokolldatei zu prüfen.
    - Wenn Sie das Problem gelöst haben, inaktivieren Sie die Visualizer-Clientprotokollierung.
  – Ja.
    - Prüfen Sie die Visualizer-Clientprotokolldateien in *installationsverzeichnis*/logs/ewas.
    - Wenden Sie sich an den Systemadministrator oder die interne technische Unterstützung. Ihr Systemadministrator oder die interne technische Unterstützung muss möglicherweise die Visualizer-Clientprotokolldatei prüfen.

5. **Visualizer blockiert**
   - Der Port, der Ihr System mit der integrierten Komponente WebSphere Application Server verbindet, ist möglicherweise blockiert, oder die integrierte Komponente WebSphere Application Server wurde möglicherweise nicht gestartet. Wenden Sie sich an Ihren Systemadministrator oder an die interne technische Unterstützung.
   - Informationen für Datenbankadministratoren, Systemadministratoren und die interne technische Unterstützung:
     – Erwägen Sie die Ausführung von Statistiken für die Tabellen der Entitätendatenbank, die Visualizer beeinflussen.
     – Tritt diese 'Blockierung' von Visualizer bei allen Visualizer-Benutzern auf, überprüfen Sie, ob die Indizes der Datenbanktabellen geändert wurden. Eine Änderung der Indizes der Datenbanktabellen kann unvorhersehbare und unerwünschte Folgen haben. Wenn Sie feststellen, dass die Indizes geändert wurden, wenden Sie sich an den IBM Software Support.
6. **Die attributbasierte Suche gibt nicht die erwarteten Ergebnisse zurück.**
   - Überprüfen Sie Ihre Suchkriterien.
     – Wenn weniger Ergebnisse als erwartet angezeigt werden, müssen Sie die Kriterien möglicherweise vereinfachen.
     – Wenn mehr Ergebnisse als erwartet angezeigt werden, müssen Sie die Suchkriterien möglicherweise eingrenzen.
     – Das System gibt standardmäßig nur maximal 1000 Datensätze pro Suche zurück. (Diese Einstellung ist jedoch konfigurierbar). Sie wird über den Parameter MAX_ENTITIES_RETURNED auf der Registerkarte **Systemparameter** der Konfigurationskonsole gesteuert. Sie sollten Ihren Systemadministrator oder die interne technische Unterstützung kontaktieren, um diese Einstellung zu prüfen oder zu ändern.)
   - Dieses Problem kann mit der Datenbankkonfiguration hinsichtlich der Groß-/Kleinschreibung zusammenhängen. Kontaktieren Sie Ihren Systemadministrator oder die interne technische Unterstützung, um die Datenbankkonfiguration hinsichtlich der Einstellungen für die Groß-/Kleinschreibung zu überprüfen.
     – Bei DB2-Datenbanken: Der Datenbankadministrator, Systemadministrator oder die interne technische Unterstützung muss möglicherweise ein Script anwenden, damit Datenbanksuchen unterstützt werden, bei denen nicht zwischen Groß-/Kleinschreibung unterschieden wird. Fordern Sie Ihren Systemadministrator auf, den IBM Software Support zu kontaktieren, um das Script und die Anleitungen zu dessen Ausführung zu erhalten.
     – Bei Microsoft SQL Server-Datenbanken: Für die Datenbank kann festgelegt werden, dass die Groß-/Kleinschreibung beachtet werden muss. Der Da-

tenbankadministrator, Systemadministrator oder die interne technische Unterstützung muss möglicherweise die Einstellung für die Groß-/Kleinschreibung für die Datenbank ändern.

– Bei Oracle-Datenbanken: Der Datenbankadministrator, Systemadministrator oder die interne technische Unterstützung muss möglicherweise funktionsbasierte Indizes mit UPPER erstellen, damit Datenbanksuchen unterstützt werden, bei denen nicht zwischen Groß-/Kleinschreibung unterschieden wird.

7. **Beim Suchen über das Fenster 'Attributbasierte Suche' wird eine Fehlernachricht zu 'unzureichenden Indizes' empfangen**
   - Sie versuchen, eine Suche für ein Feld auszuführen, das nicht indiziert ist.
     – Versuchen Sie, die Suche einzugrenzen, indem Sie zusätzliche Suchkriterien eingeben.
     – Sie können sich auch an Ihren Systemadministrator oder die interne technische Unterstützung wenden. Je nach dem, welche Auswirkungen dies auf die Systemleistung hat, ist zu empfehlen, dass Ihr Systemadministrator einen Index für dieses Feld erstellt. (Ihr Systemadministrator oder die technische Unterstützung prüft möglicherweise auch den Parameter `ENABLE_SEARCH_INDEX_CHECK` auf der Registerkarte **Systemparameter** in der Konfigurationskonsole. Ist dieser Parameter nicht auf 1 gesetzt, kann sich dies auf die Systemleistung auswirken.)
8. **Die benutzerdefinierten Symbole für die Visualizer-Diagramme werden nicht oder fehlerhaft angezeigt**
   - Die Symbole befinden sich möglicherweise nicht im korrekten Verzeichnis auf dem Anwendungsserver. Kontaktieren Sie Ihren Systemadministrator oder die interne technische Unterstützung, um die Pfadposition der angepassten Diagrammsymbole zu überprüfen.
   - Die Symbolnamen weisen möglicherweise eine gemischte Groß-/Kleinschreibung anstatt reiner Kleinschreibung auf oder stimmen nicht mit dem entsprechenden Attributtyp überein. Ist beispielsweise **`neues foto`** der Name des Attributtyps, muss der Bilddateiname komplett aus Kleinbuchstaben bestehen und ein Leerzeichen zwischen den Wörtern `neues` und `foto` enthalten. Der Dateiname muss wie folgt lauten: **`neues foto.gif`**. Kontaktieren Sie Ihren Systemadministrator oder die interne technische Unterstützung, um sicherzustellen, dass der Symboldateiname korrekt ist.
   - Die Symbole weisen möglicherweise nicht das empfohlene GIF-Dateiformat auf. Möglicherweise weisen die Symbole jedoch auch nicht die empfohlene Größe von 24 x 24 Pixel auf. Kontaktieren Sie Ihren Systemadministrator oder die interne technische Unterstützung, um sicherzustellen, dass das Symbol das korrekte Dateiformat aufweist und die empfohlene Bildgröße verwendet.
9. **Links (oder Hyperlinks) funktionieren in Visualizer nicht. Beim Anklicken eines Attributlinks wird eine Fehlernachricht angezeigt.**
   - Konfigurieren Sie die Hyperlinkeinstellungen für Ihre Workstation. Wählen Sie in den Visualizer-Systemvorgaben den Web-Browser oder das Programm aus zum Öffnen der Dateien aus, die den den Identitätsdatensatzattributen zugeordnet sind. Diese Einstellung muss für jede Workstation konfiguriert sein, auf der Visualizer ausgeführt wird.
   - Stellen Sie nach dem Konfigurieren der Hyperlinkeinstellungen sicher, dass Sie Visualizer schließen und erneut starten.

Systemzustand

Dieser Abschnitt enthält einige Tipps für Datenbank- und Systemadministratoren zur Aufrechterhaltung des guten Systemzustands von IBM InfoSphere Identity Insight.

Tipps zur Leistung

Wenn Sie eine Verschlechterung der Leistung des gesamten Systems feststellen, ermitteln Sie anhand dieser Liste die möglichen Ursachen:

- Datenbankoptimierung: Wann wurden zuletzt Datenbankstatistiken für IBM InfoSphere Identity Insight-Tabellen ausgeführt?
- Sehr große Entitäten: Verfügt die Entitätendatenbank über sehr große Entitäten, d. h. Entitäten mit einer Vielzahl Identitäten?

Diese Liste ist nicht vollständig, bietet jedoch einen Ausgangspunkt, um die optimale Leistung des Systems sicherzustellen.

Tipps zur Überwachung der Entitätendatenbank

Nachfolgend sind einige spezifische Elemente aufgeführt, die beim Überwachen des ordnungsgemäßen Betriebs der Entitätendatenbank geprüft werden sollten:

- Datenbankoptimierung: Welcher Zeitplan gilt für das Ausführen von Datenbankstatistiken für IBM InfoSphere Identity Insight-Tabellen?
- Eindeutige Nummern: Enthält die Entitätendatenbank mehrere Entitäten, die dieselbe eindeutige Nummer gemeinsam nutzen?
- Entitäten: Enthält die Entitätendatenbank Entitäten mit vielen eindeutigen Nummern?
- Überauflösung: Enthält die Entitätendatenbank sehr große Entitäten, d. h. Entitäten mit einer Vielzahl Identitäten?

Diese Liste ist nicht vollständig, bietet jedoch einige Kurztipps zur Überwachung des Zustands des gesamten Systems.

Datenbanktabellen mit Auswirkung auf die Systemleistung

Wenn das System langsam zu sein scheint, können die Datenbankadministratoren Datenbankstatistiken für mehrere Tabellen in der Entitätendatenbank ausführen, um sowohl die Pipelineleistung als auch die Funktionalität für den Visualizer-Benutzer zu verbessern.

Pipelinetabellen

Wenn eine langsame Pipelineleistung vorzuliegen scheint, versuchen Sie, Datenbankstatistiken für die folgenden Tabellen der Entitätendatenbank auszuführen:

- DQM_NAME_DICT
- NAME
- ADDRESS
- NUMS
- ATTRIBUTES
- EMAIL_ADDR
- DSRC_ACCT
- SEP_RELATIONS
- SEP_ROLES

- ENTITY
- DISCLOSED_RELATIONS
- UMF_LOG
- UMF_EXCEPT

Visualizer-Tabellen

Wenn Visualizer-Benutzer eine schlechte Visualizer-Leistung bemerken, versuchen Sie, Datenbankstatistiken für die folgenden Tabellen der Entitätendatenbank auszuführen:

- ER_ENTITY_SCORE
- ER_HISTORY
- ER_RELOCATION
- ER_DETAIL
- ER_ACCT_SCORE
- ER_ENTITY_STATE
- ER_FORCED_LOG
- SEP_CONFLICT
- SEP_CONFLICT_REL
- SEARCH
- APP_ACTIVITY_CODES
- APP_ACTIVITY_HISTORY
- APP_CONFLICT_GROUP
- APP_INBOX
- APP_ROLE
- APP_SEND
- MATCH_MERGE_RULES
- CONFLICT_RULES

Darüber hinaus sollten Datenbankadministratoren auch Datenbankstatistiken für die im Bereich der Pipelinetabellen aufgelisteten Datenbanktabellen ausführen, da Visualizer auch eine Hintergrundpipeline verwendet, um mehrere Visualizer-Tasks auszuführen (beispielsweise Hinzufügen von Entitäten, Suchen von Entitäten nach Entitätsauflösung und Offenlegen von Beziehungen).

Abfrage großer Entitäten

Diese SQL-Abfrage sucht nach großen Entitäten. Je mehr Identitätsdatensätze eine Entität enthält, desto größer ist sie. Manchmal können die Ergebnisse der Verarbeitung eingehender Identitätsdaten während der Entitäts- und Beziehungsauflösung eine Überauflösung von Identitätsdatensätzen auf dem System verursachen. Große Entitäten können zu einer deutlichen Verschlechterung der Systemleistung führen.

SQL-Anweisung zum Abfragen großer Entitäten

```
select entity_id
  count(dsrc_acct) as IDENTITY_CNT
from
 DSRC_ACCT
where
 sys_delete_dt is null
```

```
group by
 entity_id
count(dsrc_acct) > 100
order by count(dsrc_acct)desc;
```

Wie geht es weiter?

Verwenden Sie im Identity Insight-Plug-in für i2 oder im Explorer die Anzeige für die Suche nach Entitäts-ID, um nach den Entitäts-IDs zu suchen, die von den Ergebnissen der Abfrage großer Entitäten zurückgegeben wurden: Prüfen Sie, ob die zu dieser Entität gehörenden Identitäten ordnungsgemäß zugeordnet wurden. Eine ordnungsgemäß erstellte Entität weist viele verschiedene Datenquellenbenutzerkonten auf, wobei die Mehrheit der Daten für zugeordnete Namen, Adressen und Nummern eine große Ähnlichkeit aufweist. Wenn Sie nicht sicher sind, wie Sie die ordnungsgemäße Erstellung der Entität prüfen können, wenden Sie sich an den IBM Kundendienst oder an den IBM Support.

Beispielergebnisse der Abfrage großer Entitäten

Es folgt ein Beispiel für die Ergebnisse einer Abfrage großer Entitäten:

ENTITY_ID	IDENTITY_CNT
3015	22
5241	41
7854	36

Abfrage der Gesamtzahl eindeutiger Nummern nach Entität

Diese Abfrage gibt Informationen dazu zurück, wie viele verschiedene eindeutige Nummern einer bestimmten Entität nach Entitäts-ID zugeordnet sind. Diese Abfrage kann hilfreich sein, wenn jede Entität wie üblich nur eine eindeutige Nummer hat. Die Überprüfung der Entitäten auf viele verschiedene Typen eindeutiger Nummern bietet eine hervorragende Möglichkeit, um Datenanomalien festzustellen und um sicherzustellen, dass Ihre Auflösungsregeln wie erwartet funktionieren.

SQL-Anweisung zum Abfragen der Gesamtzahl eindeutiger Nummern, die einer einzelnen Entität zugeordnet sind

```
select distinct *
from
  (select entity_id,
    (select count(distinct num_value)
  from
   nums,
   num_type
  Where
   nums.num_type_id=num.type.num_type_id
   and num_type.unique_FLAG='Y'
   and nums.entity_id=dsrc_acct.entity_id
    ) as UNIQUE_NUMBER_CNT
 from dscr_acct
  )as tab1
where
 UNIQUE_NUMBER_CNT>1
order by
  UNIQUE_NUMBER_CNT DESC;
```

Wie geht es weiter?

Verwenden Sie im Identity Insight-Plug-in für i2 oder im Explorer die Anzeige für die Suche nach Entitäts-ID, um nach den Entitäts-IDs zu suchen, die von den Ergebnissen der Abfrage der Gesamtzahl eindeutiger Nummern nach Entitäts-ID zurückgegeben wurden. Durch Überprüfen der Entitätszusammenfassung für jede Entität können Sie ermitteln, ob die Entität mehr als eine eindeutige Nummer aufweisen darf. In bestimmten Fällen ist diese Situation möglicherweise ein Hinweis auf Betrug. In den Vereinigten Staaten beispielsweise sind die Sozialversicherungsnummern eindeutige Nummern. In der Regel weist jede US-Entität nur eine Sozialversicherungsnummer auf. Wenn bei dieser Abfrage eine Entität mit mehreren Sozialversicherungsnummern festgestellt wird, folgt als nächster Schritt wahrscheinlich eine weitere Untersuchung und Analyse, um die Ursache für das Vorliegen mehrerer Sozialversicherungsnummern zu ermitteln.

Beispielergebnisse der Abfrage der Gesamtzahl eindeutiger Nummern nach Entität

Es folgt ein Beispiel für die Ergebnisse einer Abfrage der Gesamtzahl eindeutiger Nummern nach Entität:

ENTITY_ID	UNIQUE_NUMBER_CNT
3003	2
3030	2
3039	2

Abfrage eindeutiger Nummern, die von mehreren Entitäten gemeinsam genutzt werden

Eindeutige Nummern sind Nummern, die in der Regel nur zu einer Entität gehören und nicht von mehreren Entitäten gemeinsam genutzt werden. Die Überprüfung, ob mehrere Entitäten dieselben eindeutigen Nummern gemeinsam nutzen, bietet eine hervorragende Möglichkeit, um Datenanomalien festzustellen und um sicherzustellen, dass Ihre Auflösungsregeln wie erwartet funktionieren. Sie können die Abfrage eindeutiger Nummern, die von mehreren Entitäten gemeinsam genutzt werden, verwenden, um Entitäten zu ermitteln, die dieselbe eindeutige Nummer gemeinsam nutzen. Bei der Abfrage wird jede eindeutige Nummer für eine einzelne Entität nur einmal gezählt, ungeachtet dessen, wie viele Identitätsdatensätze für diese Entität dieselbe eindeutige Nummer enthalten.

SQL-Anweisung zum Abfragen eindeutiger Nummern, die von mehreren Entitäten gemeinsam genutzt werden

```
select num_type,
 num_value,
  count(distinct ENTITY_ID) as cnt
from nums,
 num_type
Where   nums.num_type_id=num_type.num_type_id
 and num_type.unique_FLAG='Y'
Group by
 num_type
 num_value
Having
  count(distinct ENTITY_ID)>1
Order by
  count(distinct ENTITY_ID)desc;
```

Wie geht es weiter?

Verwenden Sie im Identity Insight-Plug-in für i2 oder im Explorer die Anzeige für die Suche nach Attributen, um nach allen Nummern zu suchen, die von der SQL-Abfrage eindeutiger Nummern, die von mehreren Entitäten gemeinsam genutzt werden, zurückgegeben werden. Prüfen Sie im Teilfenster **Ergebnisse** die Entitätsinformationen für jede Entität, die dieselbe eindeutige Nummer nutzt. Sie können auch die Entitätszusammenfassungen dieser Entitäten prüfen, um zu ermitteln, warum die Entitäten dieselbe eindeutige Nummer gemeinsam nutzen.

Möglicherweise erkennen Sie basierend auf der eindeutigen Nummer interessante Beziehungen zwischen Entitäten. Sie könnten beispielsweise feststellen, dass zwei unterschiedliche Entitäten dieselbe Sozialversicherungsnummer verwenden.

Möglicherweise stellen Sie auch ein Problem bei der UMF-Codierung für eindeutige Nummern fest. Sie könnten auch feststellen, dass zwei Entitäten dieselbe Passnummer gemeinsam nutzen, da der eingehende UMF-Identitätsdatensatz zum Angeben des Landes (Ort), das die Passnummer ausgegeben hat, nicht NUM_LOC verwendet hat. Nummern von Pässen und Führerscheinen sind nur an einem bestimmten Ort, d. h. in einem Land oder Staat, eindeutig. Losgelöst von diesem Kontext garantieren diese Nummern keine absolute Eindeutigkeit.

Beispielergebnisse der Abfrage eindeutiger Nummern, die von mehreren Entitäten gemeinsam genutzt werden

Es folgt ein Beispiel für die Ergebnisse einer Abfrage eindeutiger Nummern, die von mehreren Entitäten gemeinsam genutzt werden:

NUM_TYPE	NUM_VALUE	cnt
SSN	000-00-0000	9
SSN	111-11-1111	9
SSN	555-55-5555	5
SSN	611-00-6666	2
SSN	999-99-9999	3

Durchsuchen von Wissensbasen

Sie können häufig Lösungen für Probleme finden, indem Sie die IBM Wissensbasen durchsuchen. In diesem Abschnitt wird beschrieben, wie Sie Ihre Ergebnisse durch die Verwendung verfügbarer Ressourcen, Unterstützungstools und Suchmethoden optimieren können.

Verfügbare technische Ressourcen

Zusätzlich zu diesem Information Center helfen Ihnen die folgenden technischen Hinweise bei der Beantwortung Ihrer Fragen und der Behebung von Problemen:

Technische Hinweise zu IBM InfoSphere Identity Insight unter www.ibm.com/software/support/isa/

Suchen mit Unterstützungstools

Die folgenden Desktop-Tools sind zum Durchsuchen von IBM Wissensbasen verfügbar:

- **IBM Support Assistant (ISA)** ist eine kostenlose Software-Service-Workbench, die Sie bei Fragen und Problemen mit IBM Softwareprodukten unterstützt. Anweisungen zum Herunterladen und Installieren von ISA finden Sie auf der ISA-Website unter www.ibm.com/software/support/isa/.
- **IBM Software Support Toolbar** ist ein Browser-Plug-in, das einen Mechanismus zum einfachen Durchsuchen von IBM Unterstützungssites bereitstellt. Sie können die Symbolleiste von der Website www.ibm.com/software/support/toolbar/ herunterladen.

Suchtipps

Die folgenden Ressourcen beschreiben, wie Sie Ihre Suchergebnisse optimieren können:

- Durchsuchen der Website des IBM Support
- Verwenden der Google-Suchmaschine

Empfangen von automatischen Aktualisierungen

- **My support**. Führen Sie die folgenden Schritte aus, um wöchentlich E-Mail-Benachrichtigungen zu Programmkorrekturen und anderen Unterstützungsneuigkeiten zu empfangen:
  1. Gehen Sie zur Website des IBM Software Support unter www.ibm.com/software/support/.
  2. Klicken Sie **My support** oben rechts auf der Seite unter **Personalized support** an.
  3. Wenn Sie bereits für Unterstützung registriert sind, melden Sie sich an und springen Sie zum nächsten Schritt. Wenn Sie noch nicht registriert sind, klicken Sie **register now** an. Füllen Sie das Registrierungsformular aus. Verwenden Sie dabei Ihre E-Mail-Adresse als Ihre IBM ID und klicken Sie **Submit** an.
  4. Klicken Sie **Edit profile** an.
  5. Wählen Sie in **Products list** die Option **Software** aus. Es wird eine zweite Liste angezeigt.
  6. Wählen Sie in der zweiten Liste ein Produktsegment aus, z. B. **Systems management**. Es wird eine dritte Liste angezeigt.
  7. Wählen Sie in der dritten Liste ein Produktteilsegment aus, z. B. **Application Performance & Availability**. Es wird eine Liste zutreffender Produkte angezeigt.
  8. Wählen Sie die Produkte aus, für Sie Aktualisierungen empfangen wollen.
  9. Klicken Sie **Add products** an.
  10. Klicken Sie nach der Auswahl aller Produkt, die für Sie von Interesse sind, **Subscribe to email** auf der Registerkarte **Edit profile** an.
  11. Wählen Sie **Please send these documents by weekly email** aus.
  12. Aktualisieren Sie Ihre E-Mail-Adresse bei Bedarf.
  13. Wählen Sie in **Documents list** die Option **Software** aus.
  14. Wählen Sie die Arten von Dokumenten aus, zu denen Sie Informationen empfangen wollen.
  15. Klicken Sie **Update** an.

Nachrichtenübersicht

Wenn Sie eine Nachricht von einer Systemkomponente empfangen, können Sie das Problem häufig beheben, indem Sie den gesamten Nachrichtentext lesen und die zugehörigen Wiederherstellungsmaßnahmen ergreifen.

Nachrichten-IDs sind 10 Zeichen lang und die Zeichen in der Nachrichten-ID stellen weitere Informationen zur Nachricht bereit.

- Die ersten drei Zeichen geben das Produkt an.
  - **CWU** ist die Produkt-ID für IBM InfoSphere Identity Insight.
- Die nächsten beiden Zeichen geben die bestimmte Komponente in dem Produkt an, die die Nachricht generiert.
  - **AE** ist die Komponentenkennung für die Pipeline.
  - **AI** ist die Komponentenkennung für die Konfigurationskonsole.
  - **AK** ist die Komponentenkennung für den Ereignismanager.
  - **AL** ist die Komponentenkennung für Web-Services.
- Die nächsten vier Zeichen sind die Nachrichtennummer.
- Das letzte Zeichen ist der Nachrichtentypcode, der die Wertigkeit der Nachricht beschreibt:
  - **E** (Error) gibt eine Fehlernachricht an. Dieser Nachrichtentyp gibt ein Problem mit einer bestimmten Produktkomponente an, das eine unmittelbare Maßnahme erfordert. Prüfen Sie die Komponentenprotokolldateien auf Informationen, die Ihnen beim Beheben des Fehlers behilflich sein können.
  - **I** gibt eine Informationsnachricht an. Dieser Nachrichtentyp erfordert keine unmittelbare Maßnahme, aber es empfiehlt sich, die Komponentenprotokolldateien auf weitere Informationen zu überprüfen.
  - **W** gibt eine Warnung an. Dieser Nachrichtentyp gibt an, dass eine Bedingung aufgetreten ist, für die eventuell eine Maßnahme erforderlich ist. Überprüfen Sie die Komponentenprotokolldateien auf weitere Informationen zur Warnbedingung und zur Behebung der Bedingung.

Nachrichtenbeispiele

Wenn Sie eine Nachricht mit der Nachrichten-ID CWUAE0001E empfangen, gibt diese eine Fehlernachricht von einer Pipeline an, die sehr wahrscheinlich die Pipeline beendet und die Verarbeitung gestoppt hat. Überprüfen Sie die Pipelineprotokolldateien, um das Problem zu beheben, damit Sie die Pipeline erneut starten können.

Wenn Sie eine Nachricht mit der Nachrichten-ID CWUAE325W empfangen, gibt diese an, dass in der Pipeline eine Warnung aufgetreten ist, die jedoch die weitere Verarbeitung eingehender Datensätze durch die Pipeline nicht gestoppt hat. Sie können die Pipelineprotokolldateien auf weitere Informationen zur Warnung prüfen, beispielsweise auf Maßnahmen, die Sie ergreifen müssen, um das Problem oder den eingehenden Datensatz zu korrigieren. Wenn diese bestimmte Pipeline vom Anwendungsmonitor überwacht wird, können Sie auch die Anwendungsmonitorfenster in der Konfigurationskonsole auf weitere Informationen prüfen.

UMF-Parsing-Fehler

UMF-Parsing-Fehler treten auf, wenn eingehende UMF-Identitätssätze falsch formatiert (z. B. ein fehlender Endtag) sind oder wenn das UMF ungültige Zeichen enthält.

Tabelle 37. UMF-Parsing-Fehler

UMF-Fehlercode	Codebeschreibung	Fehlerkategorie
005	Im Tagnamen *zeichenfolge* sind führende Leerzeichen nicht zulässig	Schwerwiegend
010	Im Anfangstag der Rootebene fehlt <*zeichenfolge*>	Schwerwiegend
015	Unerwarteten Endetag </*zeichenfolge*> festgestellt.	Schwerwiegend
020	Falschen Abschlusstag </*zeichenfolge*> festgestellt, </*zeichenfolge*> erwartet.	Schwerwiegend
025	Dokument ist unvollständig, nicht genügend Endetags vorhanden... Letztes Segment: <*zeichenfolge*>.	Schwerwiegend
030	Dokument ist leer.	Warnung
035	Wenn Kinder vorhanden, dürfen Segmente nicht die Tagdaten '*zeichenfolge*' enthalten.	Schwerwiegend

Protokolle

IBM InfoSphere Identity Insight enthält Protokollierungsmechanismen, die Informationen in eine Reihe von Protokolldateien schreiben. In der Regel schreibt das System Informationen in die Protokolldateien, wenn eine bestimmte Systemkomponente eine qualifizierende Bedingung erfüllt (z. B. das Installieren oder Starten der Komponente), wenn ein Benutzer sich an der Komponente anmeldet oder wenn während der Verarbeitung ein Fehler auftritt.

Protokolldateien werden von den folgenden Systemkomponenten erstellt:

- Pipelines
- Analyst Toolkit-Webanwendungen
- Web-Services
- Ereignismanager

Pipelineprotokolldateien

Sobald Sie eine Pipeline starten, beginnt das System automatisch mit der Protokollierung. Als Basis dient die aktuelle Pipelineprotokollierungskonfiguration in der Pipelinekonfigurationsdatei. Protokolldateien werden für jede Pipeline, nach Pipelinenamen, erstellt, auch wenn Sie mehrere Pipelines mit derselben Konfigurationsdatei gestartet haben.

Typen der Pipelineprotokolldateien

Alle Pipelineprotokolldateien werden standardmäßig in das Verzeichnis auf dem Pipelineknoten geschrieben, in dem die Pipeline gestartet wurde. Es gibt verschiedene Typen der Pipelineprotokolldateien. Welche Nachricht in welcher Datei protokolliert wird, ist von dem Modus abhängig, in dem die Pipeline gestartet wurde (Debugmodus `-d` oder Dämon-/Dienstmodus `-s`), von dem Typ der protokollierten Nachricht und von der aktuellen Protokollierungskonfiguration.

Tabelle 38. Pipelineprotokolldateien nach Nachrichtentyp, Protokolldateiname und Protokollierungsmodi

Nachrichtentyp	Protokolldateiname	Aktion	Protokollmodus/ -modi
Fehlernachrichten	*pipelinename*.err Protokolliert in der Pipeline auftretende kritische Fehler.	Korrigieren Sie nach der Überprüfung der Protokolldateien die Fehler oder Probleme, die für die Pipeline angegeben sind.	Service Debug
SQL-Fehlernachrichten	*pipelinename*.SqlErr.log Protokolliert in der Pipeline auftretende SQL-Fehler. Die Größe dieser Datei ist auf 1 Megabyte begrenzt. Wenn die Datei diese Größenbegrenzung erreicht, archiviert das System die aktuelle Protokolldatei automatisch und erstellt eine neue.	Korrigieren Sie nach der Überprüfung dieser Protokolldatei die angegebenen SQL-Fehler oder -Probleme.	Service Debug
Warteschlangenfehler	*pipelinename*.MQErr.log Protokolliert Warteschlangenfehler.	Korrigieren Sie nach der Überprüfung dieser Protokolldatei die angegebenen MQ-Fehler oder -Probleme.	
Windows-Ereignisanzeige	(Nur Microsoft Windows-Plattformen) Sind für die Pipeline Services installiert und wurde die Pipeline im Servicemodus (Dienstmodus) (Pipelineoption `-s`) gestartet, sendet die Pipeline Fehler- und wichtige Nachrichten auch an die Windows-Ereignisanzeige.	Überwachen Sie die Nachrichten in der Windows-Ereignisanzeige und korrigieren Sie alle angegebenen Fehler oder Probleme.	Service (nur Microsoft Windows-Plattformen)
Nachrichten für fehlerhaftes/ ungültiges UMF, das nicht verarbeitet werden konnte	*pipelinename*.bad Protokolliert Informationen zu Datensätzen in der eingehenden Datenquellendatei, die fehlerhaftes oder ungültiges UMF enthalten. Die Pipeline konnte den Abschnitt des Datensatzes, der dieses fehlerhafte oder ungültige UMF enthält, nicht verarbeiten. Das heißt, dass die Pipeline gelegentlich Teilsätze verarbeitet.	Korrigieren Sie nach der Überprüfung dieser Protokolldatei die Datensätze in der eingehenden Datenquellendatei, die fehlerhaftes oder ungültiges UMF enthalten. Senden Sie dann die korrigierten Datensätze zur Verarbeitung zurück durch eine Pipeline.	Service Debug

Tabelle 38. Pipelineprotokolldateien nach Nachrichtentyp, Protokolldateiname und Protokollierungsmodi (Forts.)

Nachrichtentyp	Protokolldateiname	Aktion	Protokollmodus/ -modi
UMF-Nachrichten, die Ausnahmebedingungen generierten	*pipelinename*.msg Protokolliert Informationen zu Datensätzen in der eingehenden Datenquellendatei, die generierte Ausnahmebedingungen während der Verarbeitung enthalten. Die Pipeline hat den Datensatz verarbeitet. Dieser Nachrichtentyp kann ein Problem mit der Datenqualität für diese Datenquellendatei anzeigen.	Nach der Überprüfung dieser Protokolldatei müssen Sie unter Umständen trotzdem Datensätze in der eingehenden Datenquellendatei korrigieren, die die UMF-Ausnahmebedingung generiert haben. Senden Sie dann die korrigierten Datensätze zur Verarbeitung zurück durch eine Pipeline. Weitere Informationen finden Sie auch im **Laden – Ergebnisbericht** und im **Datenquelle - Ergebnisbericht**.	Service Debug
Tracefunktion für die Fehlerbehebung	Protokolliert Informationen der Tracefunktion für die Fehlerbehebung, wenn eine Pipeline im Debugmodus (Pipelineoption `-d`) gestartet wurde. Es gibt keine Protokolldatei. Die Pipeline wird im Vordergrund ausgeführt und die Ausgabenachrichten werden direkt an die Befehlsshell gesendet. Sie können mit der Umleitungsfunktion eine Datei aus der Pipelinebefehlsausgabe erstellen: `pipeline -d -f my_umf.xml > my_log_file.log`		Debug
SQL-Anweisungen und Leistungsstatistik	*pipelinename*.SqlDebug.log Protokolliert SQL-Anweisungen und Leistungsstatistikdaten, die für die Fehlerbehebung und die Leistungsüberwachung nützlich sein können. Die Größe dieser Datei ist auf 48 Megabyte begrenzt. Wenn eine Datei die Größenbegrenzung erreicht, archiviert das System die aktuelle Protokolldatei automatisch und erstellt eine neue Protokolldatei.		Debug
Pipeline wird während der Verarbeitung einer Datei beendet	*pipelinename*.cnt Während die Pipeline eingehende Datensätze verarbeitet, protokolliert sie den Namen der verarbeiteten Datenquellendatei sowie eine Satzzählung für jeweils 100 Datensätze in der Datei, die erfolgreich verarbeitet wurden. Wird eine Pipeline während der Verarbeitung einer eingehenden Datenquellendatei beendet, kann Ihnen diese Datei dabei helfen zu bestimmen, welche der Datensätze in der Datenquellendatei zur Verarbeitung erneut in die Pipeline geladen werden müssen.	Nach der Überprüfung dieser Protokolldatei und Behebung des Fehlers, der die Beendigung der Pipeline verursachte, laden Sie die nicht verarbeiteten Datensätze zur Verarbeitung erneut in die Pipeline.	Datei

Pipelineprotokollierungskonfigurationen

IBM InfoSphere Identity Insight verfügt über eine Standardprotokollierungskonfiguration, die Pipelineereignisse und -fehler protokolliert. Diese Standardprotokollierungskonfiguration wird automatisch verwendet, wenn keine benutzerdefinierte Pipelineprotokollierungskonfiguration in der Pipelinekonfigurationsdatei angegeben wird.

Zum Starten von Pipelines gibt es zwei primäre Arten: Debugmodus (Pipelineoption `-d`) oder Service-/Dämonmodus (Pipelineoption `-s`).

- Der Debugmodus wird zum Testen und zur Fehlerbehebung des Systems verwendet. Er wird normalerweise nicht in Produktionsumgebungen verwendet. Die Protokollierung im Debugmodus enthält mehr Trace- und Pipelineverarbeitungsinformationen.
- Service-/Dämonmodus ist der normale Modus für die Produktionsumgebung. Die Protokollierung im Service-/Dämonmodus ist normalerweise auf Fehler und Probleme beschränkt, die eine Maßnahme erfordern.

In allen Pipelineprotokollierungskonfigurationen (Standard und benutzerdefiniert) muss angegeben werden, wie Pipelineereignisse im Debugmodus und im Service-/Dämonmodus protokolliert werden sollen. Erfüllt die Standardprotokollierungskonfiguration Ihre Anforderungen nicht, können Sie eine benutzerdefinierte Protokollierungskonfiguration erstellen. Hierfür fügen Sie einen Protokollierungsabschnitt in die Pipelinekonfigurationsdatei ein und geben mithilfe der Pipelinekonfigurationskomponenten an, wie das System Pipelineereignisse und -fehler im Debugmodus und im Service-/Dämonmodus der Pipeline protokolliert.

Standardprotokollierungskonfiguration im Debugmodus

```
console://stdout $NODE_NAME.*;*.CRIT;*.ERR;*.NOTE
 cmeadmin:/// *.CRIT;*.ERR file://./$NODE_NAME.err *.CRIT
 file://./$NODE_NAME.SqlDebug.log?rotateSize=49152 sql.DBUG;sql.PERF
 file://./$NODE_NAME.SqlErr.log?rotateSize=1024 sql.ERR;sql.CRIT
 file://./$NODE_NAME.MQErr.log mq.!DBUG
 file://./$NODE_NAME.bad?style=bare bad_xml.*
 file://./$NODE_NAME.msg?style=bare msg.*
```

Standardprotokollierungskonfiguration im Microsoft Windows-Servicemodus

```
eventlog://./ *.NOTE;*.CRIT;*.ERR
 cmeadmin:/// *.CRIT;*.ERR file://./$NODE_NAME.err *.CRIT
 file://./$NODE_NAME.SqlDebug.log?rotateSize=49152 sql.DBUG;sql.PERF
 file://./$NODE_NAME.SqlErr.log?rotateSize=1024 sql.ERR;sql.CRIT
 file://./$NODE_NAME.MQErr.log mq.!DBUG
 file://./$NODE_NAME.bad?style=bare bad_xml.*
 file://./$NODE_NAME.msg?style=bare msg.*
```

Standardprotokollierungskonfiguration im UNIX-Dämonmodus

```
file://./$NODE_NAME.log *.CRIT;*.ERR;*.NOTE;*.INFO;logger.!DBUG
 cmeadmin:/// *.CRIT;*.ERR file://./$NODE_NAME.err *.CRIT
 file://./$NODE_NAME.SqlDebug.log?rotateSize=49152 sql.DBUG;sql.PERF
 file://./$NODE_NAME.SqlErr.log?rotateSize=1024 sql.ERR;sql.CRIT
 file://./$NODE_NAME.MQErr.log mq.!DBUG
 file://./$NODE_NAME.bad?style=bare bad_xml.*
 file://./$NODE_NAME.msg?style=bare msg.*
```

Pipelineprotokollierungskomponenten

Pipelineprotokollierungskomponenten erleichtern die Erstellung von angepassten Pipelineprotokollierungskonfigurationen. Sie liefern dem System Anweisungen zum Protokollieren von Pipelineereignissen und -nachrichten.

Protokollausgabeprogramm
Gibt an, welches Protokollausgabeprogramm zum Schreiben oder Anzeigen der Protokolldatei verwendet werden soll:

file Die Protokollereignisse und -nachrichten werden in eine angegebene Datei geschrieben.

Das Protokollausgabeprogramm file verwendet die Protokollierungskomponenten Pfad, Parameter, Leerraum und Filter. Beispiel:

```
file://absoluter_pfad?parameter [leerraum] filter
```

cmeadmin
Die Protokollereignisse und -nachrichten werden in das Protokoll cmeadmin geschrieben.

Das Protokollausgabeprogramm cmeadmin verwendet die Protokollierungskomponenten Leerraum und Filter. Beispiel:

```
cmeadmin://[leerraum] filter
```

console
Die Protokollereignisse und -nachrichten werden in die Befehlszeilenkonsole geschrieben.

Das Protokollausgabeprogramm console verwendet die Protokollierungskomponenten Position, Parameter und Filter. Beispiel:

```
console://dateiposition?parameter filter
```

eventlog
(Nur Microsoft Windows-Plattformen) Die Protokollereignisse und -nachrichten werden in die Microsoft Windows-Ereignisanzeige geschrieben.

Das Protokollausgabeprogramm eventlog verwendet die Protokollierungskomponente Filter. Beispiel:

```
eventlog://./filter
```

Pfad Gibt die Position und den Namen der Datei an, in die die Protokolldaten geschrieben werden sollen:

Dateiadresse
Beispiele für gültige Werte:

- stdout - für das Protokollausgabeprogramm console
- stderr - für das Protokollausgabeprogramm console
- *absoluter_pfad* - für das Protokollausgabeprogramm file

Dateiname
Gibt an, in welche Standardproduktprotokolldatei die Informationen geschrieben werden sollen. Die Dateinamenerweiterung bestimmt den Protokolldateityp. Folgende Erweiterungen sind für die Protokolldateinamen möglich:

- .err
- .bad
- .msg
- .SqlDebug.log
- .SqlErr.log
- .MQErr.log

Parameter
Gibt optionale Protokollierungsparameter an. Beispiele für gültige Werte:

style=bare
Gibt an, dass die Protokollierung keine Zeitmarken oder andere Kopfdaten enthält. Dieser Parameter ist normalerweise in Dateien enthalten, die UMF-Nachrichten protokollieren.

rotateSize=*maximale_dateigröße*
Gibt die maximale Dateigröße der Protokolldatei in Kilobyte an. Wenn die Protokolldatei die maximale Dateigröße überschreitet, archiviert das System die Datei automatisch und erstellt eine neue Datei für die Protokollierung. Das System hängt eine 0 an den Namen der Archivdatei an und die neue Datei übernimmt den ursprünglichen Dateinamen. Dieser Vorgang wird so lange fortgesetzt, bis das System die maximale Anzahl Archivdateien erreicht, die im Parameter `keep` angegeben ist.

keep=*maximale anzahl archivdateien*
Gibt die maximale Anzahl der Archivdateien an, die während der automatischen Dateirotation gemäß dem Parameter `rotateSize` aufbewahrt werden sollen. Wird die maximale Anzahl Dateien überschritten, überschreibt das System die älteste Archivprotokolldatei mit den neuen Protokolldaten.

Leerraum
Gibt an, welche Art Leerraum in die Protokolldatei eingefügt werden soll. Beispiele für gültige Werte:

- Leerzeichen
- Tabulator

Filter Gibt die aufzuzeichnenden Protokolldaten an. Beispiele für gültige Werte:

Modul
Gibt den Typ der zu protokollierenden Nachrichten an. Beispiele für gültige Werte:

- $NODE_NAME - generische Nachrichten
- sql - SQL-Nachrichten
- mq - Nachrichtenwarteschlangennachrichten
- bad_xml - ungültige oder fehlerhafte UMF-Nachrichten
- msg - UMF-Ausnahmebedingungen
- logger - Nachrichten der Protokollfunktion

Sollen alle Modultypen angegeben werden, verwenden Sie das Platzhalterzeichen * (Stern). Beispiel:

```
console://stdout *.ERR
```

Wertigkeit
Gibt die Wertigkeit der Protokollnachricht an. Beispiele für gültige Werte:

- CRIT - kritische Nachrichten
- ERR - Fehlernachrichten

- WARN - Warnungen
- NOTE - Hinweise
- INFO - Informationsnachrichten
- PERF - Leistungsnachrichten
- DBUG - Debugnachrichten

Sollen alle Wertigkeitstypen angegeben werden, verwenden Sie das Platzhalterzeichen * (Stern). Beispiel:

```
console://stdout *.*
```

Soll eine Wertigkeit nicht berichtet werden, verwenden Sie das Ausrufezeichen. Beispiel:

```
console://stdout mq.!DBUG
```

Konfigurieren der angepassten Pipelineprotokollierung

IBM InfoSphere Identity Insight stellt Standardkonfigurationen für die Pipelineprotokollierung bereit, die festlegen, wie Pipelines Fehler und Nachrichten im Debugmodus und im Service-/Dämonmodus protokollieren. Es wird jedoch empfohlen, die Standardkonfiguration für die Pipelineprotokollierung modifizieren oder eine angepasste Protokollierungskonfiguration erstellen, um die spezifischen Anforderungen Ihres Unternehmens zu erfüllen. Zu diesem Zweck müssen Sie zwei Protokollierungsdateien erstellen, in denen die angepasste Protokollierungskonfiguration angegeben ist, und anschließend die Konfigurationsdatei für die Pipeline modifizieren, damit diese angepassten Protokollierungsdateien verwendet werden.

Informationen zu diesem Vorgang

Die Pipelineprotokollierung wird auf dem Pipelineknoten definiert. Daher müssen Sie diese Änderungen auf jedem Pipelineknoten vornehmen. Nachdem Sie die Debug- und Standardkonfigurationsdateien erstellt haben, können Sie sie auf jeden Pipelineknoten kopieren. Sie können entweder den Text im Abschnitt [logging] einer Pipelinekonfigurationsdatei kopieren und in eine andere Konfigurationsdatei einfügen, oder Sie können die gesamte Pipelinekonfigurationsdatei von einem Pipelineknoten auf einen anderen Knoten kopieren. Vergessen Sie dabei jedoch nicht, die Verbindungseinstellungen entsprechend anzupassen.

Vorgehensweise

1. Erstellen Sie mit einem beliebigen Texteditor zwei Dateien:
   a. eine Debugkonfigurationsdatei, in der die Protokollierung für Pipelines angegeben ist, die im Debugmodus arbeiten
   b. eine Standardkonfigurationsdatei, in der die Protokollierung für Pipelines angegeben ist, die im Service-/Dämonmodus arbeiten
2. Verwenden Sie in jeder Datei die entsprechenden Pipelineprotokollierungskomponenten, um die Protokollierung in diesem Modus für das System zu definieren.
3. Speichern Sie jede Datei. Es empfiehlt sich, diese Dateien in demselben Verzeichnis zu speichern, in dem sich die Pipelinekonfigurationsdatei befindet.
4. Fügen Sie in der Pipelinekonfigurationsdatei einen Abschnitt mit dem Namen `[logging]` hinzu. In diesem Abschnitt geben Sie die Namen der beiden Dateien für die Protokollierungskonfiguration an, die Sie erstellt haben.
5. Fügen Sie unter der Überschrift des Abschnitts `[logging]` die folgenden beiden Einstellungen hinzu:
   a. `DebugConfigFile=`*`name_der_konfigurationsdatei_für_debugprotokollierung`*

b. `ConfigFile=`*`name_der_konfigurationsdatei_für_service-/dämonprotokollierung`*

   Anmerkung: Wenn Sie die Dateien für die Protokollierungskonfiguration in einem anderen Verzeichnis als die Pipelinekonfigurationsdatei gespeichert haben, stellen Sie sicher, dass Sie den vollständigen Pfad der Datei angeben.

6. Speichern Sie die Änderungen der Pipelinekonfigurationsdatei.

Nächste Schritte

Damit diese Protokollierungsänderungen in Kraft treten, müssen Sie alle aktiven Pipelines auf jedem betroffenen Pipelineknoten stoppen und erneut starten.

Protokolldateien der Analyst Toolkit-Webanwendungen

Die Webanwendungen benötigen IBM WebSphere Liberty, um eine Verbindung zu IBM InfoSphere Identity Insight herzustellen und mit diesem Programm zu kommunizieren. Die Protokolldateien von WebSphere Liberty enthalten Informationen zu den Web-Services und den Analyst Toolkit-Anwendungen sowie WebSphere Liberty-Fehler. Wenn Ihr System für die Ereignisverarbeitung (mit dem Ereignismanager) aktiviert ist, werden Ereignisfehler auch in den Webfehlerprotokolldateien gespeichert.

Der Anwendungsserver enthält zwei primäre Protokolldateien, die für die Fehlerbehebung verwendet werden können:

- Standardausgaben- und Fehlerdatenströme, die in der Datei `console.log` protokolliert werden
- Von den Protokollierungskomponenten erfasste Nachrichten, die in der Datei `messages.log` protokolliert werden. Nachrichten, die in diese Datei geschrieben werden, enthalten weitere Informationen wie die Nachrichtenzeitmarke und die ID des Threads, von dem die Nachricht geschrieben wurde.

Diese Protokolldateien befinden sich im folgenden Verzeichnis:

`installationsverzeichnis``/wlp/usr/servers/iiServer/logs`

Protokolldateien von WebSphere Liberty werden von einem Systemadministrator auf dem Anwendungsserver konfiguriert.

Visualizer-Protokolldateien

Visualizer verfügt über zwei Protokolldateitypen, die den Benutzer bei der Behebung von Visualizer-Fehlern und bei Nachrichten unterstützen sollen: Eine lokale Protokolldatei für jeden Visualizer-Client und Protokolldateien für die Instanz von WebSphere Application Server, von der Visualizer gehostet wird.

Visualizer-Clientprotokoll

Sie können in der Konfiguration von Visualizer angeben, dass Fehler, Warnungen und Informationsnachrichten, die auf dem lokalen Visualizer-Client auftreten, protokolliert werden. Jede Workstation enthält einen Visualizer-Client, sodass Sie bestimmen können, ob Visualizer-Nachrichten nach Workstation protokolliert werden.

Die Visualizer-Clientprotokollierung ist standardmäßig inaktiviert. Die Visualizer-Protokollierung aktivieren bzw. inaktivieren Sie im Fenster **Benutzervorgaben für**

die Anzeige konfigurieren auf der Registerkarte **Protokolleinstellungen**. Hier wählen Sie auch die Protokolleinstellungen aus.

Die Verzeichnisposition der Visualizer-Clientprotokolldatei legen Sie bei der Aktivierung der Visualizer-Clientprotokollierung fest. Hierfür geben Sie den Namen des Verzeichnisses ein, oder Sie wählen ein vorhandenes Verzeichnis aus. Der Standardname der Visualizer-Clientprotokolldateien ist visualizer.log. Hierbei handelt es sich um eine Textdatei, die mit einem beliebigen Texteditor angezeigt werden kann.

Nachrichten werden an die vorhandene Protokolldatei angehängt, bis die maximale Dateigröße erreicht ist. Die maximale Größe für ein Visualizer-Clientprotokoll ist 1 Megabyte.

- Wenn die Protokolldatei die maximale Dateigröße erreicht, erstellt das System eine neue Visualizer-Clientprotokolldatei an der konfigurierten Verzeichnisposition und nimmt das Protokollieren von Nachrichten in dieser Protokolldatei auf.
- Sobald die zweite Protokolldatei die maximale Größe erreicht, wechselt das System automatisch zur ersten Protokolldatei, um die Nachrichten zu protokollieren, bis diese voll ist.

Dieser automatische Wechsel der Protokolldateien findet statt, sobald die aktuelle Protokolldatei ihr Größenlimit erreicht. Beim Wechsel der Protokolldateien werden die vorherigen Nachrichten in der Protokolldatei überschrieben.

WebSphere Application Service-Protokollierung

Visualizer benötigt WebSphere Application Server, um eine Verbindung zu IBM Relationship Resolution herzustellen und um mit IBM InfoSphere Identity Insight zu kommunizieren. Web-Service-Ereignisse werden zusammen mit den Ereignissen der Konfigurationskonsole, die auch WebSphere Application Server verwenden, in den Protokolldateien des Anwendungsservers protokolliert.

Der Anwendungsserver enthält zwei primäre Protokolldateien, die für die Fehlerbehebung verwendet werden können:

- Systemnachrichten, die in der Datei `SystemOut.log` protokolliert werden
- Systemfehlernachrichten, die in der Datei `SystemErr.log` protokolliert werden

Diese Protokolldateien befinden sich im folgenden Verzeichnis:

installationsverzeichnis`/logs/ewas`

Protokolldateien von IBM WebSphere Application Server werden von einem Systemadministrator auf dem Anwendungsserver oder durch das IBM InfoSphere Identity Insight-Konfigurationsdienstprogramm konfiguriert.

Aktivieren der Visualizer-Clientprotokollierung

Verwenden Sie die folgenden Anweisungen, um die Visualizer-Clientprotokollierung zu aktivieren und die Einstellungen für die Visualizer-Clientprotokollierung zu konfigurieren. Wenn Sie Änderungen an der Protokollierung oder den Einstellungen des Visualizer-Clients vornehmen, müssen Sie Visualizer erneut starten, bevor die Änderungen wirksam werden.

Informationen zu diesem Vorgang

Protokolleinstellungen für Visualizer-Clients werden für jeden lokalen Visualizer-Client konfiguriert. Wenn Sie die Protokollierung durch Ausführen der folgenden Anweisungen aktivieren, werden nur die Einstellungen für den Visualizer-Client auf diesem lokalen System beeinflusst.

Vorgehensweise

1. Wählen Sie **Benutzervorgaben** im Menü **Datei** aus.
2. Wählen Sie die Registerkarte **Protokolleinstellungen** aus.
3. Wählen Sie unter **Protokolleinstellungen** das Kontrollkästchen **Protokollierung aktivieren** aus, sodass ein Häkchen im Kästchen angezeigt wird. (Das Kontrollkästchen sollte ein Häkchen enthalten, wenn die Protokollierung aktiviert wurde.)
4. Wählen Sie die Protokolldetailebene im Auswahlfenster **Protokolldetailebene** aus.
   a. Wählen Sie **Fehler** aus, um Visualizer-Clientereignisse zu protokollieren, die Fehlernachrichten generieren. Diese Protokollebene ist die Standardprotokollebene, wenn die Protokollierung aktiviert wurde. Diese Protokollebene sorgt für eine Ausgewogenheit zwischen der Leistung und den Protokolldaten.
   b. Wählen Sie **Warnungen** aus, um Visualizer-Clientereignisse zu protokollieren, die Warnungen oder Fehlernachrichten generieren.
   c. Wählen Sie **Informationen** aus, um Visualizer-Clientereignisse zu protokollieren, die Informationsnachrichten, Warnungen oder Fehlernachrichten generieren.
   d. Wählen Sie **Debugging** aus, um Tracenachrichten für alle Visualizer-Ereignisse zu protokollieren. Diese Protokollebene wird in der Regel nur festgelegt, wenn Sie einen bestimmten Visualizer-Fehler beheben wollen, wofür häufig die Hilfe des IBM Support erforderlich ist. Die Protokollebene **Debugging** generiert möglicherweise eine große Anzahl Tracenachrichten, die für die Fehlerbehebung hilfreich sind, aber die Visualizer-Leistung im normalen Betrieb nachteilig beeinflussen können.
5. Geben Sie in das Feld **Verzeichnispfad der Protokolldatei** den vollständigen Verzeichnispfad und den Dateinamen für die Visualizer-Clientprotokolldatei ein, oder navigieren Sie zu einem vorhandenen Verzeichnis.
   - Geben Sie den vollständigen Verzeichnispfad für die Visualizer-Clientprotokolldatei ein.
   - Sie können auch zu einem vorhandenen Verzeichnis auf Ihrem lokalen System navigieren, um es als Visualizer-Clientprotokollverzeichnis auszuwählen.
6. Klicken Sie die Schaltfläche **Übergeben** an, um Ihre Änderungen zu speichern.
7. Starten Sie Visualizer erneut, indem Sie sich zuerst von Visualizer abmelden und sich dann erneut anmelden. Änderungen an Protokolleinstellungen Ihres Visualizer-Clients werden erst wirksam, wenn Sie Visualizer erneut starten.

Inaktivieren der Visualizer-Clientprotokollierung

Verwenden Sie die folgenden Anweisungen, um die Visualizer-Clientprotokollierung zu inaktivieren, insbesondere wenn Sie die Protokollebene 'Debugging' aktiviert haben, um ein spezifisches Visualizer-Problem zu lösen. Während Protokolldateien Sie beim Lösen von Problemen unterstützen können, wirken sich möglicherweise einige Ebenen der Protokollierung, wie z. B. die Protokollebene 'Debugging', auf die Visualizer-Leistung aus. Wenn Sie Änderungen an der Proto-

kollierung oder den Einstellungen des Visualizer-Clients vornehmen, müssen Sie Visualizer erneut starten, bevor die Änderungen wirksam werden.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie bei einer aktiven Visualizer-Sitzung angemeldet sind.

Informationen zu diesem Vorgang

Protokolleinstellungen für Visualizer-Clients werden für jeden lokalen Visualizer-Client konfiguriert. Wenn Sie die Protokollierung durch Ausführen der folgenden Anweisungen inaktivieren, werden nur die Einstellungen für den Visualizer-Client auf diesem lokalen System beeinflusst.

Vorgehensweise

1. Wählen Sie **Benutzervorgaben** im Menü **Datei** aus.
2. Wählen Sie die Registerkarte **Protokolleinstellungen** aus.
3. Wählen Sie unter **Protokolleinstellungen** das Kontrollkästchen **Protokollierung aktivieren** aus, sodass kein Häkchen im Kästchen angezeigt wird. (Das Kontrollkästchen sollte leer sein, wenn die Protokollierung inaktiviert wurde.) Wenn die Protokollierung inaktiviert wurde, sind die Konfigurationseinstellungen für die Protokollierung inaktiviert.
4. Klicken Sie die Schaltfläche **Übergeben** an, um Ihre Änderungen zu speichern.
5. Starten Sie Visualizer erneut, indem Sie sich zuerst von Visualizer abmelden und sich dann erneut anmelden. Änderungen an Protokolleinstellungen Ihres Visualizer-Clients werden erst wirksam, wenn Sie Visualizer erneut starten.

Protokolldateien des Ereignismanagers

Wenn Ihr System für die Verarbeitung von Ereignissen mithilfe des Ereignismanagers aktiviert ist, erstellt das System eine Protokolldatei, die Programminformationen zu Ereignissen enthält. Fehlernachrichten vom externen Ereignisprozessor werden in Fehlerprotokolldateien von WebSphere Liberty protokolliert. Während der Pipelineverarbeitung festgestellte Standardpipelinefehler werden basierend auf der aktuellen Pipelineprotokollierungskonfiguration in den Pipelineprotokolldateien protokolliert.

Der Anwendungsserver enthält die primären Protokolldateien, die zur Behebung von Fehlernachrichten und Problemen im Ereignismanager verwendet werden können:

- Programminformationen zum Ereignismanager, die in der Datei `gem_prog_`*`datum`*`.log` protokolliert werden
- Fehlernachrichten des Ereignismanagers, die im Verzeichnis *`installationsverzeichnis`*`/logs` protokolliert werden.

Nachrichten werden dem Programm- und dem Datenprotokoll nach Ereignisdatum angehängt. Diese Protokolldateien sollten regelmäßig überprüft werden und anschließend je nach den in Ihrem Unternehmen geltenden Richtlinien entweder archiviert oder gelöscht werden.

Diese Protokolldateien befinden sich im folgenden Verzeichnis:

`installationsverzeichnis``/logs`

Traceerstellung

Traces sind Aufzeichnungen der Komponenten- oder Transaktionsverarbeitung. Mit den von einem Trace erfassten Informationen können Sie Probleme und die Leistung beurteilen. In IBM InfoSphere Identity Insight sind Traces Teil der Protokollierung für Komponentendebugging.

Abrufen von Programmkorrekturen

Unter Umständen ist eine Produktkorrektur verfügbar, die Ihr Problem löst. Sie können Produktkorrekturen herunterladen, indem Sie die folgenden Schritte ausführen:

Vorgehensweise

1. Stellen Sie fest, welche Programmkorrektur Sie benötigen. Rufen Sie das Dokument *Fixes by version for IBM InfoSphere Identity Insight* auf, das Sie unter http://www-1.ibm.com/support/docview.wss?rs=2216&uid=swg27008307 finden. Klicken Sie anschließend eine der aufgeführten Programmkorrekturen an, um weitere Informationen zu allen Programmkorrekturen für die bestimmten Version anzuzeigen. (Programmkorrekturen werden mit den Angaben zu Version, Release und Änderung aufgeführt.)
2. Laden Sie die Programmkorrektur herunter. Klicken Sie in der Liste den Link **Download information** an. Klicken Sie im Abschnitt „Download package" den Link „Download Options" für Ihre Umgebung an.
   - Wenn die Anzeige mit der IBM Lizenzvereinbarung geöffnet wird, lesen Sie die Informationen und klicken Sie **I Accept** an, wenn Sie die Vereinbarung akzeptieren und mit dem Herunterladen der Programmkorrektur fortfahren wollen.
   - Wenn Sie **I Do Not Accept** anklicken, wird die Programmkorrektur nicht heruntergeladen.

   Klicken Sie in den Fenstern **File Download** die Option **Save** an und speichern Sie die Programmkorrekturdatei lokal.
3. Wenden Sie die Programmkorrektur an. Wechseln Sie zur Speicherposition, an der die Programmkorrekturdatei gespeichert wurde. Extrahieren oder dekomprimieren Sie die Dateien aus der komprimierten Programmkorrekturdatei und befolgen Sie die Anweisungen in der Readme-Datei, um die Programmkorrektur zu installieren.

Informationen zu Programmkorrekturen und Funktionsaktualisierungen

Wenn Sie in IBM InfoSphere Identity Insight auf ein Problem stoßen, prüfen Sie zuerst die Liste empfohlener Aktualisierungen, um zu bestätigen, dass das neueste Programmfix auf Ihre Software angewendet wurde. Prüfen Sie dann in der Liste der korrigierten Fehler, ob IBM bereits einen Einzelfix zum Beheben Ihres Problems veröffentlicht hat.

Einzelfixes werden so häufig veröffentlicht, wie es zur Behebung von Mängeln im Produkt erforderlich ist. Zudem werden zwei Arten von kumulativen Programmkorrektursammlungen (Fixpacks und Refresh-Packs genannt) regelmäßig veröffentlicht, um Benutzer auf den neuesten Stand zu bringen. Installieren Sie diese Aktualisierungspakete so schnell wie möglich, um Probleme zu vermeiden.

Abonnieren Sie E-Mail-Aktualisierungen von der Unterstützungsfunktion (My Support), um wöchentlich Benachrichtigungen zu Programmkorrekturen und Aktualisierungen zu erhalten.

In der folgenden Tabelle werden die Merkmale der einzelnen Fehlerkorrekturtypen beschrieben.

Tabelle 39. Merkmale einer Programmkorrektur, eines Fixpacks und eines Refresh-Packs

Name	Merkmale
Programmkorrektur	• Ein Einzelfix, der zwischen Aktualisierungen veröffentlicht wird, um ein bestimmtes Problem zu beheben, z. B. PQ79582. • Testen Sie nach der Installation einer Programmkorrektur alle Funktionen, auf die sich die korrigierte Komponente auswirkt.
Fixpack	• Ein kumulatives Programmkorrekturpaket, das alle seit dem vorherigen Fixpack oder Refresh-Pack veröffentlichten Programmkorrekturen enthält. Ein Fixpack kann auch neue Programmkorrekturen enthalten. • Fixpacks erhöhen die Modifikationsstufe des Produkts und werden entsprechend benannt, z. B. 4.0.2. • Ein Fixpack kann bestimmte Komponenten oder das gesamte Produktimage aktualisieren. • Während der Fixpackinstallation werden alle zuvor angewendeten Fixes automatisch deinstalliert. • Nach der Installation eines Refresh-Packs sollten Sie alle kritischen Funktionen einem Regressionstest unterziehen. • Die beiden letzten Fixpacks können heruntergeladen werden (z. B. 4.0.2 und 4.0.1). Frühere Fixpacks sind nicht als Download verfügbar.
Refresh-Pack	• Ein kumulatives Programmkorrekturpaket, das alle seit dem vorherigen Fixpack oder Refresh-Pack veröffentlichten Programmkorrekturen und neue Programmkorrekturen enthält. • In der Regel enthält ein Refresh-Pack zusätzlich zu Programmkorrekturen neue Funktionen und aktualisiert das gesamte Produktimage. • Refresh-Packs erhöhen die Modifikationsstufe des Produkts und werden entsprechend benannt, z. B. 4.0.2. • Während der Fixpackinstallation werden alle zuvor angewendeten Fixes automatisch deinstalliert. • Nach der Installation eines Refresh-Packs sollten Sie alle kritischen Funktionen einem Regressionstest unterziehen.

Funktionsaktualisierungen

Mit Funktionsaktualisierungen können Sie Ihr System auf dem neuesten Software-Maintenance-Stand halten.

Sie können über die IBM InfoSphere Identity Insight-Produktunterstützungsseite auf die neuesten Funktionsaktualisierungen zugreifen. Die URL lautet:

```
https://www-947.ibm.com/support/entry/portal/Overview/Software/
Information_Management/InfoSphere_Identity_Insight
```

Gehen Sie wie folgt vor, um den Pipeline-Service-Level auf Ihrem System zu ermitteln:

1. Geben Sie den folgenden Befehl in eine Befehlszeile auf dem Pipelineknoten ein:

   ```
   pipeline
   ```

2. Die Pipelineversion befindet sich in der ersten Zeile. Die Zahl legt den Service-Level fest.

Gehen Sie wie folgt vor, um den Service-Level der Konfigurationskonsole auf Ihrem System zu ermitteln:

1. Starten Sie die Konfigurationskonsole.
2. Melden Sie sich an der Konfigurationskonsole an.
3. Wählen Sie **Produktinfo** aus dem Menü oben aus.
4. Sehen Sie sich die im Fenster **Produktinfo** angezeigte Versionsnummer an. Die Zahl legt den Service-Level fest.

Kontaktieren des IBM Software Support

Vom IBM Software Support erhalten Sie Hilfe bei Produktfehlern.

Vorbereitende Schritte

Bevor Sie sich an den IBM Software Support wenden, muss Ihr Unternehmen einen gültigen IBM Softwarewartungsvertrag abgeschlossen haben und Sie müssen berechtigt sein, Probleme an IBM zu übergeben. Informationen zu den Typen verfügbarer Wartungsverträge finden Sie im Abschnitt „Enhanced Support" des *Software Support Handbook* unter techsupport.services.ibm.com/guides/services.html.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um den IBM Software Support bei einem Problem zu kontaktieren:

Vorgehensweise

1. Definieren Sie das Problem, stellen Sie Hintergrundinformationen zusammen und bestimmen Sie den Schweregrad des Problems. Hilfe hierzu finden Sie im Abschnitt „Contacting IBM" des *Software Support Handbook* unter techsupport.services.ibm.com/guides/beforecontacting.html.
2. Stellen Sie Diagnoseinformationen zusammen.
3. Sie sollten die folgenden Informationen im Fehlerbericht für den IBM Software Support bereitstellen können:
   - Produktname und -version
   - Datenbanktyp und -version
   - Betriebssystemname und -version
4. Übergeben Sie Ihr Problem mit einer der folgenden Methoden an den IBM Software Support:
   - Online: Klicken Sie die Option zum Senden und Nachverfolgen von Problemen auf der Website des IBM Software Support unter http://www.ibm.com/software/support/probsub.html an.

- Telefonisch: Die Telefonnummer, die Sie für einen Anruf in Ihrem Land benötigen, finden Sie auf der Seite mit den Ansprechpartnern im IBM Software Support Handbook unter techsupport.services.ibm.com/guides/contacts.html.

Nächste Schritte

Wenn das Problem, das Sie übergeben, einen Softwarefehler oder fehlende bzw. fehlerhafte Dokumentation betrifft, erstellt der IBM Software Support einen APAR (Authorized Program Analysis Report). Der APAR beschreibt das Problem detailliert. Wann immer dies möglich ist, stellt der IBM Software Support eine Ausweichlösung bereit, die Sie implementieren können, bis der APAR behoben und eine entsprechende Programmkorrektur geliefert ist. IBM veröffentlicht behobene APARs täglich auf der Website des IBM Software Support, sodass andere Benutzer, bei denen dasselbe Problem auftritt, von derselben Lösung profitieren können.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für die in diesem Handbuch beschriebenen Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
J46A/G4

555 Bailey Avenue
San Jose, CA 95141-1003
USA

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM. Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellensprache geschrieben sind und Programmiertechniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten.

Marken

IBM Marken und bestimmte Marken anderer Hersteller sind bei ihrem ersten Vorkommen in diesen Informationen mit dem entsprechenden Symbol gekennzeichnet.

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Sind diese und weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

Die folgenden Namen sind Marken oder eingetragene Marken anderer Unternehmen:

Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Intel, das Intel-Logo, Intel Inside, das Intel Inside-Logo, Intel Centrino, das Intel Centrino-Logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium und Pentium sind Marken oder eingetragene Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA oder anderen Ländern.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

Java und alle auf Java basierenden Marken sind Marken der Oracle Corporation in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken oder Servicemarken anderer Hersteller sein.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z